CHARLES UNIVERSITY

FACULTY OF LAW

Mgr. Jiří Moravec, J.D.

Financial Aspects of Global Payment Systems

Dissertation Thesis

Dissertation Thesis Supervisor: doc. JUDr. Michael Kohajda, Ph.D.
Study program: Theoretical Legal Sciences – Financial Law and Financial Science
Completion Date (Closure of Manuscript): 22. 06. 2022

I hereby declare that I have prepared the present dissertation Thesis independently, that all sources used have been properly acknowledged and that the work itself has not been used to obtain another or the same degree.

I further declare that the actual text of this Thesis, including footnotes, is characters 420 047 long, including spaces.

Prohlašuji, že jsem tuto disertační práci vypracoval samostatně, že jsem řádně uvedl všechny použité prameny a že práce samotná nebyla použita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této disertační práce včetně poznámek pod čarou má 420 047 znaků včetně mezer.

Mgr. Jiří Moravec, J.D.

V Praze dne:

Acknowledgements

I would like to express my utmost gratitude to my supervisor doc. JUDr. Michael Kohajda, Ph.D., who has kindly supported me throughout the creation of this Thesis. His valuable advice, leadership, and organization has been a great antipole to my somehow chaotic state of mind.

No less of my appreciation belongs to my parents, who have expressed a great interest not only in me and my struggles, but also in this complicated topic itself. Thank you very much.

My dearest thanks also belong to all of the academics of Department of Financial Law and Finances, who allowed me to research this topic.

I cannot forget of Giulia and her obscure obsession with this Thesis, which I summarize as: "*Sarebbe un vero idiota non finire questa tesi.*" Quindi, l'ho finito. Grazie.

Table of Contents

1. Introduction to Financial Aspects of Global Payment Systems

1.1. General introduction to the researched topic

Bitcoin and Digital Assets[1] represent an area in which we have been interested in for quite some time now. Our first exposure dates back to 2013, when have been fascinated by the geniality of the invention and its immense technological promise and also the surrounding mysticism of its unknown creator. That is why we have decided to understand this topic more thoroughly and were grateful for the opportunity to write a Thesis about it.

Even now Digital Assets are widely considered to be a revolution happening in front of our eyes. There are many voices echoing with the promise of independent finance. Secure and fast transactions that are also very cheap compared to the classic payment systems. Improved anonymity and governance of one's monetary funds. Followed by statements like "be your own bank" has motivated millions of people to start using (investing in) Digital Assets. After all the technology behind Digital Assets the Blockchain promises to achieve a new financial order and then a new trustless society.

We were therefore very interested in evaluating what Bitcoin and other similar projects, what should be the regulatory response to them and what is the general value it brings to the society. However, the more time we have spent studying the topic at hand, the more negative our general feeling about Digital Assets was. This led us to question, whether any comprehensive regulation of Digital Assets is actually needed or whether their use should be outright banned as certain countries did.

The situation with Digital Assets is sort of grotesque. While the technological and possibly even societal promise of a revolution in governance is entirely real, the general society still ignores Digital Assets and the majority of those who say that are interested in Digital Assets, namely

[1] Please see: General Explanations

its users, do not use Digital Assets for payments. As such, when we wanted to approach this topic as a review of new global payment systems and evaluate it from legal point of view, we quickly figured that we have to change our approach.

We therefore decided to evaluate Digital Assets based on its material use and see the regulatory response to them and if it can bring something valuable to the society or whether it should be outright banned or heavily restricted as it happened in some jurisdictions. We believe that for an evaluation of such complicated and complex topic as Digital Assets are, one should focus on this phenomenon with all of its aspects. We therefore divide the Thesis in two major parts in harmony with following research questions.

1.2. Introduction to the historically technical part

In the first part of this Thesis, we are establishing ground for further understanding of the new phenomenon. The first part itself is composed of two major areas, which are mutually interconnected. We are starting with the history of Digital Assets in a view of private digital payment systems.

1.2.1. Can the history of Digital Assets help us with its understanding and with regulatory approach?

To answer this question, we have chosen a number of now discontinued projects that all show the struggle of its developers to find the technology that would allow them to operate a payment system using the Internet, which itself would not be dependent on the financial system.

We have chosen the BitGold, B-Money and other similar systems because the mysterious developer of Bitcoin has said in his whitepaper that he had drawn inspiration from some of them. We believe that had drawn inspiration from all of them. We further believe that the inspiration was not purely technical, but that he has also evaluated the failure of such projects from legal

point of view. Because, as we will show in the case relating to E-Gold, creating a private payment system, and taking credit for its creation will most likely get you sued.

Given that this topic is quite technically challenging we also decided to help readers ease in the dedicated technological part, by explaining some of the fundamental technology used for functioning of Digital Assets in the historical part. Therefore, we describe the origins of the technological solutions using the above-mentioned projects as examples. An approach we use in different light and shape through the Thesis. The technological aspect of this historical part also shows the research and development that not only leads to a payment system without a trusted third-party, but also to a payment system without a liable creator and intermediary.

1.2.2. What are the technological aspects of Digital Assets?

The next chapter following after the predominantly historic approach is purely technological. We are looking at Blockchain and the way it works and into its division. We believe that for future regulation of Digital Assets the thorough understanding of the technology behind them will be crucial. Further, we consider that a common user of Digital Assets has a very limited understanding how Digital Assets function. However, a minority of Digital Assets users poses a substantial knowledge about Digital Assets and is able to use this information asymmetry to personal gain and to commit various crimes.

We thus provide summary of the main Blockchain components giving some actual examples derived from Bitcoin functionality. We strive to provide a common reader the deeper understanding of Blockchain and its risks. We also use the contents of this chapter for the second part of the Thesis.

1.3. Introduction to the social, criminal, and regulatory part.

In the second part of this Thesis, we aim to be more current and practical. We are looking at Digital Assets not as virtual currencies as they are often called, but rather by its practical use.

1.3.1. What is the actual use of Digital Assets?

Digital Assets are often promoted as novel and revolutionary payment system. To a person not familiar with the situation surrounding Digital Asset economy a large part of the Internet users is giving the feeling that investing fiat money in Digital Asset would be largely beneficial for her. However, mostly the opposite would be true.

Using this research question, we were interested not only in the actual use of Digital Assets, but also what its use can cause to society and repressive authorities. Having established that apart from small numbers of user no one use Digital Assets for payments. We evaluate its other use, which is predominantly risky investments, but also outright scams.

1.3.2. Are Digital Assets and associated service providers abused or used for criminal activity?

Further, using the two previous parts and available resources, we summarize the general characteristics of Digital Assets, and we show that while Digital Assets could positively impact the financial inclusion it serves as a major tool in different criminal schemes.

The more one knows about Digital Assets and its Aspects, the more this question makes sense. We further considering whether the Digital Assets are being used by criminals even if its intended use would be primarily legitimate or whether the Digital Assets and associated services are developed and used with malice from the very beginning.

1.3.3. To what extend are Digital Assets integrated in the current regulatory framework?

Using mostly the case studies we describe in other parts of the Thesis we are looking at the regulatory response from various authorities. We are describing the issues connected with integration of Digital Assets in existing legal framework, but we are also showing that without mutual international approach such endeavors are hardly possible.

1.3.4. Do Digital Asset make any sense as global payment systems?

Given that our approach to Digital Assets have proven to be rather negative, we evaluate if there is at least a subset of Digital Assets, which we would not find predominantly troubled and abused. In the last section of the second part of this Thesis we focus on so called Stablecoins. Over the time we were working on this Thesis European Union has proposed its first comprehensive regulation of Digital Assets, which seems to be aimed on Stablecoins as well, and therefore we are also considering its scope and approach.

1.3.5. Methodology

Here we present short summary of used scientific methods. At the beginning of the Thesis, we used a combination of analytic and descriptive method to explain some of the basics to our readers. Descriptive method also prevails when we talk about the historic and technical part. Nevertheless, we also analyze some of the posed issue therein. As we continue with the paper, we use more of analytic and synthesis method, to show and explain practical examples. We mostly employ the analytic and synthesis method in the part of the Thesis, where we research, whether Digital Assets are used or abused. Comparative method is used sporadically, throughout the Thesis, usually only when we draw partial conclusions.

Before we begin with the Historic part itself, we also provide an introductory chapter called General Explanations, which should help the reader to find her way around the rather complex topic that follows.

2. General Explanations

2.1. The necessity of simplification – why we are using bitcoin as an example

In this Thesis, we are facing a complex issue. Bitcoin, which started as an obscure project, have sparked the origin of wide variety of new services and businesses. Not only it created its own environment. Its technology transcendences to existing businesses and promises to influence them.[2] Thereby, creating its secondary sphere of influence.

The primary environment is rapidly growing. In 2008 Bitcoin was introduced, being the first "Cryptocurrency". Five years later, in 2013 there was approximately 66 similar projects.[3] As of now, the number have grown to over 10.000.[4] With some sources evidencing even higher numbers.[5] While most of those digital assets is completely irrelevant. Each of them is unique and might become a technological breakthrough such as Bitcoin in 2008.

It is not just the inflation of new projects that makes this topic complex. Among others, it is also its underlining technology the Blockchain, the decentralized nature of majority of the projects, and the fractional regulation. For a person who does not follow this phenomenon from the beginning, it may be difficult to establish a reference point.

To help our readers understand this topic and establish such a point. We decided to simplify the specific scope of the Thesis. Therefore, the introductory parts and majority of the examples

---

[2] The technology behind Bitcoin, the Blockchain, is promising to change many business branches including the banking and finance, healthcare, supply chain management, real estate, big data, internet of things, and many others. INSIDER INC. The growing list of applications and use cases of blockchain technology in business and life. Insider.com [online]. 2022 [cit. 2022-03-23]. Available at: https://www.businessinsider.com/blockchain-technology-applications-use-cases (archived version available via: https://archive.ph/E0o6k)

[3] Number of cryptocurrencies worldwide from 2013 to February 2022. Statista.com [online]. 2022, February 8, 2022 [cit. 2022-03-21]. Available at: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/ (archived version available via: https://archive.ph/IkZGD)

[4] *Id.*

[5] The webpage CoinMarketCap, which evidence, among others, the valuation, and graphs of most of the existing digital assets projects states over 18.000 different digital assets. Cryptocurrency prices, Charts and Market Capitalizations. Coinmarketcap.com [online]. March 21, 2022 [cit. 2022-03-21]. Available at: https://coinmarketcap.com (archived version available via: https://archive.ph/58VUG)

throughout the Thesis will be focused on Bitcoin[6]. As most of the novelties, unique terminology, and technology stems from the invention[7] of Bitcoin, it forms the best reference point. Further Bitcoin is usually the most used and researched project, therefore most of the available materials do the same.

2.2. On the used notion Digital Asset

2.2.1. Introduction

The advent of Bitcoin fueled vast number of scientific, economic, academic, and legal articles. To describe and categorize the new technology, the authors of such articles have used various notions. To this day however, the terminology is rather diverse, even though it is developing. In this part, we explain why we diverted from the typical terminology and why we decided to use the collocation Digital Assets[8].

Since the early years following Bitcoin's inception the predominantly used descriptive collocation was Virtual Currency[9]. This term seems to have established and even in 2021-2022 is still widely used[10]. Jointly with the notion Virtual Currency authors have also used the nomenclature Digital

[6] For further clarity, we are using "Bitcoin" with capital "B" any time we are addressing the network as a whole (as a whole payment system) and we are using "bitcoin" with lower case "b" when we are addressing its medium of exchange.

[7] As the reader can read on the following pages dedicated to the historical-technical development, some of Bitcoin's predecessors came very close to facilitate the same functions as Bitcoin with a different technical solution and most of the technology behind Bitcoin comes from such projects.

[8] As the time has progressed while we were writing the Thesis, the notion Digital Assets became used more widely.

[9] Early examples the use of Virtual Currency in reputable sources: EUROPEAN CENTRAL BANK. Virtual Currency Schemes [online]. October 2012. EU, 2012 [cit. 2022-03-21]. ISBN 978-92-899-0862-7. Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (archived version available via: https://archive.ph/jYQ4f) or in: SMITH, Daniel. More Money, More Problems: The Bitcoin Virtual Currency and the Legal Problems that Face it. Journal of Law, Technology, & the Internet. Texas, USA, 2012, 3(2), 427-442. ISSN 1949-6451. Available also at: https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1035&=&context=jolti&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fq%253Dvirtual%252Bcurrency%252Bbitcoin%2526hl%253Den%2526as_sdt%253D0%25252C5%2526as_ylo%253D2008%2526as_yhi%253D2012#search=%22virtual%20currency%20bitcoin%22 (archived version available via: https://archive.ph/fwjJW)

[10] YANO, Mokoto, Chris DAI, Kenichi MASUDA a Yoshio KISHIMOTO, at all. Blockchain and Crypt Currency: Building a High Quality Marketplace for Crypt Data. Tokyo, Japan: Springer, 2020, 1-135. ISBN 978-981-15-3376-1. Also available at:

Currency[11]. For which we have also partially argued in our first work, and we suggested that Bitcoin should be referred to as the "digital medium of exchange", even if we were more focused on the difference between the adjectives virtual and digital.[12] Also, the denomination Digital Currency is still used in the academic articles[13], however sporadically. It is because in the recent years terminology Digital Currencies it is associated with more apt monetary instrument – Central Bank Digital Currency (CBDC)[14].

Further, the name Cryptocurrency is used as a synonym to Virtual Currency and Digital Currency. While Virtual Currency and Digital Currency are predominantly used in the academic and scientific sphere, Cryptocurrency or simply Crypto seems to be the term used by its developers, users, and ordinary people. Nevertheless, some academic articles still use it as well.[15]

For the purpose of this Thesis, we decided not to use any of the above-mentioned terms. Our main rational is that none of those notions is precise and could be potentially misleading.

---

https://library.oapen.org/bitstream/handle/20.500.12657/37713/2020_Book_BlockchainAndCryptCurrency.pdf?sequence=1#page=71 (archived version available via: https://archive.ph/3WkhM)

[11] Early examples the use of Digital Currency in reputable sources: KAPLANOV, Nikolei. Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation. Loyola Consumer Law Review [online]. USA: LAW eCommons, 2012, 2013, 25(1), 111-174 [cit. 2022-03-22]. Available at: https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1920&context=lclr (archived version available via: https://archive.ph/Qsksl) or in: DOGUET, Joshua. The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System. Louisiana Law Review [online]. Luisiana, USA: LSU Law Digital Commons, 2013, 73(4), 1120-1153 [cit. 2022-03-22]. Available at: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=6425&context=lalrev (archived version available via: https://archive.ph/Qsksl)

[12] MORAVEC, Jiří. Bitcoin - Legal Aspects and Regulation. 2016. Master thesis. Charles University, Faculty of Law, Department of Financial Law and Financial Science. Thesis supervisor Kohajda, Michael. Available at: https://dspace.cuni.cz/bitstream/handle/20.500.11956/82909/DPTX_2015_2_11220_0_327151_0_177426.pdf?sequence=1&isAllowed=y (archived version available via: https://archive.ph/KSLok)

[13] FANUSIE, Yaya a Tom ROBINSON. Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services [online]. 2018, s. 1-16 [cit. 2022-03-22]. Available at: https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf (archived version available via: https://archive.ph/rfvPg)

[14] A CBDC is a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank. BANK OF INTERNATIONAL SETTLEMENTS. Central bank digital currencies: foundational principles and core features [online]. 2020, 1-21 [cit. 2022-06-14]. Available at: https://www.bis.org/publ/othp33.pdf (Archived version available via: https://archive.ph/Ztscf)

[15] DROZD, Oleksii, Yaroslav LAZUR and Ruslan SERBIN. THEORETICAL AND LEGAL PERSPECTIVE ON CERTAIN TYPES OF LEGAL LIABILITY IN CRYPTOCURRENCY RELATIONS. Baltic Journal of Economic Studies [online]. 2017, 3(5), 221-227 [cit. 2022-03-22]. Available at: http://www.baltijapublishing.lv/index.php/issue/article/view/289/pdf (archived version available via: https://archive.ph/7g4C2)

2.2.2. Virtual, digital, or cryptographic?

First point to argue in our reasoning is that each of those collocations are a combination of the word currency and an adjective. While the adjectives are rather fitting, there is still the need to select the corresponding one.

As a second point, we a priori decided to exclude the adjective "cryptographic" or "crypto". Cryptographic, derived from the word "Cryptography", means "the use of special codes to keep information safe in computer networks."[16] However, the use of cryptographic in connection with currency in this sense is figurative. It originated due to the fact that the technology behind Bitcoin is based on cryptographic proof. However, on the Internet cryptography is used everywhere and for wide variety of purposes. Majority of all applications, communications, computer programs, raw data, and websites are encrypted. Therefore, while cryptographic (crypto) is theoretically possible to use in connection with Bitcoin and similar projects we do not prefer it. As outlined above, the usage of this term is rather disconnected from the academic sphere. Also, due to the connection of the term "crypto" to general talk as compared to academic or scientific research, we feel its use would be unprofessional.

In the next lines, we are going to decide between virtual and digital. The meaning of the adjective "Virtual" is defined as "something that is not physically existing but made by a software to appear to do so."[17] A similar definition can be find also in the Cambridge dictionary: "[something] created by computer technology and appearing to exist but not existing in the physical world."[18]

[16] Cambridge Dictionary: Meaning of cryptography in English in computing [online]. [cit. 2022-03-27]. Available at: https://dictionary.cambridge.org/dictionary/english/cryptography (Archived version available via: https://archive.ph pF4UM)

[17] Lexico - English Dictionary. Lexico.com [online]. [cit. 2022-03-27]. Available at: https://www.lexico.com/en/definition/virtual (Archived version available via: https://archive.ph/CR2Lz)

[18] Cambridge Dictionary: Meaning of virtual in English [online]. [cit. 2022-03-27]. Available at: https://dictionary.cambridge.org/dictionary/english/virtual (Archived version available via: https://archive.ph/ZAtf3)

The meaning of the adjective “Digital” is defined as something “expressed as series of the digits 0 and 1. Relating to, using, or storing data or information in the form of digital signals.”[19] In this case the Cambridge dictionary has the exact same definition. Nevertheless, to prove our point we would like to also show the meaning of the word “Digitalize”, which according to Etymology Online means “*[to] convert into sequence of digits*.”[20]

The definitions above suggest the main difference between the two adjectives. Virtual is something often contained in a designed environment without a direct intractability with the real world. In our opinion, a good example is virtual in game object. Such object is limited with interaction to preset rules in a computer game. Such as a legendary sword or a tank. The virtual object cannot leave the given boundaries and does not have any additional use, then in given game. In example such object cannot be sold.

Whereas digital does not seem to be held by such boundaries. Digital has the meaning as being expressed in certain way. Further, it seems to us that digital is not confined to an artificial environment, rather it belongs to the real world, even if it can be manipulated trough a specific technology.

Since Bitcoin is not confined to a predefined virtual world, but rather allows for interaction with the real world. We decided to pick the adjective digital as it seems to fit out purposes better than the adjective Virtual.

[19] Lexico - English Dictionary. Lexico.com [online]. [cit. 2022-03-27]. Available at: https://www.lexico.com/en/definition/digital (Archived version available via: https://archive.ph/FYgky)

[20] Online Etymology Dictionary: Digitalize. Etymonline.com [online]. [cit. 2022-03-27]. Available at: https://www.etymonline.com/word/digitalize#etymonline_v_53950 (Archived version available via: https://archive.ph/UZ2gx)

2.2.3. On the issue of money

Having addressed the adjectives, we can focus on the main issue, which is with the word currency itself. Not only that currency is a word with stable meaning in the general society it also bears distinctive legal sense.

As for its legal meaning, currency is sort of higher level of money. In theory, currency therefore requires that the underlining medium should amount to money. While currency is a strictly formal term. The term money has more perspectives to weigh in on. First, we are going to address the monetary aspects.

From the formal point of view and in the words of Bank of England: "In particular, something may be considered money from the perspective of economic theory to the extent that it serves as a medium of exchange with which to make payments; a store of value with which to transfer 'purchasing power' (the ability to buy goods and services) from today to some future date; and a unit of account with which to measure the value of any particular item for sale."[21]

Whether private digital mediums of exchange such as Bitcoin satisfies even the basic economic function of money is a subject to ongoing discussions. However, during the composition of this Thesis, we did not find one (reliable) source that would prove that Bitcoin is money[22]. Dr. Saifedean Ammous in his paper: Can cryptocurrencies fulfil the functions of money?[23] gives

[21] ROBLEH, Ali, John BARRDEAR, Roger CLEWS a James SOUTHGATE. *Innovations in payment technologies and the emergence of digital currencies* [online]. Bank of England Quarterly Bulletin 2014 Q3. 2014, 262-275 [cit. 2022-03-23]. Available at: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/innovations-in-payment-technologies-and-the-emergence-of-digital-currencies.pdf?la=en&hash=AB46869B3EF355A0486F7B0BAF086F2EEE31554D (archived version available via: https://archive.ph/lw1wj)

[22] MORAVEC, Jiří. The Perfect Digital Money That Nobody Wants. Daně a finance. 2019, 27 (3-4), 30-35. ISSN 1801-6006.

[23] AMMOUS, Saifedean. *Can cryptocurrencies fulfil the functions of money?* [online]. In: Working Paper no. 92. Columbia University: Center on Capitalism and Society, 2016, 2016, s. 1-31 [cit. 2022-03-22]. Available at: https://capitalism.columbia.edu/files/ccs/workingpage/2017/ammous_cryptocurrencies_and_the_functions_of_money.pdf (archived version available via: https://archive.ph/wp2vT)

at least some hope to Bitcoin to satisfy the economic functions of money. He argues that: "Cryptocurrencies are currently wholly inadequate as a unit of account due to fluctuating demand and inflexible supply, and the absence of an authority that can manage the supply to maintain a constant value. Of the cryptocurrencies studied here, and arguably, of all cryptocurrencies, only bitcoin can attract demand as a store of value, due to the high degree of credibility and predictability to its supply and the resilience it has shown in eight years of existence."[24] Nevertheless, Dr. Ammous adds that all the "Cryptocurrencies", including Bitcoin have a long way to go, before being able to satisfy the basic monetary functions.[25]

The fact that Bitcoin and similar projects does not satisfy the monetary economic functions is nothing new and not much has changed since it was argued for the first time. Nevertheless, as suggested by Dr. Ammous things are relative and development is still possible. We share the opinion.

We agree that, theoretically, there is certain hope for Bitcoin to become money. In his philosophical article called How is Bitcoin Money Ole Bjerg essentially argues that all types of money are flawed.[26] Bitcoin and the money we are, as a society using now, are both flawed. Is Bitcoin susceptible to financial crime? Well, it is. A lot of people have probably first heard about Bitcoin in connection with a massive scam. On the other hand, isn't Dollar or Euro susceptible to financial crime? Well, it is. Similarly, one can argue that Bitcoin has no intrinsic value. But what is the value of credit money (money established by future obligations and claims)? Often represented only by some data kept in a ledger on a network. Isn't such concept pretty much

[24] *Id*. at 26
[25] *Id*.
[26] BJERG, Ole. How is Bitcoin Money. Theory, Culture & Society. Copenhagen Business School: Sage, 2016, 33(1), 53-72. DOI: 10.1177/0263276415619015, Available at: https://d1wqtxts1xzle7.cloudfront.net/52627298/Theory_Culture_Society-2015-Bjerg-with-cover-page-v2.pdf?Expires=1648047733&Signature=BbLNI~gZ15z1FUzSDXcv3QqM8P7VRccd-NnPoB-21TGLo1~QmmTS9U6kkRqdhIPEKax2GFMCqBXNCHRTGDh3plBfQ0vWKRJznSt0c05u~pscZnpsUHOdsTALR-9d8m9kSpLihSZu6IMt0UPCJHgB4XrfsGJC4iQY-oF1ASAPJrg0-erqSN4Gi27VLvRHx-90ZFcJTGSIwipwQb8GSUF84jFA4UqPoWBqgwsj1IB0tmBKdS9orin5xsLbblKFENL~YTr4AnN~1ijlaBqM2q-bGcz5klaj-I3KSl1yh0LKcU7huUCdwje6iXxXbiuEP7miPKUp8KoZ~Zf6N5NLpLKaww__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (archived version available via: https://archive.ph/DAMZn)

the same as Bitcoin? This analogy could continue, but as Mr. Bjerg summarizes in a way similar to Churchill: "Bitcoin is the worst form of money, except for all the others".[27]

The point we can take from Mr. Bjerg's article is that the society accepts the flaws of the money they are using, and therefore even an object that is inherently flawed might be used as (become) money, if the society decide to do so[28]. Which made us to question the following:

1. Do people intent to use Bitcoin as a medium of exchange (monetary instrument)?
2. What is the predominant use case of Bitcoin?

In order to answer the questions, we have decided on dual approach. First, research and evaluate the general mood of Bitcoin users to see if we can understand their intentions and second assess what they are actually doing.

The first part was a very easy endeavor. The Internet is full of people broadcasting their intention to "invest" in Bitcoin especially on social networks and forums. Further, we have spent years around the Bitcoin community and the mood does not seem to have changed since 2013. One notable example from 2013, which defines the community, is a bulletin post on a forum Bitcointalk.com. This post gave rise to now accustomed term "HODL", which is nothing else then misspelled term hold.[29] The meaning of the post is, that the post author is not selling his bitcoins, because he is expecting increase in their value in long term. The responses from other user in the thread are predominantly stating that they are also holding expecting the increase in value.[30]

---

[27] *Id*. at 69

[28] In example the "Cigarette Money" as described in an article under the same name in: BURDETTH, Kenneth, Alberto TREJOS a Randall WRIGHT. [online]. January 22, 2000, 117-142 [cit. 2022-03-25]. Available at: https://reader.elsevier.com/reader/sd/pii/S0022053100927315?token=9BCC20937B3F6F87286305271751 44BC7D491EA93AEA67F71BD89CA5500BFA3F69BD4E8463D50F1B864066A35D2DC12E&originRegion=eu-west-1&originCreation=20220325134415 (Archived version available via: https://archive.ph/X9hsU)

[29] I AM HODLING. Bitcointalk.com [online]. [cit. 2022-03-23]. Available at: https://bitcointalk.org/index.php?topic=375643.0 (archived version available via: https://archive.ph/M3adv)

[30] *Id.*

Additionally, various websites are recommending investment opportunities for different projects.[31] Google search for: "Which cryptocurrency to buy" returns shy of two billion results.[32] However, Google search for: "Which is the best cryptocurrency for transactions" returns only about thirty million results.[33] YouTube is literally full of "crypto investment videos" of questionable quality.[34] To conclude, from the author's experience and from the available internet sources it seems that the dominant mood between the people using Bitcoin (or different digital assets) is the intention to invest.

The limited supply of bitcoins and its raising price already suggest that people do actually invest fiat money into bitcoins without the intention to spend the bitcoin. However, we found a number of articles that provide scientific data on bitcoin use. The first and youngest of those articles is called: "Bitcoin Asset or Currency? Revealing User's Hidden Intention" and is from the year 2014.[35] To assess what is the predominant use of Bitcoin, the authors have chosen a following methodology. First, they selected data sources that aggregate two different types of bitcoin

[31] To show just a few randomly chosen: EBIEFUNG, Will. 2 Top Cryptocurrencies to Buy and Hold for Decades. The Motley Fool: Fool.com [online]. 2022 [cit. 2022-03-23]. Available at: https://www.fool.com/investing/2022/03/22/2-top-cryptocurrencies-to-buy-and-hold-for-decades/ (Archived version available via: https://archive.ph/99rPt), TRETINA, Kat a John SCHMIDT. Top 10 Cryptocurrencies In March 2022. Forbes.com [online]. 2022, March, 2022 [cit. 2022-03-23]. Available at: https://www.forbes.com/advisor/investing/top-10-cryptocurrencies/ (Archived version available via: https://archive.ph/s6EQx).

[32] Google.com [online]. [cit. 2022-03-23]. Available at: https://www.google.com/search?client=safari&rls=en&q=what+cryptocurrency+to+buy&ie=UTF-8&oe=UTF-8 (archived version available via: https://archive.ph/13lR5) – as a side note, the tool we are using for to archive the links, is unable to process all of Google's links and therefore shows a lesser number.

[33] Google.com [online]. [cit. 2022-03-23]. Available at: https://www.google.com/search?client=safari&rls=en&q=which+cryptocurrency+is+best+for+transactions&ie=UTF-8&oe=UTF-8 (archived version available via: https://archive.ph/L9S1F)

[34] To show just a few randomly chosen: 5 CHEAPEST Altcoins to Make You RICH (Under a Penny). Youtube.com [online]. 2021, 2021 [cit. 2022-03-23]. Available at: https://www.youtube.com/watch?v=12LB1SpQMMo (archived version available via: https://archive.ph/nbxHd) or How I Would Invest $1,000 in Cryptocurrency in 2022? | CryptosRUs. Youtube.com [online]. 2022 [cit. 2022-03-23]. Available at: https://www.youtube.com/watch?v=hOxH-YL_exY (archived version available via: https://archive.ph/a6OqS).

[35] GLASER, Florian, Kai ZIMMERMANN, Martin HAFERKORN, Moritz Christian WEBER a Michael SIERING. BITCOIN - ASSET OR CURRENCY? REVEALING USERS' HIDDEN INTENTIONS. Twenty Second European Conference on Information Systems [online]. Tel Aviv, 2014(1), 1-14 [cit. 2022-03-25]. Available at: https://deliverypdf.ssrn.com/delivery.php?ID=659113087090031100005100106064073095007085007037003090100005002104097066091124070102026056048010010036110094097024089084113002104006091005020071011089029112066078004004007050007012107029066112103028115002088072021012070127009103007118080019082002026081&EXT=pdf&INDEX=TRUE (Archived version available at: https://archive.ph/yI0qW)

transactions. Those data sources then provide two different data sets.[36] First data sets reveal the changes in bitcoin's price by tracking the aggregate trades on centralized points – so called crypto exchanges.[37] The second data set is then monitors the transactions within the Bitcoin network itself to determine the network's volume.[38]

If Bitcoin's users want to use Bitcoin as an alternative payment system, the first data set should show an increase in volume. The value and number of bitcoins traded on the exchanges should rise, as users transfer their fiat money into the Bitcoin network. Further, such users should also increase the transaction volume monitored by the second data set as, because after they have purchased bitcoin, they should be sending them to a different party in order to settle an obligation (purchase services or goods).If Bitcoin's users want to use Bitcoin as an alternative investment medium, then the second data set should not show any increase in volume, as most of the people leaves their bitcoin in the exchange itself. Therefore, if Bitcoin is used as a currency both of the data set should increase, if Bitcoin is however used as an asset, then only the first data set should show increase.

The research reveals that while Bitcoin users raise the transaction volume on exchanges and correspondingly the bitcoin price.[39] There is not corresponding rise in the volume of the transactions within the Bitcoin network itself.[40] Thus, in words of the authors: "One interpretation of the results is that exchange users buying [b]itcoin for the first time are likely to keep these [b]itcoins in their exchange wallet for speculation purposes and do not have the intention to use these acquired [b]itcoins for paying goods or services."[41]

[36] Ibid. at 7.
[37] Ibid. Crypto Exchanges are web-based services that allow the exchange of fiat money into digital assets as well as exchange of digital assets for different digital assets. We provider further explanation in part 5.
[38] Ibid.
[39] Ibid. at 13.
[40] Ibid.
[41] Ibid.

Authors of a different study have reached similar results, while using different methods.[42] In this article, the authors have not only researched Bitcoin's transactions data, but also analyzed Bitcoin wallets[43] and subsequently created a typology of Bitcoin users. The typology was derived based on user's activity. Authors, among others, differentiate between users who only or mostly accumulate bitcoin and call such users investors.[44] The group called investors is further divided based on the number of bitcoins they hold and send into active and passive investors. Users who send small amounts of bitcoin are then called currency users.[45] Users who both hold larger amounts of bitcoins and send small transactions are referred to as the hybrid users.[46]Those groups were monitored for three years.[47] The research have shown that largest group of users, about 75%, fit between the hybrid users and passive investors definition.[48] Further, the currency users group proportion has fallen from 5.1% in 2011 to 2.5% in 2013.[49] Based on those results the authors conclude: […] that there are very few users that use Bitcoin purely as a medium of exchange and a dominant group of users that use Bitcoin for investment.[50]

Based on the analysis above we conclude that Bitcoin is not money. Not only it does not satisfy the basic monetary functions, nor its users are intending to use it as money.

[42] BAUR, Dirk, KiHoon HONG a Adrian LEE. Bitcoin: Medium of exchange or speculative assets? Journal of International Financial Markets, Institutions and Money [online]. May, 2018, 54, 177-189 [cit. 2022-03-25]. Available at: https://www.sciencedirect.com/science/article/pii/S1042443117300720?ref=cra_js_challenge&fr=rjs doi: https://doi.org/10.1016/j.intfin.2017.12.004, (archived version available via: https://archive.ph/0rk3E)

[43] For the purpose of this part, please think of Bitcoin wallet as a bank account. The information you can obtain about this bank account are semi anonymous. You can see the incoming and outgoing transactions, as well as the number of bitcoins kept in such wallet, however you cannot see who the owner is. The owner is only represented by symbols.

[44] BAUR at all., Ibid 42 at 184.

[45] Ibid

[46] Ibid

[47] Ibid.

[48] Ibid. at 185.

[49] Ibid.

[50] Ibid. at 185.

2.2.4. On the issue of currency

First, as we argued above, currency is rather formal term, the explanation of difference between money and currency can be found in legal theory as well as in various legislations. A well written, synthetical explanation, provides Czech primer on the theory of financial law: "What makes money a currency, however, is not only a higher degree of concreteness, the fact that an object is considered money, but above all it is a certain authority that stands behind the concreteness of the respective form of money, defines the form of money as currency in a qualified way and sets the conditions for its existence and use. This authority is usually the State, which determines the currency and its particulars for its territory as part of the exercise of sovereignty over that territory."[51]

In the same source we can find a good definition of currency itself: a particular system of money established in a particular state and systematically regulated by the legal system of that state. Alternatively, a currency can be defined as a type of money that is recognized by a sovereign authority (a state, an international organization, a community of states, a group effectively exercising control over a particular territory) and is backed or enforced by that authority and also accepted in payments to that authority.[52]

To completement the theoretical explanation a fitting legal definition (including also foreign currencies) can be borrowed from the U.S. 31 CFR § 1010.100(m), which defines currency as: "the coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a

[51] From the Czech original: Co však činí peníze měnou, není jen vyšší míra konkrétnosti, skutečnost, že nějaký předmět je za peníze považován, ale především je to určitá autorita, která za konkretizací příslušné formy peněz stojí, kvalifikovaným způsobem formu peněz jakožto měnu definuje a stanoví podmínky její existence a používání. Touto autoritou je zpravidla stát, který pro své území určuje měnu a její náležitosti jako součást výkonu svrchovanosti nad tímto územím. Translation of the author. Bakeš, M., Karfíková, M., Kotáb, P., Marková, H. et al. Financial Law. 6th revised edition. Prague: C. H. Beck, 2012, 549 p. at 335.

[52] Ibid. at 186. from the Czech original, authors translation: "konkrétní soustava peněz zavedená v určitém státě a systematicky upravená právním řádem tohoto státu. Alternativně lze měnu definovat jako druh peněz, který je uznáván určitou suverénní autoritou (stát, mezinárodní organizace, společenství států, skupina fakticky vykonávající kontrolu nad určitým územím) a touto autoritou zaštítěn nebo prosazován a rovněž i při platbách této autoritě akceptován."

medium of exchange in the country of issuance."[53] Since none of the countries recognizes Bitcoin as a legal tender and it can hardly satisfy the current definition of money, we conclude that Bitcoin is not a currency.[54]

2.2.5. On the issue of assets

To provide a closure to the above analysis we shall look into the meaning of assets as well. An economic definition of asset might be: "a resource with economic value that an individual, corporation, or country owns or controls with the expectation that it will provide a future benefit."[55] Black's Law Dictionary then defines asset as a "Property of all kinds, real and personal, tangible and intangible, including, inter alia, for certain purposes, patents and causes of action which belong to any person including a corporation and the estate of a decedent."[56]

As the reader can see, asset is very general term. Such term can be used for description of anything that can be owned or controlled and has some value. We are of the opinion that such notion is fitting description of Bitcoin. Further it can serve as an umbrella term for all the different types of similar technological projects.

[53] The Code of Federal Regulation, title 31 is available via: https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010/subpart-A/section-1010.100 (archived version available via: https://archive.ph/pppFR)

[54] Here, we are faced with an issue. When we first wrote this chapter, it was easy to conclude that since none of the Countries issues or recognizes Bitcoin as a legal tender, Bitcoin is not a currency. The reasoning for this conclusion was turned upside down on September 7, 2021. When El Salvador has made Bitcoin its official national currency. Given that El Salvador, while a sovereign country, is not an important financial player, we will leave the impacts of such decision on future researchers, and for the purposes of this Thesis we will remain looking at Bitcoin as something else than currency.

[55] Asset Definition. Investopedia.com [online]. 2022 [cit. 2022-03-27]. Available at: https://www.investopedia.com/terms/a/asset.asp (Archived version available via: https://archive.ph/wjgpA)

[56] BLACK, HENRY, JOSEPH NOLAN a JACQUELINE NOLAN-HALEY at all. Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern. 2nd Reprint. United States of America: WEST PUBLISHING CO., 1990, 1-150. ISBN 0-314-77165-4. Available at: https://thelawdictionary.org/asset-2/ (Archived version available via: https://archive.ph/1iOrm)

2.2.6. Conclusion

In this introductory chapter we analyze the most widely used terms used to described Bitcoin. We identify three essential collocations. Virtual Currency, Digital Currency, and Cryptocurrency. While the first two are interchangeably used in scientific and academic article, the term Cryptocurrency is used by developers and in general talk.

We briefly address the adjectives, and argue that out of the given options, the adjective Digital seems as the best fit. After eliminating the adjective “Cryptographic” do due its connection with colloquial talk rather than academic sphere. While we find virtual less problematic than cryptographic, its true meaning seems to encompass sort of illusion, which exists only within artificial boundaries outside of the real world.

Subsequently, we are addressing the issue of currency. We divide this issue into three sub issues. Focusing on the aspects of money, currency, and assets. The term currency seems unsuitable because Bitcoin does not fulfil the three basic functions of money. Neither we can accept the fact that Bitcoin is a currency in the legal sense, despite the fact El Salvador decided to install Bitcoin as its forced legal tender.

We thus argue for the usage of the term asset. Asset is a very general term, which meaning might have a better use, as an umbrella term for Bitcoin and similar projects. Combining our findings in this chapter, we decided to use the collocation Digital Asset (digital assets respectively) to talk about Bitcoin and similar projects.

Further, we establish that Digital Assets are predominantly used in different capacity than in its payment capabilities. This fact we address more thoroughly throughout the Thesis itself.

3. Historical Aspects

3.1. Introduction and how to approach this chapter

To a person who is not familiar with the technology behind Bitcoin, its sudden introduction in 2008 (2009) may seem like a radical breakthrough invention. However, as we will show in the following pages, it was rather gradient process, which terminated with the creation of the first Blockchain, which we then describe in separate chapter.

The first Blockchain developed by the mysterious developer Satoshi Nakamoto combined existing technology originating in various projects. Some of those projects had nothing to do with Digital Assets and were simply trying to resolve issue of this own, such as fighting the internet spam. However, other of those projects had striven for similar goals as Satoshi with his Bitcoin. Interestingly, most of the authors of such projects belonged to one ideological group having similar libertarian ideals as Satoshi[57]. This group named itself Cypherpunks and we address it partially throughout this chapter.

Nakamoto posted the Bitcoin's whitepaper with the following introduction: "*What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.*"[58] In other words, authors of such projects aimed to create private electronic payment system without direct governmental oversight. In this chapter we are going to follow a few of such examples. Including E-Gold, eCash, B-Money, and Bit Gold[59] all of which could be considered ancestors to Bitcoin in a way.

[57] And if they did not belong to Cypherpunks, they have at least shared the same libertarian views and general dissatisfaction with then existing financial system.

[58] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. October 31, 2008, s. 1-9 [cit. 2022-03-29]. Available at: https://bitcoin.org/bitcoin.pdf (Archived version available via: https://archive.ph/b7ICx)

[59] There were other attempts to develop private payment systems. Other influential project, which would qualify was Adam Black's Hashcash. Hashcash also used Proof-of-Work to create new monetary units and was generally similar to current Digital Assets. Since Hashcash was also similar to B-Money and Bit-Gold we decided to use the latter two. For more information on Hashcash please see: BLACK, Adam. Hashcash - A Denial of Service Counter-Measure [online]. September 2002, 1-10 [cit. 2022-04-11]. Available at:

On the following pages we thus considering our first posed question – Can the history of Digital Assets help us with its understanding and regulatory approach? This chapter should therefore facilitate not only the historical and technological transition into the blockchain technology. But it should also help us to highlight certain specifics associated with the believes of its authors and specifics associated with the decentralized character of Digital Assets. Since none of the above-mentioned projects is functional for one reason or another, we will also use this space to highlight some of its faults.

On this note, one of the flaws prone to any of Digital Assets is its susceptibility to so called Double Spending Issue. This issue is very important and since the projects we are going to mention below were, among others, trying to resolve this issue, we decided to dedicate a separate introduction to the Double Spending Issue.[60]

3.2. The double spending issue and trusted third party

Double-spending issue is defined as "*a potential flaw in a [Digital Asset] or other digital cash scheme whereby the same single digital token can be spent more than once, and this is possible because a digital token [monetary unit] consists of a digital file that can be duplicated or falsified.*"[61] Double spending is a major issue, thus, it is no coincidence that Nakamoto's Bitcoin white paper starts with the statement: "*We propose a solution to the double-spending problem using a peer-to-peer network.*"[62] As the solution to double-spending problem was what made Bitcoin relevant.

---

https://www.researchgate.net/publication/2482110_Hashcash_-_A_Denial_of_Service_Counter-Measure (Archived version available via: https://archive.ph/h09S9)

[60] In this sense it is important to note that what makes Blockchain, and the Bitcoin invention stand out of the projects, which description follows is its ability to resolve the double spending issue theoretically and also encompass it into a computer code.

[61] CHOHAN, Usman. The Double Spending Problem and Cryptocurrencies. Discussion Paper Series: Notes on the 21st Century [online]. Critical Blockchain Research Initiative, 2017, 6th January, 2021, 1-10 [cit. 2022-03-12]. Available at: https://deliverypdf.ssrn.com/delivery.php?ID=107064121121024002092084007007102002098014089077064041076068086098122007091113120094058057003006039016043112010113119092097096106078031069085002081098107071122124113073040045013124085090098076004023107068089103106094022006021096116030101103098116111074&EXT=pdf&INDEX=TRUE (archived version available via: https://archive.ph/QkmxM)

[62] NAKAMOTO, Ibid. 58, at 1

3.2.1. Example explaining the double spending issue

To show the significance of the above-mentioned solution, please see the following (simplified) example:

Imagine a person A who wants to transfer fiat money to a person B and also a person C. Person A has $ 2000 in her bank account. In the first transaction, she decides to send $ 1500 to the person B. Subsequently, she decides to send another $ 1000 to the person C. When Person A initiates the first transaction the affiliated bank will verify, among others, whether Person A is able to dispose of $ 1500. Once the bank confirms she indeed can transfer such amount, the bank will carry out such transaction. Person B shall receive the money.

Subsequently, when Person A initiates the second transaction, the bank will again carry out the previous steps (the verification), only to establish that Person A does not have sufficient monetary funds in her account to conduct such transaction. The bank will, therefore, decline to credit Person's B account.

The bank in these transactions serves the role of a trusted third party or in other words the bank acts as an intermediary. Since Person C is unable to verify herself, whether person A has the right to dispose of $ 1000, she must trust the bank to conduct the verification on behalf of her. Both person B and C, are therefore, required to trust the bank to conduct the transactions.

3.2.2. Further explanation

In majority of the cases, the trusted third party is motivated to act lawfully. However, as the trusted third party is an entity with ability to act independently, there will always be a certain level of risk involved. Trusted third party may simply abuse its power for her own benefit. Intermediary in any transaction is therefore a potential problem. On the other hand, without trusted third party Person A would be able to conduct transaction to Person C, even if she would not dispose of the total amount of money, she promised to transfer. In other words, Person A could try to double spend her funds.

In the not-so-distant past, any digital payment system was therefore faced with a problem. Implement a trusted third party – have risk factor involved. Do not implement a trusted third party – have a double spending factor involved. Of course, with any digital files there are other issues such as the possibility to create an unlimited number of copies of such files, which makes the case for existence of Intermediary overseeing such issues even more compelling.

The ideal solution would be to solve double spending problem, without having a trusted third party, which is a risk factor. In this chapter, we therefore also follow how the technological development, which allowed to dispose of trusted third party, while also eliminating the double spending issue (to some extent).

3.3. The case of E-gold ltd., and the need for decentralization

3.3.1. Introduction to E-Gold ltd.

As a first example we chose project called E-gold Ltd. This project was launched in 1996 by a Florida oncologist Dr. Douglas Jackson and attorney Barry Downey[63]. Around the same time similar projects, such as Liberty Dollar, were introduced. Liberty Dollar could have served as an example as well. Except, E-gold was designed exclusively for the use over the Internet and so have established it as better fit for the historical development.

In addition to its online character, we decided to start with E-gold for one other reason. As described below, E-gold services were finally terminated by a court order. During the proceedings the lawyers for E-gold have raised a few compelling arguments, which would still be valid even in case of current Digital Assets, had it not been denied. In fact, Financial Crimes Enforcement Network (known also as "FinCEN") still relies on some of the given reasoning.[64]

[63] WHITE, Lawrence. The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-Gold. Cato Journal [online]. Washington DC, USA, 2014, 2014(34), 281-301 [cit. 2021-12-21]. Available at: https://ciaotest.cc.columbia.edu/journals/cato/v34i2/f_0031473_25521.pdf (archived version available via: https://archive.fo/FWaBK)

[64] LEE KUO CHEUM, David. Handbook of Digital Currency. Elsevier Books, 2015, 612 p, at 168 p., ISBN 0128021179.

As such, we also bring a short summary of the proceeding including said argument. The outcome of the court's proceeding also shows, why it was so important for the success of the current Digital Assets to dispose of the trusted third party.

Further, from the available resources, both Bitcoin and E-Gold seems to have had similar motivation. This motivation was partially economical and partially political. For the economic part Dr. Jackson seemed to have distrusted the fractional reserve banking and was concerned about inflation.[65]

3.3.2. E-Gold payment systems and its functionality

E-Gold was a gold backed payment system hosted on the web page www.e-gold.com. E-gold allowed for transfer of user held accounts, which contained certain number of units. However, did not allow for the transfers of the individual units. Each unit was backed 1:1 by precious metals, the dominant of which was gold. The gold itself was held in vault in London administrated by a trust fund[66]. At the peak of its existence, the E-gold payment system grew to a respectable size of $2.0 billion USD worth of annual transactions.[67]

E-Gold relied on centralized structure. From the customers point of view the trusted third party was the E-gold Ltd. company.[68] It was reviewing the transactions, checking whether the accounts were not double spent etc.

A timely description of the use and functioning of E-gold was provided in Bloomberg Businessweek in 2006: "*E-gold is a "digital currency." Opening an account at www.e-gold.com takes only a few clicks of a mouse. Customers can use a false name if they like because no one checks. With a credit card or wire transfer, a user buys units of e-gold. Those units can then be transferred with a few more clicks to anyone else with an e-gold account.*

[65] WHITE, Ibid. at 63, at 289
[66] Ibid.
[67] Ibid.
[68] Ibid.

For the recipient, cashing out -- changing e-gold back to regular money -- is just as convenient and often just as anonymous.[69]

As E-gold became widely known, the United States government started to take interest. Mainly because its benevolent approach to security, know your customer, and frankly all anti-money laundering measures, which were tightened at that time following the 9/11 incident.

Even if Dr. Jackson argued that "*e-gold operates legally and does not condone persons attempting to use e-gold for criminal activity*"[70] and further that: "e-*gold has a long history of cooperation with law enforcement agencies in the US and worldwide, providing data and investigative assistance in response to lawful requests.*"[71] The company soon became subject of criminal proceeding.

3.3.3. The E-Gold court proceedings

3.3.3.1. Legal basis

The above-mentioned benevolence was later the bane of E-gold's existence, as it was cut short following the indictment, among others, for the operation of unlicensed money transmitting business in violation of 18 U.S.C. § 1960.[72] Title 18 of the United States Code is a federal law that regulates crimes and the corresponding criminal procedure. Specifically, 18 U.S.C. § 1960 makes it a crime to operate an unlicensed money transmitting business.[73] Anyone who "*knowingly*

[69] Grow, B.; Cady J.; Rutledge, S.; and Polek, D. (2006) "Gold Rush." Business Week (8 January). Available at www.businessweek.com/stories/2006-01-08/gold-rush (archived version available via: https://archive.fo/Ffp3K#selection-3219.0-3219.461)

[70] E-Gold [online]. [cit. 2022-03-29]. Available at: https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/Bitcoins/e-gold.html (Archived version available via: https://archive.ph/b8abu)

[71] Ibid.

[72] United States v. E-Gold, Ltd., 521 F.3d 411, 412 (D.C.Cir. 2008), available at: https://scholar.google.com/scholar_case?case=8874345388360794335&q=UNITED+STATES+of+America,+Appellee+v.+E-GOLD,+LTD.,+et+al.,+Appellants&hl=en&as_sdt=2006 (archived version available via: https://archive.fo/ppzmZ)

[73] US v. E-Gold, Ltd., 550 F. Supp. 2d 82 - Dist. Court, Dist. of Columbia 2008, available at: https://scholar.google.com/scholar_case?case=11718339043645598961&q=US+v+E+gold&hl=en&as_sdt=2006 (Archived version available via: https://archive.ph/4Itef)

conducts, controls, manages, supervises, directs or owns all or part of an unlicensed money transmitting business."[74] It also provides that:

As used in this section —

(1) the term "unlicensed money transmitting business" means a money transmitting business which affects interstate or foreign commerce in any manner or degree and —

(A) is operated without an appropriate money transferring license in a State where said operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;

(B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or

(C) otherwise involves me transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity;

(2) the term "money transmitting" includes transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier....[75]

[74] 18 U.S.C. § 1960(a) (2008).
[75] United States v. E-Gold, Ibid. 72.

3.3.3.2. The arguments of the defense

As a defense, the lawyers of E-gold raised an argument that since the E-gold system was not transmitting cash money per se it should not be covered by the 18 U.S.C. § 1960. The legal team of E-gold further claimed that the E-gold system was transferring proof-of-ownership of gold among its customers.[76]

A quote from the defense's memorandum itself: "*By its terms, Section 1960 applies only to "money transmitting business[es].*" 18 U.S.C. § 1960.... *[I]n order to qualify as a "money transmitting business," a business must engage in cash transactions*. Because the Indictment fails to allege that either e-Gold or G & SR engages in cash transactions — and indeed specifically alleges that e-Gold merely transfers e-gold between accounts and that G & SR transacts in wires — they cannot constitute a money transmitting business, either individually or collectively. Thus, under the terms of the Indictment, the defendants could not have violated the law by operating an unlicensed money transmitting business, or by conspiring to operate an unlicensed money transmitting business."[77].

As the reader can see, the defense relied on the fact that what is being transferred (transacted) does not amount to physical cash. It is because the defense further argued with 31 U.S.C. § 5330. This section 31 U.S.C. § 5330 provides that, for purposes of that section, "*money transmitting business" means:*

any business other than the United States Postal Service which —

(A) provides check cashing, currency exchange, or money transmitting or remittance services, or issues or redeems money orders, travelers' checks, and other similar instruments or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network

[76] WHITE, Ibid. 63, at 291.
[77] US v. E-Gold, Ibid. at 73.

of people who engage as a business in facilitating the transfer of money domestically or internally outside of the conventional financial institutions system;

(B) is required to file reports under section 5313; and

(C) is not a depository institution (as defined in section 5313(g))[78]*.*

3.3.3.3. Author's opinion on the arguments

In our opinion the pinnacle of the argument was, that those conditions set forth in 31 U.S.C. § 5330 are cumulative. Meaning all of those conditions must be satisfied for E-Gold to engage in money transmitting business. Thus, E-Gold should have been required to file reports under 31 U.S.C. § 5313 to be considered a business engaged in money transmitting business. The relevant part of section 5313 provides:

(a) When a domestic financial institution is involved in a transaction for the payment, receipt, or transfer of United States coins or currency (or other monetary instruments the Secretary of the Treasury prescribes), in an amount, denomination, or amount and denomination, or under circumstances the Secretary prescribes by regulation, the institution and any other participant in the transaction the Secretary may prescribe shall file a report on the transaction at the time and in the way the Secretary prescribes. A participant acting for another person shall make the report as the agent or bailee of the person and identify the person for whom the transaction is being made.

As per this section only a person (business entity in this sense), who carries out transactions in coins or currency (cash) is required to file such reports. To provide a synthesis, the defendants essentially argue that since they were not conducting transactions in cash, they were not required to file reports pursuant to 31 U.S.C § 5313. As such, the cumulative conditions pursuant to with 31 U.S.C. § 5330 were not satisfied and thus E-Gold did not participate in money

[78] US v. E-Gold, Ibid. at 73.

transmitting business. Thus, the Defendants have argued E-Gold could not be in breach of 18 U.S.C. § 1960, in other words to commit the crime to operate an unlicensed money transmitting business.

3.3.3.4. Court's decision

Needless to say, the Court did not agree with defenses argument. The rationale of the Court was that sections 31. U.S.C. § 5330 and 18 U.S.C. § 1960 are not mutually dependent. The Court argued that the meaning of 18 U.S.C. § 1960 is not derived from 31. U.S.C. § 5330 and thus the definition contained in section 5330 is not relevant. Specifically, the Court argued that line of text reading "unlicensed money transmitting business" should be read as a plain text rather than looked upon as a phrase including specific terminology concerning a specific (money transmitting) business. Court further argued that 18 U.S.C. § 1960 includes the word "funds" as opposed to cash only, as argued by defendants. Defense's argument regarding section's 5330 cash dependency was therefore denied. While the Court's reasoning is rather complex, including case law on how to interpret plain language, it can be summarized with following Court's reasoning: "The answer is no — for two reasons: (1) Section 1960 does not borrow the definition of "money transmitting business" from Section 5330, and (2) Section 5330's definition of "money transmitting business" is not limited to cash transactions, but rather includes transmissions of funds by any means."[79] Additionally the Court explained that: The definition of "money transmitting business," as defined in Section 5330(d)(1), […], only applies to Section 5330, and not to Section 1960.

The core of the defendant's argument, the requirement to file reports, was also addressed by the Court: This argument misses the mark: Sections 5330 and 5313 apply to them [E-Gold] right now, if, as alleged, e-Gold and GS & R are engaged in money transmission. Section 5313 imposes no present, affirmative duty on either business, according to their descriptions, but it applies to them at all times, and in the eventuality that they ever are involved in a transaction in excess of a prescribed amount of currency, they will be required

[79] US v. E-Gold, Ibid. at 73.at 89.

to file a currency transaction report ("CTR") under Section 5313.[80] Following the Court's reasoning above, Dr. Jackson (and others) pleaded guilty to conspiracy to engage in money laundering and operating an unlicensed money transmitting business.[81]

3.3.4. Conclusion to the E-Gold project

In conclusion, E-Gold was a private online payment system which allowed for transfer of accounts holding units tied to precious metals. The payment system was centralized, which means there was a central authority who served as a trusted third party. As this payment system was centralized, it was easily susceptible to authorities due to the existence of an entity, which could be prosecuted. Additionally, E-Gold payment system operator was rather liberal with satisfying the relevant regulation and allowed its users to use it without their proper identification. E-Gold was subsequently sued among others for unlicensed money transmitting business. Attorneys for the defendants (E-Gold and others) argued that since the payment system does not operate with cash it was not required to satisfy the regulative obligations concerning money transmitting business. This argument was refused by the court and E-gold was forced to terminate its services.

This example shown that successful private medium of exchange attracts criminal activity and regulatory response. Anyone who would be interested in making a successful private payment system using its own medium of exchange would have to resolve the issue of liability making the system decentralized and the issue of privacy making such system anonymous.

[80] US v. E-Gold, Ibid. at 73. at 94 -95.

[81] United States Secret Service: In U.S. Secret Service-Led Investigation, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges. Secretservice.gov [online]. USA: U.S. Secret Service Media Relations, 2008 [cit. 2021-12-22]. Available at: https://www.secretservice.gov/press/releases/2008/07/us-secret-service-led-investigation-digital-currency-business-e-gold-pleads (archived version available via: https://archive.fo/Ga6pw)

3.3.5. What do we infer from the E-Gold payment system case?

To anyone (in example the creator of the Digital Asset Bitcoin) who was familiar with the case of E-gold and wanted to create a private payment system must have been apparent one thing. Government is not fond of developers creating private money.

In the end a functioning private currency could be a potential systemic risk for the financial system.[82] Further, if the project is technically working it will likely attract criminal activity, which will intensify the regulative pressure, unless it will be outright banned. Therefore, to create such system, the system should be decentralized. Should there be no central authority and no creator, who would remain to be responsible for the creation or for the abuse of such system? A smart developer of such system would likely decide to remain anonymous as if the system would be working the associated liability would definitely be great.

Nevertheless, the liability of the creator is just a tip of the iceberg. The users of such system would likely be also liable. Thus, another necessary part of private payment systems would be anonymity. Just for the sake of protection, it would be convenient if the users and their data remain anonymous as well. Any future private payment systems thus needed a general cloak of privacy.

Of course, the main problems to solve still remains - among others, the combination of double spending issue and trusted third party. Yet, one thing was sure centralized structure is deemed to fail. The successful system therefore would ideally be anonymous, decentralized, and trustless. Luckily, there are other private payment systems, which developers were concerned with privacy and anonymity, to learn from.

[82] As the company Meta Inc., who is behind major social networks found out. The financial regulators are not fond of projects that have actual chance of success as was Meta's Libra, which was then rebranded as Diem. The project was faced with response of both regulators from the US and EU, voicing concerns among others over Privacy and Antitrust issues. The project was supposed to be a Digital Asset facilitating payments among the numerous users of Meta's social network. The project itself was abandoned at the beginning of 2022.

3.4. The case of DigiCash's eCash

3.4.1. Introduction

Even before E-gold, ltd. came into existence, cryptographer Dr. David Chaum from University of California, Berkley founded a company called DigiCash.[83] Similar to Dr. Douglas Jackson Dr. Chaum had concerns about existing payment systems. While the authors of E-gold seem to have had concerns about the fractional reserve banking system and inflation, Dr. Chaum's work was more oriented towards internet privacy. Dr. Chaum alleged that: "*[…] knowledge by a third-party of the payee, amount, and time for every transaction made by an individua l can reveal great deal about individual's whereabout, associations and lifestyle.*"[84] Dr. Chaum therefore decided to develop his own cash-like electronic payment system. Introducing eCash an online payment method, which mimicked the attributes of cash, while adding certain characteristics natural to electronic money transfers such as proof of payment.

DigiCash was responsible for digital cash payment system called eCash, which was based on Dr. Chaum's 1983 paper describing blind signatures for untraceable payments technology. In this paper Dr. Chaum proposed idea for a better and anonymous electronic payment system at the dawn of e-commerce.[85]

At first Dr. Chaum states the issues associated with then current electronic payment systems. According to his paper a modern electronic payment system should find the balance between personal privacy and the safety from criminal abuse of electronic payments.[86] He argues that an electronic payment system should hold both the positives of cash and the positives of electronic payment systems while eliminating the negatives of both. He further points

[83] PITTA, Julie. Requiem for a Bright Idea. Forbes.com [online]. Nov 1, 1999 [cit. 2022-01-02]. Available at: https://www.forbes.com/forbes/1999/1101/6411390a.html (archived version available via: https://archive.fo/FZD4Y)

[84] CHAUM, David. Blind Signatures for Untraceable Payments [online]. Santa Barbara, CA, 1983 [cit. 2022-01-02]. Available at: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF. University of California. (Archived version available via: https://archive.ph/QPK9u)

[85] Ibid. at 199

[86] Ibid.

out that any trusted third-party in electronic payment (in example a bank) systems who knows the time, amount, and the type of goods or service purchased by an individual obtains a great deal of information about such individual, however banknotes and coins, which provide for anonymous payment, suffer from lack of control and security.[87]

3.4.2. The functioning of eCash payment system

The actual functioning of the payment system should be interesting to the readers, because it bears some similarities with Bitcoin design. Given of course the fact that eCash was dependent on the central authority, which was verifying whether the digital medium of exchange was not used more than once. The eCash payment system was centralized and fully integrated into the existing financial system. In fact, to conduct a payment transaction both the payer and payee had to share a common bank.[88] At first eCash relied on cooperation with Mark Twain Bank[89]. Later, more banks have joined eCash and supported the system[90].

The eCash payment system did not create its own medium of exchange per se. Rather it relied on cooperation with a bank. The bank then allowed its customers to essentially issue the money themselves. At first client of such bank would choose couple of random and unique numbers herself.[91] Second such client would scramble the numbers (encrypt them) and send them to the bank for validation.[92]

---

[87] Ibid.

[88] ABRAR, Waleed. Untraceable Electronic Cash with Digicash [online]. University of Konstanz, 2014, 1-3 [cit. 2022-01-02]. Available at: https://www.researchgate.net/profile/Waleed-Abrar/publication/277598468_Network_and_communication_Privacy_Digi_cash/links/556e5fc008aeab777226a488/Network-and-communication-Privacy-Digi-cash.pdf (archived version available via: https://archive.ph/IfZLj)

[89] Digicash to Test Live Internet Cash System with Mark Twain. American Banker [online]. USA, October 23, 1995 [cit. 2022-01-02]. Available at: https://www.americanbanker.com/news/digicash-to-test-live-internet-cash-system-with-mark-twain (archived version available via: https://archive.ph/FEv0v).

[90] CHAUM, David. DigiCash. Chaum.com [online]. [cit. 2022-04-14]. Available at: https://www.chaum.com/ecash/ (archived version available via: https://archive.ph/iuZyq)

[91] CHAUM, Ibid. 84, at 202

[92] Ibid.

The creation of money itself was based on the concept of blind signatures, which is a subset of typical digital signatures as explained below. Compared to the normal digital signature concept, the blind signature scheme makes it possible for a third-party to do the signing (validation), without knowing what information is signed.[93] In short it means that a person, business entity, or an institution can confirm the origin of information (a payment is coming from a certain person) without being able to read the information itself (the details of the payment such as its amount).

Rather comprehendible explanation of the technology is described by the author himself[94]. Dr. Chaum compares blind signatures to a set of special envelopes holding a secret information inside. In his case the envelope holds a person's voting preference. Imagine a person inserts a slip of paper containing a secret information in a carbon lined envelope. To help our readers with imagination, a carbon lined envelope has its insides covered with carbon. Subsequently, puts the carbon lined envelope into another normal envelope with her return address on top, seals it, and sends it to the desired trustee (third-party). The third party will verify whether the return address corresponds with a person who satisfies all the desired requirements (eligible voter) and if yes, opens the outer envelope, takes out the carbon lined envelope and signs it. Thanks to the carbon lining inside the envelope the signature gets copied on the slip inside and the slip of paper becomes ascertained by a signature, without the third-party knowing the voting preference of the person. The signed ballot can be then delivered where needed.

In a less imaginative way the transactions (signatures) were facilitated via basic cryptography based on trap door function (one way function)[95]. This type of cryptography is called asymmetric cryptography or public key cryptography and relies on two correlated numbers, which are usually

[93] FRIIS BO, Jens. Digicash implementation [online]. University of Aarhus, 1-21 [cit. 2022-01-02]. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.197.7531&rep=rep1&type=pdf (archived version available via: https://archive.ph/2cHeg)

[94] CHAUM, Ibid. 84, at 200

[95] A trap door function is a something like one way street, the function is easily computable from one way, but nearly impossible to reverse. In example to multiply two large prime numbers is easy, however figuring out the correct prime numbers from the product is very hard and as of the time of writing this Thesis can done only by trial and error approach.

referred to as keys, a public key (encryption key) and a private key (decryption key).[96] A public key is not secret and may be shared with public, however the private key shall remain undisclosed to anyone but its owner[97]. Further the number representing a private key is generated randomly, whereas the number representing public key is derived from the corresponding private key.[98] While it is easy to derive public key from private key, its merely impossible[99] to derive private key from public key.

While this type of cryptography can be used to hold a secret conversation. With participants simply sharing their public keys to encrypt a message and decrypt it with corresponding private key. It may be also used for a financial transaction as basically any string of data can be digitally signed. To do so, a private key need to be combined with a given string of data. Once combined the result will be a random string of characters (digital signature), which however relates to the corresponding public key. Therefore, the validity of digital signature (transaction) can be verified against corresponding public key, which is safely sharable. The now signed (encrypted) string of data can be once again "opened" with the corresponding private key.

What Dr. David Chaum added to this already existing technology was addition layer of anonymity. Essentially, before sending a message (initiating transaction) Dr. Chaum's invention allowed to digitally sign not only encrypted content, but also the underlining original message through the encryption. As such the validator would receive a message its contents it would not understand, but once such message was decrypted, the validator would still be able to verify that she had signed it.

[96] MENEZES, A., van OORSCHOT, P. and VANSTONE S., Handbook of Applied Cryptography. Handbook of applied cryptography [online]. Boca Raton: CRC, 1997, s. 1-780 [cit. 2022-01-04]. CRC Press series on discrete mathematics and its applications. ISBN 0-8493-8523-7. Available at: https://cacr.uwaterloo.ca/hac/about/chap1.pdf (archived version available via: https://archive.fo/AR1Rm)
[97] ibid at 27.
[98] Ibid. at 26.
[99] With the current (2021) known and readily available technology, it is practically impossible. In 2022, still impossible.

3.4.2.1. Illustration of transactions in the eCash payment system

Just as an interesting addition below we show the eCash transaction in steps. Please assume that person (hereinafter referred to as the "P") has a valid bearer account at bank (hereinafter referred to as the "B") and so does a shop (hereinafter referred to as the "S").

1. P creates a random number of messages, where every message contains a possible transaction;
2. P further encrypts all those messages so the content of them is secret;
3. P sends all those messages to B;
4. B randomly choses one of those messages and digitally blind sings it;
5. B sends the message back to P;
6. P partially decrypts the message, therefore its content is not a secret anymore;
7. P sends the partially decrypted message to S;
8. S accepts the message and sends it to B;
9. B validates the message from S, which means that B simply checks whether she signed it in the first place;
10. B confirms to S that the message was valid;
11. B further validates, whether the message has not been already spent to prevent the double spending;
12. B deposits corresponding amount to S; and
13. S sends the service or goods to P.

The bank knows that it verified the message (transaction). Once it receives the message again it will see the transaction was verified by the bank, therefore the initiator had the necessary funds to conduct such transaction. However, the bank should not be able to tie the amount to the corresponding sender, because it comes decrypted. The bank has never seen such message decrypted. The bank has only seen the message encrypted. Further, now the transaction comes from different person – the shop. Yet, the bank know that it is a valid transaction because

it validated it itself. Also, it is important to note, that the more participants use this system the more anonymous the payments become.

Digi Cash's ECash journey came to its end by 1998 when the company filed for bankruptcy.[100] Even though in this case, the end of the project was not a fierce legal dispute, but rather poor economic decisions from the team.[101] Dr. Chaum subsequently sold of his patents and the whole project was scraped for assets.[102]

3.4.3. Conclusion

Besides the blind signature scheme, there are a couple of points to take from this chapter. First is the issue of anonymity which Dr. Chaum argued and presented a solution. Basically, all of the Digital Assets that are currently on the market offer some degree of anonymity. A common internet user would be unable to decipher, who is actually in possession of the Digital Asset address. Some Digital Assets even provide full anonymity as their selling point.

Further, this was the first private payment structure employing the public and private key structure. Public and private keys are used in Bitcoin as well. Even if, in different capacity. In the modern conception of Digital Assets Public key represents the address, where Digital Assts can be received, similarly as a bank account number. Private key then serves as the signature, which allows for the transaction to be validated.

---

[100] O'MAHONY, Donal a Hitesh TEWARI. Electronic Payment Systems. EDPACS the EDP audit, control and security newsletter [online]. January 1997, 1-36 [cit. 2022-03-30]. doi:DOI: 10.1201/1079/43233.25.11.19980501/30170.7 Available at: https://www.researchgate.net/profile/Hitesh-Tewari/publication/220693934_Electronic_Payment_Systems/links/56470d7508ae451880abcae8/Electronic-Payment-Systems.pdf (Archived version available via: https://archive.ph/NNVJj)

[101] Dr. Chaum's DigiCash had an offer for one hundred million dollars from Microsoft to integrate its payment system into the operation system Windows 95. Dr. Chaum refused because he was not satisfied with the offered amount. For more information please see: NIMFUEHR, Marcel. The Amazing Story of Cryptocurrencies Before Bitcoin. Medium.com [online]. [cit. 2022-03-30]. Available at: https://medium.com/hackernoon/the-amazing-story-of-cryptocurrencies-before-bitcoin-fe1b0e55155b (Archived version available at: https://archive.ph/Uzmrb)

[102] What was DigiCash? A super speedy walkthrough the grandfather of cryptocurrencies. Decrypt.com [online]. Feb 4, 2019 [cit. 2022-03-30]. Available at: https://decrypt.co/resources/digicash-what-is-cryptocurrency-explainer (Archived version available via: https://archive.ph/vC8gf)

It is also relevant to highlight that similar to E-gold, this project had to be fully integrated with the financial system. It would not be functional without the presence of banks. Even if it was able to "print" its own money, it still relied on typical financial institutions to verify and validate the issued digital bank notes.

Further, it was centralized with accountable party – the DigiCash company. As such the project was subject to applicable legislation. Further, it did not bring any applicable solution to the double spending problem as it did not address it. However, this project served as an inspiration for others who wanted to create a private digital payment system. David Chaum was one of the first members of a group called Cypherpunks.

3.4.4. What do we infer from the eCash payment system?

There are two main aspects, beside the provided technical innovation, we can infer from the eCash Payment System. One of them is the emphasis on anonymity and the other is a grasp on the creation of monetary units.

The independent creation of monetary units (or rather units that may be used as a medium of exchange) is used by nearly all of the current Digital Assets as it is one of its defining characters. The difference being that here the value of such unit was not determined in any way by the code and had to rely on a financial intermediary. Similarly, the concept used here did not use a limited supply of such units and rather tied it onto existing face value of a united states dollars.

The emphasis on the inner system anonymity and also the universal anonymity is an aspect that is generally applied in Digital Assets. The transactions itself do not reveal any personal information about the holder of the relevant sending address nor receiving address.

3.5. The case of B-Money

3.5.1. Introduction and the connection to Satoshi Nakamoto and Bitcoin

B-Money is a theoretical concept of a payment system designed by Chinese computer scientist Wei Dai.[103] This purely theoretical project is interesting for a wide variety of reasons. One of the interesting aspects is also the author himself and his allegiances. Wei Dai is alumnus of the University of Washington, developer of widely used Crypto++[104], and also a prominent member of underground cryptographic movement called Cypherpunks.[105]

Under the name Cypherpunks operated (some still do) a number of cryptographers, developers, mathematicians, and scientists, who shared mutual appreciation for crypto-anarchic values. Cypherpunks understood the importance of the free Internet since its beginning. They were afraid that once the Internet becomes truly worldwide, it will catch the attention of world regulators and will become over-regulated and centralized.[106] Thus losing its liberty.

Over the time, the Cypherpunks have individually formed a pallet of values, by which they decided to protect the Internet's freedom. To reflect on some of the values, we can quote from the Cypherpunks' manifesto: "*We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.*"[107]

Apart from Wei Dai and David Chaum, other members were in example Julian Assange, Hal Finney, Nick Szabo, and an unknown number of anonymous subscribers and contributors. The members of the Cyberpunk movement have communicated through email mailing list.

[103] Weidai.com: B-money. Weidai.com [online]. [cit. 2022-03-30]. Available at: http://www.weidai.com/bmoney.txt (archived version available via: https://archive.ph/9YprR)
[104] For more information, please see in example: https://en.wikipedia.org/wiki/Crypto%2B%2B
[105] Weidai.com: Cyberpunks. Weidai.com [online]. [cit. 2022-03-30]. Available at: http://www.weidai.com (archived version available via: https://archive.ph/O0luA)
[106] QURESHI, Haseeb. The Cypherpunks. Nakamoto.com [online]. Dec., 29, 2019 [cit. 2022-04-05]. Available at: https://nakamoto.com/the-cypherpunks/ (Archived version available via: https://archive.ph/Jr1dW)
[107] HUGHE, Eric. Manifesto. Activism.net [online]. 9 March 1993n. l. [cit. 2022-03-30]. Available at: https://www.activism.net/cypherpunk/manifesto.html (Archived version available via: https://archive.ph/6of6P)

Satoshi Nakamoto, the anonymous inventor, and Bitcoin developer, has also monitored the mailing list and knew of Wei Dai's work.[108] Nakamoto and Wei Dai subsequently engaged in conversation.[109]

From the above mentioned it seems that the Cypherpunks movement was convinced that the internet needs its own medium of exchange (money in the colloquial sense). However, they apparently realized that for such a medium of exchange to be truly neutral, it could not be tied in any way to the existing financial system or otherwise tied to existing fiat currencies. Tying such internet money to existing currency would sooner or later give power over it to the corresponding central bank and to some extent even to the legislators. Therefore, the medium of exchange that would live up to the ideal of Cypherpunks should be independent of the financial system.

The dependence on the financial system would be then mainly caused by reliance on existing financial subjects (financial infrastructure) with the transaction facilitation and with the creation of monetary units. Thus, should the monetary units be created in similar fashion as in eCash, the existing financial regulators would still have influence over the medium of exchange, albeit limited. Ideally then, the monetary units should be created independently without the need of reliance on existing financial establishments. The same would be true for the monetary transactions.

With similar thoughts in mind Wei Dai introduced the theoretical concept of B-Money: "*efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities.*"[110]

[108] NAKAMOTO, Ibid. at 9.
[109] Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails [online]. 2014 [cit. 2022-03-31]. Available at: https://www.gwern.net/docs/bitcoin/2008-nakamoto (Archived version available via: https://archive.ph/02G8p)
[110] DAI. Ibid. 103, at 1.

3.5.2. The theoretical concept of B-Money with aim on transactions

Below we describe the basic functionality of B-money as proposed by Wei Dai. Since this payment system was designed not to be dependent on the classic financial systems, it addresses primarily two main areas. The creation of money (medium of exchange) itself and transmission of monetary units, the transactions.

We are going to address the functioning of the transactions first. Wei Dai proposed to different protocols. In first, the system required that each participant in such system maintains a separate database.[111] In order to evidence, which participants in the system are in possession of the used medium of exchange and how much do they own. In the second one, the system required a subset of participants, which Wei Dai calls "servers", who act as the ledger keepers and maintain the database for everyone.[112]

Since the servers would require a certain level of trust from other participants a mechanism needs to be set up to keep the server acting honestly. To keep those servers honest, each of them would be required to deposit a certain number of monetary units. Those units could be subsequently subtracted in case of server's misconduct. Further, since the servers would be administrating the ledgers on behalf of everyone else (other participants) additional mechanism needed to be in place to prevent the servers from inflating the monetary base without monetary value being actually created. The other participants in the second protocol would therefore be acting as supervisors to the servers monitoring the monetary base.[113]

3.5.2.1. Illustration of transactions in the theoretical concept of B-Money

Similarly, with the eCash, we believe that the best way for the reader to understand the transactions is to describe them in steps. Please, imagine there are the following participants. A person A who wants to send monetary units (hereinafter referred to as the "A") to a recipient

[111] Id.
[112] Id.
[113] Id.

(hereinafter referred to as the "B") and a third person who acts as an arbitrator in case the transactions does not follows as indented (hereinafter referred to as the "C"). The following example is taken from Wei Dai's whitepaper, except we have made it a bit more descriptive.[114]

1. B is in interested in paying for a solution of a problem, and values such solution at 100 monetary units;
2. Further B is willing to "insure" her payment of 100 monetary units by 200 monetary units;
3. A is interested in solving the problem posed by B and offers 2000 monetary units, should she not deliver her promise;
4. C is willing to act as an arbitrator for the transactions and offers 500 monetary units as a maximum reparation should she fail as an arbitrator;
5. Upon the solution of B's problem by A, B Broadcasts the intention to conduct a payment to the rest of the network;
6. Upon the receiving of the Broadcast everyone (each participant or servers in the second scenario) subtracts the monetary units from B's account;
7. Should this broadcast result in negative balance for B, the broadcast message will be ignored and the none of the units will be subtracted or credited;
8. If the transaction follows thru without a problem, each of the participants (or the servers) broadcasts the results to the other participants;
9. Participants credit the corresponding amounts to A.
10. Should the transaction between A and B fail for any reason, C should broadcast a solution to the network in example A pays to B fine in the amount of 100 monetary units.
11. Should C fail to conduct her duties the rest of the network should come up with appropriate solution.[115]

[114] Ibid.
[115] Ibid.

It is worth noting, that Wei Dai did not describe all the possible issues, therefore the actual functioning of the payment system remains questionable. In example this proposal shows a concept where the double spending issue is solved by other participants, rather than a third-party authority. Nevertheless, this concept still suffers from trust-based problems. In the above given example we are unsure what power C has in order to enforce the transaction.

3.5.3. The theoretical concept of B-Money aimed on money creation

Similar to the transactions, B-Money also proposes two different possibilities to create the monetary units. Common to both alternatives, Wei Dai first proposes that the medium of exchange should be completely without value (no intrinsic value) before being created (basic line of code).[116] The medium must however be able to reflect how much computational power was used to created it.[117] To illustrate Wei Dai gives an example: "*if a problem takes 100 hours to solve on the computer that solves it most economically, and it takes 3 standard baskets to purchase 100 hours of computing time on that computer on the open market, then upon the broadcast of the solution [Creation of new money.]*[118] *to that problem everyone credits the broadcaster's account by 3 units.*"[119] Therefore the computational power used by a computer (electricity burned) should give value to the medium of exchange.

In the alternative Wei Dai proposes the monetary units should be created in competition. First the participants or servers decide how much monetary units should be created for a respective period depending on the macroeconomic needs of the system. Subsequently, all the participants can submit bids. The bid is composed of a – how much money wants such participant to create out of the agreed number of monetary units, and b- what computational problem is such participant going to solve. In other words, how much, computational power is she willing to spend on the creation of the monetary units. Once the bidding participants spent the computational power and broadcasts the solution to the network, the network then decides

[116] Ibid.
[117] Ibid.
[118] Author's note.
[119] Ibid.

what bids are the best in term of the ratio – monetary units created, and computational power spent and credits the bidder's monetary units to their respective accounts.[120]

Both of those concepts allow for a creation of monetary units without a direct investment denominated in fiat currency. This approach allows for independence from the existing financial system and thus from its supervision[121]. Interestingly, the pay with computational power part of those concepts is older than it may seem. This concept is called Proof-of-Work. Proof-of-Work is important to understand as it is the basic technology used in Bitcoin, which allows for validation of transactions within the Bitcoin's network itself. Wei Dai was one of the first to see that the computational effort can be used to create valuable digital properties.

3.5.4. Introduction to Proof of Work

Proof of Work was not a new technology at that time. In 1992 Dr. Cynthia Dwork and Dr. Moni Naor have published article named Pricing via Processing or Combatting Junk Mail.[122] In this article the authors address and propose solution to everlasting problem, the unsolicited e-mail messages. Authors among others argue that one of the reasons for the proliferent use of emails is that such messages are essentially free to send.[123]

The cost of sending one email message, thousand or even a million does not substantially differ. In the above-mentioned article, the authors have proposed a sort of postage for emails. "*The main idea is for the mail system to require the sender to compute some moderately*

[120] Ibid.
[121] The difference between previous attempts to create digital medium of exchange and this proposal is that so far all of the previous attempts required a trusted third-party, which would facilitate the transactions. Interestingly, the technology that would allow for trustless transactions started due to the somewhat annoying problem of e-mail spam.
[122] Dwork C., Naor M. (1993) Pricing via Processing or Combatting Junk Mail. In: Brickell E.F. (eds) Advances in Cryptology — CRYPTO' 92. CRYPTO 1992. Lecture Notes in Computer Science, vol 740. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48071-4_10 available at: https://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf (archived version available via: https://archive.fo/kkvkb)
[123] Id. at 1.

expensive, but not intractable, function of the message and some additional information."[124] Such a function is called a pricing function.[125] This cost will deter junk mail but will not interfere with other uses of the system.[126]

In other words, the system proposed by Dr. Dwork and Dr. Naor did not require a user to pay anything directly. It did not propose a digital postage per se. Rather it required the user to use a certain amount of electricity to send an email as the computation of given problem was demanding on the hardware. While the user's electricity bill would remain pretty much the same if she used the email client for normal purposes, should she send a thousand emails an hour, the cost of electricity raises substantially. Therefore, making the use of electronic mail less desirable for spam.

Later on, in 1997 Marcus Jakobson and Ari Jules, published a paper, where they expanded on the knowledge presented by Dr. Dwork and Dr. Naor and use the notion Proof-of-Work for the first time.[127] They also define Proof of Work in apt way: *This is a protocol in which a prover demonstrates to a verifier that she has expended a certain level of computational effort in a specified interval of time.*[128]

3.5.5. Conclusion

In this part we have summarized a theoretical conception of private digital payment system called B-Money. In the first part of this subchapter, we are talking about the political motivations of the author Wei Dai and his association with the group Cypherpunks. Subsequently, we describe Dai's conception of B-Money as he has divided it. First with aim on the solution on transactions

[124] Id.
[125] Id. at 139-140.
[126] Id. at 139.
[127] JAKOBSSON, Markus a Ari JUELS. PROOFS OF WORK AND BREAD PUDDING PROTOCOLS (EXTENDED ABSTRACT). Secure Information Networks [online]. Springer Science+Business Media Dordrecht, 1999, 258-272 [cit. 2022-04-05]. Available at: https://link.springer.com/content/pdf/10.1007/978-0-387-35568-9_18.pdf (Archived version available via: https://archive.ph/YLvkx)
[128] Id. at 259.

and then with the aim on the solution of money issuance. In connection with the monetary creation, we also describe the origin and functioning of the Proof-of-Work technical solution.

As for the political motivation we show that influential group of scientists, including the author of B-Money, have decide to dedicate their time and knowledge to the development of a new payment system with accent on privacy and its disconnection from existing financial system.

As for the B-Money concept, we first address the system that revolves around transaction facilitation, addressing primarily the proposed system of check and balances, which was intended to allow for diminishing the need of trust between its participants. The check and balances had predominantly economic motivators using the system medium of exchange and escrows. However, we also note that since this concept was purely hypothetical the actual functioning of it was questionable. Nevertheless, we believe that the whole proposal of B-Money was more interesting in the secondary money creation design.

The money issuance according to Wei Dai shall have been facilitated using the Proof-of-Work technology, which allows essentially to pay with computer power. In other words, the technology it able to monitor how much computational power and electricity one had to expand in order to provide a solution to a given problem, which subsequently allows for creation of value derived from this used computational power. This allows for independent creation of monetary units because the protocol understands that one hour of certain amount of computational power amounts to, in example, 100 monetary units.

3.5.6. What do we infer from Wei Dai's B-Money?

Wei Dai's proposal B-Money seems to have been quite influential on the current Digital Assets conception. First, the political stand to create anonymous payment systems independent of the classic financial system is important to understand. In our opinion, it may be motivated by a different economical belief, as stated by the various authors. Such as the disagreement with

fractional reserve banking, the guided fiat money inflation, central banking et cetera. however, to embody such believes in digital protocols also means to shrug off the regulation accompanying the classic financial system and products. As we will show in the later chapters, this is easily abused by criminals. Not to forget that the proclaimed need for anonymity just embraced such interests and makes it even more interesting for them.

B-Money, also show a great step forward for the decentralization and ability to function without the trusted third party. Employing the distributed database systems, which allows for each participant to verify the validity of transactions independently, thus diminishing the information asymmetry to very low levels compared to classic financial systems. Additionally, the introduction of game theory based economic motivators, which encourage participants to act honestly to receive an economic incentive. Further, the introduction of independent money creation using the Proof-of-Work concept is revolutionary, as it allows to coin value into digital files, which can then be used as a medium of exchange.

Still, it shall be noted that since the B-Money system remains purely theoretical, it cannot be established, whether it would have been successful in reality. Nevertheless, the Digital Asset Bitcoin uses much of those above-mentioned principles and remains one the most successful technical projects of its type.

3.6. The case of BitGold

3.6.1. Introduction and about Nick Szabo

The next addition to Bitcoin precursors is the idea of yet another Cypherpunk - Nick Szabo. Nick Szabo is alumni of University of Washington and George Washington University. He is both a computer scientist and legal scholar. Nick Szabo is quite an active thinker. He keeps a BlogSpot called Enumerated, where he posts his thoughts and articles. In this BlogSpot he also published the idea of Bit Gold. Even though the first idea of a digital online only payment system Bit Gold

came to Nick Szabo in 1998. He fully described it in 2005 Mr. Szabo. Similar to Wei Dai's B-Money the concept of Bit Gold remains purely theoretical.[129]

Nick Szabo also does not consider the existing financial system perfect. He argues that the inflationary and hyperinflationary prominence of central bank issued fiat money is not ideal state of affairs.[130] Further he seems to generally disagree with the concept of trusted third parties.[131] To the extend Mr. Szabo published a couple of studies where he disagrees with the extended use and power given to trusted third parties in the current world. In example a study with self-explanatory title "Trusted Third Parties Are Security Holes".[132]

Regarding money, Nick Szabo finds the scarcity of precious metals and collectibles ideal underlining value for money, but he argues that the issue with metals and collectibles is that a person cannot pay online with them.[133] "*Thus, it would be very nice if there were a protocol whereby unforgeable costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.*"[134]

3.6.2. Bit Gold payment system

Bit Gold utilized the Proof of Work concept introduced by Dr. Dwork and Dr. Naor. This concept was used in order to create a new money similar to Wei Dai's B-Money. Money creation was also conceptionally similar to Dr. Chaum's eCash, as the actual monetary unit was a hash. This fact

[129] Unless the reader feels like Bit Gold is actually Bitcoin, as those concepts are so close in its functionality it raises intriguing questions.
[130] SZABO, Nick. Bit Gold. Blogspot.com [online]. December 27, 2008 [cit. 2022-04-05]. Available at: https://unenumerated.blogspot.com/2005/12/bit-gold.html (Archived version available via: https://archive.ph/4RWXv)
[131] Id.
[132] In example SZABO, Nick. Trusted Third Parties Are Security Holes. Www.fon.hum.uva.nl [online]. 2001 [cit. 2022-04-07]. Available at: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/ttps.html (Archived version available via: https://archive.ph/YQpMa)
[133] SZABO, Ibid. at 130
[134] Id.

gives us an opportunity to describe the Hashcode as it is an integral part of the current Digital Assets. Hashcode or simply Hash is a specific technological term describing an outcome of an algorithmic function.

3.6.2.1. The Hash function

This function is, as we have said, widely used in Digital Assets.[135] While it may seem complex in the beginning the function itself is not that complicated. One-way hash function is a function h satisfying the following conditions:

1. The argument X can be of arbitrary length and the result h(X) has a fixed length of n bits (with $n \geq 64$).

2. The hash function must be one-way in the sense that given a Y in the image of h, it is "hard" to find a message X such that h(X) = Y, and given X and h(X) it is "hard" to find a message $X' \neq X$ such that h(X') = h(X).[136]

3.6.2.2. Practical examples of the hash function

In other words, the function h shall work in the following sense: Function h (one way hash function) shall be applicable to any number of characters. In the formula above, the number of characters – the data set is represented by the letter x. Out of such number of character (x) the outcome shall be always fixed to a certain length. In this case the length is limited to 64 characters or less. Further condition is, that it shall be easy to compute the combination of h and x. However, given the h and existing outcome of h and x the h(x) should

[135] However, for different purposes than to represent the monetary units. As explained below, Hash Function is used for passing information anonymously on blockchain.

[136] PRENEEL, Bart. CRYPTOGRAPHIC HASH FUNCTIONS. Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 161–171, 1993. [online]. 1-29 [cit. 2022-04-07]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.800.5133&rep=rep1&type=pdf (Archived version available at: https://archive.ph/V2Btv)

be computationally infeasible to find the x itself. Meaning the amount of energy and time spent on figuring out the x should be detrimental.[137]

To give practical example, we take the following quote from Friedrich A. Hayek: "*It is one of the saddest spectacles of our time to see a great democratic movement support a policy which must lead to the destruction of democracy, and which meanwhile can benefit only a minority of the masses who support it. Yet it is this support from the Left of the tendencies toward monopoly which make them so irresistible and the prospects of the future so dark.*"[138], and use the above-mentioned h function the result, the hash, will look like this:

b24cde2d2afb178294ab72343d128bbe01686a47a27d0999fadc68a5d681e663[139]

Should we change the x (data input) even in the sightliest form – using the same sentence, however omitting the dot at the end the result will look like this:

778397da420ed477a985964e07c4a63753d0a1e3de39ceef2da2c7735b631f2f[140]

As the reader can see, even the sightliest change in the data input will completely transform the outcome. Therefore, even if the data input will be nearly identical the outcome will be completely different every time. As the reader can see, the outcome of the hashing function is therefore completely unpredictable.

---

[137] SOBTI, Rajeev a G. GEETHA. Cryptographic Hash Functions: A Review. International Journal of Computer Science Issues [online]. March, 2012, 9(iss. 2) [cit. 2022-04-07]. ISSN 1694-0814. Available at: https://www.researchgate.net/profile/Geetha-Ganesan/publication/267422045_Cryptographic_Hash_Functions_A_Review/links/549cf6d10cf2b8037138c35c/Cryptographic-Hash-Functions-A-Review.pdf (Archiver version available via: https://archive.ph/EWzTw)

[138] The quote was hashed without the quote's symbols. HAYEK, Friedrich. The Road to Serfdom. Fiftieth Anniversary Edition, 274 p. 205. Chicago USA: University Of Chicago Press, 15th 1994n. l. ISBN 9780226320618.

[139] For the actual hashing we are using this internet tool: https://emn178.github.io/online-tools/sha256.html, which however does not keep the text, therefore, to access the example we have given, please access this link: https://www.linkpicture.com/q/Sha256-vr-1.png (Archived version available via: https://archive.ph/MYrO0)

[140] For the actual hashing we are using this internet tool: https://emn178.github.io/online-tools/sha256.html, which however does not keep the text, therefore, to access the example we have given, please access this link: https://www.linkpicture.com/q/Sha265-vr2.png (Archived version available via: https://archive.ph/kMO3b)

Should we use a shorter sentence or even just a small number as an x, the result will still be 64 bits. Using the number "135":

13671077b66a29874a2578b5240319092ef2a1043228e433e9b006b5e53e7513[141]

From the string of the characters, the reader is unable to figure out what is the value of the x, without using a significant (virtually impossible) amount of power. In conclusion, this one-way function allows to input a substantial amount of information to create fixed length output, out of which is practically impossible to derive the input.

3.6.2.3. Money creation in Bit Gold payment system proposal

Now, when the readers have an idea what a hash is, we can describe the money creation under Bit Gold. To create the monetary units used by Bit Gold a person first needed to discover a valid hash. Valid hash was such hash, which satisfied certain conditions. In example the condition may state that the valid hash should start with a given number of zeros at the beginning of the data string. Taking the previous example, the valid hash could look like this:

00000077b66a29874a2578b5240319092ef2a1043228e433e9b006b5e53e7513.

The user is however not looking for the exact match, but only for a similar Hash that has the same number of zeroes in the beginning. To discover such hash, user first had to choose a so-called candidate string offered by the network itself.[142] To simplify, candidate string is basically a random number. To find a valid hash user subsequently needed to combine the candidate string with another randomly created number. As we have pointed out above, the exact outcome of such process is unpredictable. Therefore, to find valid hash user would have to use trial

[141] For the actual hashing we are using this internet tool: https://emn178.github.io/online-tools/sha256.html, which however does not keep the text, therefore, to access the example we have given, please access this link: https://www.linkpicture.com/q/Sha265-vr-3.png (Archived version available via: https://archive.ph/1xWvC)
[142] SZABO, Ibid. at 130

and error, because there was no other way to determine, which candidate string and random number combination would yield valid hash. Thus, the users would have to spent computer power to create the exact hash, which would make it valuable.

Once such hash was found the user who found it could keep it, similar to finding a real gold in the ground. As distinct from a real-world gold, the hash would include a candidate string for the other hash.[143] Once the other (following) hash would be found, the hashes would form a chain, which would include all the proof of works that had to be used to produce such hash. In a way similar to Blockchain.

Also similar to Bitcoin the owners of valid hashes would keep them in a public registry, which would be composed of public keys corresponding to the valid hashes. The public registry was based on another article written by Szabo.[144] This public registry was to be administrated by designated users similar to Wei Dai's servers. Those designated users would keep track of which public addresses held what hashes.

3.6.3. The Timestamp Function

This project also used a piece of technology relevant to current Digital Assets, so called timestamp. Timestamp refers to a protocol that allows registering the current time and date to digital file. A timestamp or time stamp is a time registered to a file, log, or notification that records when data is added, removed, modified, or transmitted.[145] Timestamps have a variety of uses nowadays. In example photos taken by digital camera are usually timestamped to show the day and time when such picture was taken. Similarly, digital signatures are timestamped

[143] Id.

[144] SZABO, Nick. Secure Property Titles with Owner Authority. Nakamotoinstitute.com [online]. 1998 [cit. 2022-04-11]. Available at: https://nakamotoinstitute.org/secure-property-titles/ (Archived version available via: https://archive.ph/uTHzS)

[145] What is a Timestamp? Computerhope.com [online]. 2022 [cit. 2022-04-11]. Available at: https://www.computerhope.com/jargon/t/timestam.htm (archived version available via: https://archive.ph/K0S9z)

to show when such signature was executed.[146] Timestamp also found its use in the blockchain technology.

In Bit Gold timestamp was used as a part of the solution which controlled inflation. Within the bit gold payment system inflation would be caused by the improving computational power. As the computers would get better, it would be easier for them to find valid hashes. Hashes would therefore become more common over time and therefore less valuable.

To solve this inflationary problem Nick Szabo implemented timestamp. Once a valid hash was found the bit gold payment system would automatically timestamp it. As the hash would bear time and date it would be possible to estimate how much computational power had to be expended in order to find valid hash from such date. Because it was harder to find valid hashes in the past, the older the hash is the more valuable it should be. The exact value of hashes would be then determined relative to new hashes by the network market.

3.6.4. Conclusion

Since the Bit Gold payment system is very similar to Wei Dai's B-Money, we use it primarily to describe some of the used technological solutions. The two solutions we describe are the hashing technology and the Time Stamp technology. In case of the Hash technology, we also describe its role in money creation in Bit Gold payment system proposal. We also once again address the political believes of the author of the described payment system, this time Nick Szabo. Nick Szabo argues for the independence of classic financial systems, inflationary currencies, and the concept of trusted third parties.

At first, we summarize the functioning of the Hash technology giving practical examples. The Hash function is a function that allows to create a fixed length output, called the hash, from

[146] Other examples can find here: LUTKEVITCH, Ben. Timestamp. Techtarget.com [online]. 2021 [cit. 2022-04-11]. Available at: https://www.techtarget.com/whatis/definition/timestamp (archived version available via: https://archive.ph/bE66w)

basically unlimited length input. Since the function is based on trapdoor mathematics one cannot derive the input from the output. Further, any even the smallest changes in the input will completely change the output, this function can be used in example in verifying data integrity. The Hash function is easy to compute (execute) but extremely hard to reverse engineer (in fact it is currently impossible). Therefore, any attempt on its hostile solution must be executed via brute force (guessing).

The money creation in Bit Gold was based on the combination of the above-mentioned Hash function and brute force, which expenditure was validated trough the Proof-of-Work concept to ascribe value to digital hashes. To put simply, Bit Gold users were using computer power to guess a value (respectively a part of) of a preset hash, once they found such value they were awarded with money.

As per the Time Stamp technology, we summarize that it's a protocol, which permanently ascribes time and date to any data upon its modification. Since the time moves only in one direction, this function allows to anchor such data and serve as a reference point in case of its hostile change attempts.

3.6.5. What do we infer from the case of Bit Gold?

We mention Bit Gold because it is often compared to the Bitcoin. We use it primarily to show the two other essential pieces of technology that allows for trust lessness of private payment systems.

Since the system was never implemented, we cannot evaluate the whole concept from practical point of view. Nevertheless, the money creation process bears many similarities with the one used in Bitcoin and other Digital Assets, therefore we can infer that it served as an inspiration for the creation of Bitcoin itself.

3.7. The case of Bitcoin and chapter conclusion

Satoshi Nakamoto have said in his own whitepaper to have drawn some inspiration from those previous attempts on private payment systems[147]. In this part, we decided to synthetize the basic of Bitcoin with the historical and technological facts we have summarized in this chapter. While there is no reason to get predominantly technical about Bitcoin and its background, as we are dedicating a whole chapter to description of Blockchain with accent on Bitcoin examples, there are certain specificities of Bitcoin that we will also address here.

Bitcoin could be view upon as a digital, decentralized, partially anonymous asset that may serve as a medium of exchange, which is not backed by any government or other business (legal) entity, and not redeemable for gold or other commodity, but it can be exchanges for fiat currency using third party services. For transactions Bitcoin relies on peer-to-peer networking and cryptography to maintain its integrity.[148].

We have summarized that since the inception of E-Gold, the authors were trying to use the internet as a utility backbone for private payment systems. Further, all of the described systems and proposals had in common the goal of independence from a current financial system. As a functioning private payment system, we have introduced E-Gold, which facilitated for transaction of accounts, holding units denominated in precious metals. While the system seemed to have achieved a partial independence from the financial system it was rooted with legal problems.

The Case of E-Gold has proven that once even partial independence is attained, and such system is actually working, it will inevitably attract the criminal element. In connection with E-Gold we have summarized that its centralized nature was susceptible to regulatory repression.

---

[147] NAKAMOTO, Ibid at 58.

[148] Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 Hastings Sci. & Tech. L.J. 159, 160 (2012) Available at: https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1063&context=hastings_science_technology_law_journal (Archived version available via: https://archive.ph/ZCb0g)

Even if the founders had fought a legal battle arguing that the system should not fall within the then current regulatory scope, in the end they have lost as their arguments were rejected by the court. Thus, we infer that to create a independent private payment system, it would have to be trustless, meaning it would have to work without central authority.

As we summarize with the subsequent subchapter, the decentralization was inspected by the projects B-Money and Bit Gold, but as those projects had reminded purely theoretical the first actual decentralized was achieved by Bitcoin. The decentralization of Bitcoin simply means that there is no central authority that oversees Bitcoin system, its state, or its work.[149] In other words, it means that there is no intermediary facilitating the money creation, as it was in the case of DigiCash's eCash nor any authority helping with the transactions.

Specifically, however, as Bitcoin does not have a central authority, it lacks a central point such as a person or a business entity that could be pressured into cooperation with authorities. That means that there is no entity that could be effectively regulated, and there is no general "off switch" to turn Bitcoin off. We suppose that that is a reason, why the Digital Asset Bitcoin have survived until now, without any major changes and allowed for creation of other its alternatives, which are often called "Altcoins".

To achieve the trust lessness, Bitcoin is employing wide variety of technological solutions. Some of them we have described in the historic chapters, such as the use of Hash function, private and public keys (asymmetry cryptography), the Proof-of-Work and the Time Stamp function. Additionally, Bitcoin also employ game theory-based solutions such as economical motivation and inspiration in order to provide incentive to its honest users. These incentives systems we describe mainly in the two theoretical projects of B-Money and Bit Gold.

[149] Ibid. at 174

We also dedicated part of this chapter to the project called eCash, which focused primarily on the anonymity of transactions and the anonymity in general. We use this project as an anchor to show that all of the authors of those projects have believed in full financial anonymity and conceived developed the payment systems with such thoughts in their mind. We further argue that the combination of anonymity with the absence of a trusted third party is something that attracts the criminal element to such payment systems.

The Bitcoin was conceived with pretty much identical ideals. As such the system is partially anonymous. In case of Bitcoin that means that anyone can see the trail of all transactions from all accounts. However, all such spectator (without additional tools) will see is a combination of public keys (which represent the accounts), but nothing in the system ties those accounts to individuals. In other words, one cannot infer any personal data just from the public key – address. Further, anyone can create unlimited accounts represented by those public keys instantly and for free.[150]

The accounts used in the Bitcoin network are called addresses.[151] Despite what we summarized above it was proven over the time however, that the partial anonymity of Bitcoin is not unbreakable. Since the trail of all transaction from all accounts is publicly accessible it necessarily leaves a followable trail.[152] According to the American Court in Second Circuit Bitcoin is therefore anonymous but the transactions can be traced.[153] We shall still add that the deanonymization requires additional tools and mechanisms. We further addressing this topic in the technological and regulative parts of this Thesis.

[150] Ibid. at 164 – 165
[151] Address - Bitcoin Wiki, https://en.bitcoin.it/wiki/Address (last visited Jun 6, 2019) (Archived version available via: https://archive.ph/WbtTP)
[152] Wade V. Davies, *Bitcoin Criminals*, 53 Tenn. B.J. 24, 26 (July 2017) Available at: https://www.tba.org/index.cfm?pg=LawBlog&blAction=showEntry&blogEntry=28335 (Archived version available via: https://archive.ph/AfPca)
[153] Ibid.

In this chapter we have also addressed the money creation. At first the projects used centralized solution. In the regard to the E-Gold money creation process we have summarized that the solution chosen was an internal trusted intermediary who enabled the creation of accounts and the IUO units. Even more reliant on the financial system was the second project we described – eCash. ECash needed a bank to create money, as its creation was more of just its anonymization. With the inception of B-Money and Bit Gold, the proposed solution both utilized proof-of-work concept to create monetary units. Proof-of-Work is a process that verifies that computational power was used to conduct an operation. An example is to solve a large number of fairly easy mathematical operations. The computation power can be "coined" using proof-of-work. This solution was used by Bitcoin, which is the first project to use it real payment system. We describe the actual implementation of Proof-of-Work in Bitcoin in the following chapter.

For the sake of completeness, we also address how the Bitcoin transactions works. As mentioned above, the Digital Asset Bitcoin does not use accounts per se, but rather so-called addresses. In order to partake in Bitcoin transaction both the sender and receiver must have an address.[154] Instead of providing institutional protection of any kind (as Bitcoin does not use any intermediaries), the Bitcoin equip each address with private and public keys.[155] Those codes essentially work like a routing number and transfer authorization.[156] Each bitcoin transaction is irreversible.[157] The validity of each transaction is verified by the Bitcoin network itself by comparing the codes.[158] The network of users is economically motivated to verify transactions similarly as in Wei Dai's B-Money. However, in Bitcoin the participating users will receive not only the fees associated with each transaction but also a newly minted bitcoins, which serve as a medium of payment. The Bitcoin networks, respectively the users with computing

[154] Sasha A. Klein, Andrew R. Comiter, *Bitcoin Are You Ready for This Change for A Dollar?*, 29 Prob. & Prop. 10 (March/April 2015) Available at: https://heinonline.org/HOL/Page?handle=hein.journals/probpro29&div=23&g_sent=1&casa_token=&collection=journals (Archived version available via: https://archive.ph/3Tynz)
[155] *Ibid.*
[156] *Ibid.*
[157] *Ibid.*
[158] *Ibid.*

power behind it, verify transactions with higher fees before transactions that have lower, or no fee added.[159] We also further describe the transaction functionality in the following chapter. In conclusion Bitcoin network is a self-executory, partially anonymous completely decentralized network able of transactions without any need for intermediary.

[159] Some argue that this system is not sustainable long term. Kerem Kaskaloglu, *Near Zero Bitcoin Transaction Fees Cannot Last Forever*, INT'L CONF. ON DIGITAL SECURITY & FORENSICS 91, 91-93 (June 2014) Available at: https://www.researchgate.net/profile/Natalie-Walker-15/publication/263617788_Proceedings_of_the_International_Conference_on_Digital_Security_and_Forensics_DigitalSec2014/links/0f31753b5cd085c06a000000/Proceedings-of-the-International-Conference-on-Digital-Security-and-Forensics-DigitalSec2014.pdf#page=93 (Archived version available at: https://archive.ph/oTgo4)

4. Blockchain

4.1. Introduction to Distributed Ledger Technology and Blockchain

Distributed Ledger Technology, also known under DLT forms technological backbone of the majority of Digital Assets. The terms Blockchain and Distributed Ledger Technology are often being used interchangeably. Nevertheless, Blockchain is a more specific term. As such we consider important to describe the difference between DLT and Blockchain.

Essentially, DLT is a distributed database. Any information contained in such distributed database is located at multiple mutually interconnected in participating data storages. Those data storages are termed ledgers. Ledgers are then maintained in different geographical locations. In other words, ledgers are stored and distributed over the Internet around the world[160]. Blockchain then is a subset of so-called Distributed Ledger Technology.[161]

The data records contained in ledgers should be always identical. Basically, every ledger connected to the same DLT is a real time updating clone of each other. Each ledger is collectively maintained by a network of participating computers. Computers upkeeping the ledgers are referred to as nodes. Nodes both update and share the information contained in ledger on a real time basis between each other creating a decentralized network. In other words, nodes are those participants who create the new blocks[162].

[160] 3. BIS Annual Economic Report 2018: V. Cryptocurrencies: looking beyond the hype. 2018. 91-114 [cit. 2021-12-19] Available at: https://www.bis.org/publ/arpdf/ar2018e5.pdf (archived version available via: https://archive.ph/LdFXi)

[161] HOUBEN, Robby a Alexander SNYERS. Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion [online]. European Parliament, 2018, 1-100 [cit. 2021-12-19]. ISBN 978-92-846-3200-8. Available at: https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (archived version available via: https://archive.fo/u1cEi)

[162] PARK, Sehyun, Seongwon IM, Youhwan SEOL a Jeongyeup PAEK. Nodes in the Bitcoin Network: Comparative Measurement Study and Survey [online]. 30 April 2019, 57009 - 57022 [cit. 2022-04-14]. ISSN 2169-3536. Available at: https://ieeexplore.ieee.org/abstract/document/8703385 (Archived version available via: https://archive.ph/DG8Bx)

In short: "*DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes.*"[163]

It is important to note that nodes provide append-only data to the ledgers. In DLT the participating nodes are only allowed to add new data to the ledgers but are forbidden by code to rewrite (change) ledger's existing data. Therefore, the data contained in ledgers should be theoretically immutable.

Since Blockchain is still the major application of DLT in digital assets we decided to focus primarily on Blockchain rather than the whole universe of DLT. However, should the underlying technology of given digital asset differ to an extent which would have legal implications we will describe its technical differences separately.

4.2. Permissioned and Permissionless Blockchain

Before we approach the description of Blockchain itself, we need to explain the basic division of Blockchains. The division is based on an important - is who allowed to participate. While Blockchains are often perceived as an open to all environments it is not that simple. Some Blockchains require certain conditions for its users to participate. Therefore, the Blockchain can be divided between Blockchains, where the user does not need any permission to participate so called Permissionless Blockchain. Additionally, there are Blockchains that are closed to participation unless some conditions are satisfied. Those Blockchains are called Permissioned Blockchains. However, please understand that the following division of Blockchain represents rather the two ends of a spectrum than two possibilities.

[163] HOUBEN at all., Ibid. 161, at 15

4.2.1. Permissionless Blockchain

Blockchain may be set to be completely open for participation. The access to such networks is only limited by technical means such as the download of a current client (usually open-source software).[164] Therefore, the participants can join or leave the network at will, without being pre-approved or vetted by any entity[165]. Every user is allowed to carry out all the activities within the network. Any user can initiate transactions, read the ledgers, write into the ledgers, propose, and add new blocks.

The ownership of such Blockchains is disputable and arguable belongs to the community or to no one, as there is no central owner of a Permissionless Blockchain[166]. Permissionless Blockchains therefore have no central point of liability. Generally, this kind of Blockchains maintain open and transparent ledgers to all nodes[167]. However, as the Permissionless Blockchains are open to anyone those Blockchains are more vulnerable to user's abuse and needs to employ mechanisms to prevent malicious behavior.

Since anyone can participate without limitation the user's identity may remain anonymous or pseudo-anonymous[168]. Usually there is no know your customer check to join a permissionless Blockchain. The permissionless Blockchains therefore have to employ mechanisms that allows for cooperation between mutually unknown and distrusting users. Those mechanisms allow for consensus, however, are often slower in processing transactions (data) and usually requires energetically demanding consensus mechanisms such as Proof of Work[169]. Permissionless Blockchains are therefore slower and more resource demanding. Typical representant

[164] YAGA, Dylan, Peter MELL, Nik ROBY a Karen SCARFONE. Blockchain Technology Overview. National Institute of Standards and Technology [online]. October 2018, 1-43, at 5, [cit. 2022-04-14]. Available at: doi:https://doi.org/10.6028/NIST.IR.8202 (Archived version available via: https://archive.ph/PbsmJ)
[165] World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed- Ledger-Technology-and-Blockchain-Fintech-Notes.pdf (archived version available via: https://archive.fo/SyRup)
[166] Id.. at 11
[167] Ibid. at 12
[168] Ibid. at 12
[169] Ibid. at 12

of Permissionless Blockchain is Bitcoin's blockchain. It is perceived that permissionless blockchains are completely trustless, but as we will explain later on, the trust is involved in case of permissionless blockchains as well.

4.2.2. Permissioned Blockchain

Permissioned Blockchain is a Blockchain with regulated access. This second type of Blockchain therefore must have some sort of authority (centralized or decentralized) which imposes rules on the participants[170]. Such authority then decides the allowed level of participation of users, i.e. whether such users can publish new blocks. However, this authority is not needed for the actual functioning of a Blockchain. Therefore, the transactions are still processed automatically without the need of a trusted third-party, but the access to participation in such Blockchain is to some extent limited and only pre-selected participants can join[171]. Permissioned Blockchains' ledgers are less transparent compared to the Permissionless Blockchains, but can process data faster, which allows for faster transaction times and higher transaction volume[172]. This type of Blockchain also allows for less energetically demanding consensus mechanisms such as Proof of Stake.

Permissioned Blockchains may find better applicability in business environment, where a single entity may be interested in maintaining the blockchain. In example the basic rules can be that all users are allowed to initiate and broadcast transaction, however only the business entity is allowed to publish new blocks (confirm the transactions, maintain the blockchain). Under such rules and if the permissioned Blockchain is limited to only one entity, then the users must have trust in such business entity, which essentially becomes trusted third party. A permissioned blockchain is not completely trustless. Transactions could be rolled back by a centralized agency with override authority. Transaction records could also be reversed if the majority of the members choose to do so. Therefore, the trust-lessness of a permissioned blockchain

[170] Ibid. at 11
[171] Ibid. at 12
[172] Ibid. at 12

relies on the credibility of the centralized agency and the architecture of the consensus protocol.[173]

Permissioned Blockchain can be therefore further divided between Open or Public Permissioned Blockchain and Enterprise Permissioned Blockchain[174]. The main difference between those two types is that on Enterprise Permissioned Blockchain only the central authority, the owner or administrator, is allowed to participate[175]. Public Permissioned Blockchain then imposes certain access rules, but generally does not limit the participation to only one party.

The rules applying to participation within Permissioned Blockchain may also regulate the anonymity of users. As only preselected nodes can participate in such networks, the anonymity of users is diminished, and some degree of identity verification is generally required[176]. Permissioned Blockchains can require all of its users to submit to identity verification. Once the users are no longer anonymous or pseudo anonymous, they have higher incentive to act honestly as they can be exposed to legal enforcement.

Virtually all aspects of Blockchain can be limited to some extent in Permissioned Blockchain. In example, transaction information can be made public, anonymous, or known only to the participating parties. Typical representant of Permissioned Blockchain is Ripple.[177]

[173] LIU, Manlu, Kean WU a Jennifer JIE XU. How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain. CURRENT ISSUES IN AUDITING American Accounting Association [online]. 2019, 13,(2) [cit. 2022-04-18]. Available at: https://www.researchgate.net/profile/Kean-Wu/publication/335472340_How_Will_Blockchain_Technology_Impact_Auditing_and_Accounting_Permissionless_Vs_Permissioned_Blockchain/links/5e270a3e299bf15216707ef4/How-Will-Blockchain-Technology-Impact-Auditing-and-Accounting-Permissionless-Vs-Permissioned-Blockchain.pdf (Archived version available via: https://archive.ph/VpXpR)

[174] HOUBEN at all., Ibid. 161, at 16.

[175] Ibid.

[176] NATARAJAN at all., Ibid. 165, at 12.

[177] For more information please see: https://ripple.com

4.3. Blockchain's elements

Blockchain is now one of the possibilities how to organize information using the Distributed Ledger Technology.[178] There are many definitions of Blockchain. In example a rather formal definition: "*Blockchain […] uses cryptographic and algorithmic methods to create and verify a continuously growing, append-only data structure that takes the form of a chain of so- called 'transaction blocks' – the Blockchain – which serves the function of a ledger.*"[179]

Additionally, a more apprehensible definition of Blockchain could be: Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.[180]

[178] We would like to note that each Blockchain can be developed differently. Therefore, some of the information here does not necessarily have to be true to each and every Blockchain. We have chosen the Bitcoin's Blockchain as a reference point.
[179] NATARAJAN at all., Ibid. 165, at 1.
[180] YAGA., Ibid. at 164

Blockchain is therefore a tool that can be used to organize ongoing influx of data. The Blockchain technology itself is composed of a number of elements working together. In order to understand, how Blockchain actually works we are going to describe individual elements of Blockchain technology in the following subchapters. The segments we are going to address in greater details are following:

1. Blocks,
2. Hash Function,
3. Cryptography
4. Address (accounts) and Transactions
5. Consensus Models

4.3.1. Blockchain's Elements – the Hash function

We have already introduced the Hash Function when we talked about Nick Szabo's project Bit gold. In this subchapter we can therefore continue in deeper details. Hash function is a function that is easy and quick to compute.[181] Hash function has the following additional criteria, it is preimage resistant, second-preimage resistant, and collision resistant.[182]

In simple words, preimage resistance means that a person knowing the output (digest of the function) is unable to count the input. Second preimage resistance means one cannot find an input that hashes to a specific output.[183] Collision resistance then means that the digests of two different inputs should never be the same. While collision remains theoretically possible, the chance of collision happening is so low, its occurrence under normal conditions is rather

[181] RAJPUT, Dharmendra, Ramjeevan THAKUR, Syed BASHA. Transforming Businesses with Bitcoin Mining and Blockchain Applications. India, 2019, 282 p at 209. ISBN 9781799801863.
[182] WANG, Maoning, Meijiao DUAN a Jianming ZHU. Research on the Security Criteria of Hash Functions in the Blockchain [online]. 2018 [cit. 2022-04-18]. ISBN 978-1-4503-5758-6/18/06. Available at: https://dl.acm.org/doi/epdf/10.1145/3205230.3205238 (Archived version available via: https://archive.ph/xaQV2)
[183] YAGA., Ibid. at 164. More specifically, cryptographic hash functions are designed so that given a specific input, it is computationally infeasible to find a second input which produces the same output (e.g., given x, find y such that hash(x) = hash(y)). The only approach available is to exhaustively search the input space, but this is computationally infeasible to do with any chance of success.

impossible.[184] To illustrate it is forty-five times more likely the Earth will be hit by a Chicxulub like asteroid in the next few seconds than that a collision would occur under the Bitcoin used SHA256 hashing algorithm.[185]

Hash function has widespread use withing Blockchains. Hash function is used in example in connection with consensus mechanisms, address generation, pseudorandom number generation, and data digests.[186]

4.3.2. Blockchain's Elements – Transactions

Transaction is rather wide term. A broad definition of transaction could be: Something which has taken place, whereby a cause of action has arisen. It must therefore consist of an act or agreement, or several acts or agreements having some connection with each other, in which more than one person is concerned, and by which the legal relations of such persons between themselves are altered.[187]

In Blockchain environment transaction may also represent mutual or reciprocal action between actors. In example a transfer of Digital Assets is a transaction. Similarly, creating a smart contract on a blockchain or uploading data on Blockchain could amount to a transaction. Any transaction

---

[184] In example, the popular Hash algorithm SHA-256 allows for 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 possible outputs. For more information please see: RAJPUT, Dharmendra, Ramjeevan THAKUR, Syed BASHA. Transforming Businesses with Bitcoin Mining and Blockchain Applications. India, 2019, 282 p at 209. ISBN 9781799801863.

[185] PORNIN, Thomas. Is it safe to ignore the possibility of SHA collisions in practice?. Stackoverflow.com [online]. 2010 [cit. 2022-04-18]. Available at: https://stackoverflow.com/questions/4014090/is-it-safe-to-ignore-the-possibility-of-sha-collisions-in-practice (Archived version available via: https://archive.ph/6JH6i)

[186] DILHARA, Shashie. A Review on Application of Hash Functions and Digital signatures in the Blockchain Industry. Department of Network & Security [online]. Sri Lanka: NSBM Green University, September 2021, 1-5 p., at 2 [cit. 2022-04-18]. Available at: https://www.researchgate.net/publication/354700341_A_Review_on_Application_of_Hash_Functions_and_Digital_signatures_in_the_Blockchain_Industry/link/61489c713c6cb310697fbd67/download (Archived version available via: https://archive.ph/f847M)

[187] BLACK, HENRY. BLACK'S LAW DICTIONARY: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern [online]. 4th Ed. Rev. WEST PUBLISHING CO., 1968 [cit. 2022-04-18]. Available at: https://heimatundrecht.de/sites/default/files/dokumente/Black%27sLaw4th.pdf (Archived version available via: https://archive.ph/GGcjS)

on a Blockchain is represented by data. The data in any Blockchain transaction are very important. The Blockchain network works autonomously using protocol. Based on the protocol the Blockchain is checking, whether the transaction's data is valid, which then means the transaction itself is valid.

Data contents of transaction involving Digital Assets may differ based on Blockchain[188]. Usually, such transaction is comprised of identifiers, inputs, and outputs.[189] Once such transaction is initiated all the information included within, will be broadcasted to the whole network, to all of the participating nodes.[190]

Identifiers refers to information that the protocol uses to identify, who is conducting the transaction. In example in Bitcoin's Blockchain the sender's address is used as an identifier.

Input could be also looked upon as the body of the transaction. It often includes the digital assets that are subject to the transaction. The data regarding those digital assets are recorded in form of its source. Meaning the data will either include information from past transfers regarding such Digital Assets. In such case the network monitors whether the initiator has the right to spent (use) such Digital Assets. In case the Digital Assets are completely new, were newly emitted, the input will reference to the origin event.[191]

The input may also include information about, whether the digital assets send should split into new assets, basically creating change, or whether such assets should be combined creating more value. This possibility (necessity) exists, because the information that makes transaction valid

[188] In example Bitcoin employs transaction centered model and Ethereum employs account centered model for transactions.
[189] WU, Jiajing, Jieli LIU, Yijing ZHAO a Zibin ZHENG. Analysis of Cryptocurrency Transactions from a Network Perspective: An Overview. Journal of Network and Computer Applications [online]. Elsevier, 7 august 2021n. l., 1-24 p. at 4 [cit. 2022-04-18]. Available at: https://arxiv.org/pdf/2011.09318.pdf (Archived version available via: https://archive.ph/ZPtML)
[190] Ibid. at 4.
[191] YAGA., Ibid. at 164

refers to the last time such Digital Assets were spent, and the amount of such Digital Assets is set and can't be changed unless those Digital Assets are spend again.

This issue is quite complex to describe generally, therefore we will explain it on specific example. Please imagine a Persons A, B and C, all of them are users of Bitcoin's Blockchain. Person A has received 1 bitcoin from person C and have other 0.2 bitcoin of her own. Those bitcoins represent all of Person's A property. Person B requests that Person A pays her 0.8 Bitcoin.

The whole transaction may now go two ways, depending on the state of Person A's bitcoins in the past. Bitcoin network (its protocol) will first check whether Person A have already her bitcoins (data including the information from past transfer). However, this past even cannot be changed so the past data have to include the exact composition of the value transfer.

The face value of 1.2 bitcoin only represents the total value of the units not its composition. Therefore, the value of 1.2 bitcoin can be composed of 1 bitcoin and 8 times 0.025 bitcoins as each of bitcoins have a different origin event. Person C have sent exactly 1 bitcoin to person A. The origin event for the right to spend this 1 bitcoin is therefore one transaction from Person C for exactly 1 bitcoin.[192] The remaining 0.2 bitcoins will have different origin events. Person A might have sold something worth 0.025 bitcoins 8 times, which all represents the past origin event that must be included in the input data part of a transaction.

Should this be the case Person A would have the right to spent exactly 1 bitcoin or 8 times exactly 0.025 bitcoins. Technically speaking, Person A would not have right to spend, say 0.8 bitcoin, she must spend the whole 1 bitcoin and exchange it. It is because the protocol rule regarding unspent transaction is following. The inputs are made up of a set of unspent transaction outputs whose sum of amount is not less than the amount that is to be paid, and the payer can designate a new address to receive the change.[193]

[192] We simplify here a little bit. Under normal circumstances, this transfer would be only the last transfer out of many.
[193] WU at all., Ibid. 189, at 4

As such if Person A decided to initiate the transaction to Person B, who requested 0.8 bitcoin, Person A will broadcast information in the input of the transaction that she is sending 1 bitcoin, which shall split to 0.8, which will be addressed to person B and 0.2 which will be addressed back to Person A.

In case the situation would be different and Person A's bitcoin value structure would be represented by 6 times 0.2 bitcoin. Then the input would involve information that 4 0.2 bitcoin should merge into exactly 0.8 bitcoin, but the data structure of the transaction would involve four 0.2 bitcoin origin events.

The last component input must involve is the digital signature of rightful owner (possessor) of the digital assets to be transferred. This digital signature is represented by a private key. Private key allows the sender to validate the transaction and prove to the network such sender has the right to spend the Digital Assets.

Output then contains data (information) about the number of Digital Assets being transferred (rights to spent them) the localization data, such as the address of the receiving party. Transaction output will serve as a transaction input for the subsequent transaction relating to those Digital Assets.[194]

[194] EMERY, Jules a Matthieu LATAPY. Full Bitcoin Blockchain Data Made Easy. 2021 IEEE/ACM International Conference on Advances in Social Network Analysis and Mining (ASONAM 2021) [online]. Netherlands, 2021, 1-16 [cit. 2022-04-19]. Available at: https://hal.archives-ouvertes.fr/hal-03443053/document (Archived version available via: https://archive.ph/P5KUW)

4.3.3. Blockchain's Elements – asymmetric cryptography and localization points.

4.3.3.1. Asymmetric cryptography

One of the key elements common to Blockchains is the Asymmetric Cryptography[195]. We have already introduced its basics in the history chapter, while talking about David Chaum's eCash. Nevertheless, we can provide synthesis of the basics for this part of the Thesis as the asymmetric cryptography is responsible for verification of transactions by digital signatures and for verification of such digital signatures by public key.[196] Further, it allows for creation of directories – blockchain to and from points.[197]

Particular part of cryptography (encryption) can be divided between symmetric and asymmetric. Both symmetric and asymmetric cryptography is based on so called keys. Those keys are used encrypting and decrypting information (data). Symmetric-key algorithms are cryptographic algorithms that use the same cryptographic keys for both encryption and decryption.[198] Whereas, the asymmetric cryptography uses a key pair consisting of public and private keys.[199] The public key can be shared with a third party without compromising the security. Private key, however, must be kept in secret.

---

[195] Y. Xinyi, Z. Yi and Y. He. Technical Characteristics and Model of Blockchain 2018 10th International Conference on Communication Software and Networks (ICCSN), 2018, pp. 562-566, [cit. 2022-04-19]. Available at: https://ieeexplore.ieee.org/abstract/document/8488289 (Archived version available via: https://archive.ph/TS6jB)

[196] YAGA., Ibid. at 164

[197] Id.

[198] HENRIQUES, Michelle a Nagaraj VERNEKAR. Using symmetric and asymmetric cryptography to secure communication between devices in IoT. 2017 International Conference on IoT and Application (ICIOT) [online]. 19 October 2017n. l., 1-4 [cit. 2022-04-19]. Available at: https://ieeexplore.ieee.org/abstract/document/8073643 (archived version available via: https://archive.ph/574QF)

[199] JIRWAN, Nitin, Ajay SINGH a Sandip VIJAY. Review and Analysis of Cryptography Techniques. International Journal of Scientific & Engineering Research [online]. 2013, 4(3), 1-6 [cit. 2022-04-19]. Available at: https://d1wqtxts1xzle7.cloudfront.net/44421110/Review_and_Analysis_of_Cryptography_Tech20160404-17928-1wutbod-with-cover-page-v2.pdf?Expires=1650387017&Signature=fl7AWaGnt00tsn-Bq-s-aGffQCY~66q1lOCUbLwi7diksMmgrV3tXAvimZvKNqMsAVSd0uSOx5NcFeKxubZoIiE4w1iTQ2YQfwUJzASPxYLMWLn2chfV-em-GT9hBvgEyJxSgBeFj6v7hbfmk-7IScbq1ZBUFuQGTe1dtcOVxSQLd9GkPKdgEO8keKYYkFja~nGdeELNbd00MAavjJvH~fH9Y7ifOCjBnuQlORe5o86bVIH38SxECN1p0jnSEIdPR-ylW6k5eMq9cln84uJM9vrxeAFUdahIvAg7fmvlcmP-zs08R8G-iZD3tpjbs8fe6aYSUAYpDIqUluEI7TBN7A__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (Archived version available via: https://archive.ph/wip/2WySo)

Each type of the above-mentioned cryptography is better suited for a different type of communication. In an environment where the participants know each other, and therefore the level of trust among such participants is higher a symmetric cryptography may be sufficient. However, in blockchain environment, especially in permissionless blockchains the users do not know each other and the level of trust between them is very low.

For such environment the asymmetric cryptography is suited better. As the participant have two keys at their disposal, they can act without trusting each other. In practice and simplified a transaction on Bitcoin's blockchain can be described in a following fashion.

Person A and Person B are both users of Bitcoin's Blockchain. Person A possesses 10 bitcoins and Person B possesses 5 bitcoins. Person A holds her bitcoins in a bitcoin address X. Person B holds her bitcoins in address Y. Person A wants to satisfy her obligation, which she holds against Person B. The obligation is in the amount of 1.35 bitcoins. Person A is interested in sending 1.35 bitcoins to Person B.

Before Person A can send the bitcoins to person B, person A needs to know, where (to which account) she should send the bitcoins. As explained in greater details below, the public key basically serves as bitcoins address. Address then can be used as a reference point to receive bitcoins. Therefore, the first thing Person B is going to do is to inform Person A about her address. In other words, Person B will provide her public key to person A. Person B will therefore inform Person A that her address is Y.

Person A now knows Person B's public key (Y), which holds 5 bitcoins. However, since Person A does not know Person B's private key, she is unable to handle the bitcoins in address Y. In essence, anyone can know Person B's address (public key), because without private key no one is able to do anything with its contents. In this example the knowledge of Person B's public key only allows to receive transactions to address Y.

The situation with Person A is different. In order to send bitcoins, she must use her private key. This private key is mathematically interconnected with her address X and it is essential Person A does not tell it to Person B. Should Person A make the private key publicly available everyone would be able to use it and transfer all the contents of her address X.

Person A then creates a transaction with the amount of 1.35 bitcoins. We have already established the contents of typical transaction above, but for the purpose of this example, imagine the output here simply reads: "Person A sends 1.35 bitcoins to Person B's address Y". Before Person A sends the transaction, she uses her private key to encrypt the message. Creating the outcome of "CCH5655".

For the important part, the Bitcoin protocol (rather its nodes) can verify the outcome of CCH5655 using Person A's public key, whether it was actually her who have signed the transaction to Person B. The Bitcoin's protocol allows for verification using the outcome CCH5655 as a reference. It will combine Person A's public key, the data in transaction (Person A sends 1.35 bitcoins to Person B's address Y) and the outcome CCH5655 to verify, whether it was really Person A who initiated the transaction. So, in other words, the private key in this scenario allows for generation a unique outcome (signing transaction), the public key allows anyone to verify the unique outcome origin.

4.3.3.2. Localization points in Blockchain

Blockchains associated with digital assets use so called addresses to create reference points. Those reference points then allow for targeting the digital asset transfers.[200] Address itself looks like a string of random digits. In example Bitcoin address looks like this: 1Feik8opcZepiCLTWdFDkq5Ln4AqqgA5hK. Each address is unique, and all of the addresses are created at the inception of given Blockchain.[201]

In fact, it is again the Hash function, which allows for creation of the address string. Address string is derived from the corresponding public key.[202]

4.3.4. Blockchain's Elements – the blocks.

The concept of Blockchain was conceived in order to deal with ongoing influx of data. The incoming data to Blockchain are divided into packages of fixed size. Those packages are called blocks. Those blocks are then mutually interconnected forming a virtual chain. This chain can be endlessly[203] extended by addition of new data packages (blocks).

Each block can contain any type of data. In case of Digital Assets, the majority of the block data is represented by transactions in corresponding network. The data in a block can be divided as utility data and the block data. The purpose of utility data, which are located in the block header is the functioning of the Blockchain. The utility data most commonly involve[204]:

---

[200] BODZIONY, Norbert, Paweł JEMIOŁO, Krzysztof KLUZA a Marek OGIELA. Blockchain-Based Address Alias System. Journal of Theoretical and Applied Electronic Commerce Research [online]. 2021, (16), 1280-1296, at 1283 [cit. 2022-04-19]. Available at: https://www.mdpi.com/0718-1876/16/5/72/htm (Archived version available via: https://archive.ph/ 5r1on)

[201] Id. at 1283

[202] RAHALKAR, Chaitanya a Anushka VIRGAONKAR. Summarizing and Analyzing the Privacy-Preserving Techniques in Bitcoin and other Cryptocurrencies [online]. 1-11 [cit. 2022-04-19]. Available at: https://arxiv.org/pdf/2109.07634.pdf (Archived version available via: https://archive.ph/rJAyJ)

[203] At least in theory. Practically the data storage could be a problem in future. Yet, given the pace the data storage availability is growing, it will be an unlikely problem.

[204] SWANSON, Tim. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems [online]. April 6, 2015, 1-66 [cit. 2022-04-14]. Available at: https://allquantor.at/blockchainbib/pdf/swanson2015consensus.pdf (Archived version available via: https://archive.ph/rXdGG)

1. The block number, or block height. Height is the number of the block, which presents the block's order.[205]
2. Hash value of the previous block utility data (block header).
3. Hash value of the block data.
4. Timestamp.
5. The data size of the block.
6. The nonce value. Nonce is a random number, which is added for possible verification of the block.[206]

The fact that data inside blocks are hashed is very important. Each new block contains the hash of the data inside of the latest timestamped block. In other words, a new block (child block) contains the information from the previous block (parent block). As we have explained in previous chapter, any modification of just a single digit inside a data package would change the output hash to a completely different value. Therefore, by having the data hashed their integrity is insured. A theoretical alternation of data contained in a block already attached to the chain is therefore impossible as all the subsequent blocks would be suddenly based on a wrong hash value, which would subsequently change the hash value in all the subsequent blocks due to its interconnections.[207].

In the Bitcoin's Blockchain the transaction data (block data) are not added to Blockchain right as the transaction happens, rather the addition happens in a given timeframe. In Bitcoin's

[205] MA, Guangkai, Chunpeng GE a Lu ZHOU. Achieving reliable timestamp in the bitcoin platform. Special Issue on Security and Privacy in Machine Learning Assisted P2P Networks [online]. 13 May 2020, (13), 2251–2259 [cit. 2022-04-14]. Available at: https://link.springer.com/content/pdf/10.1007/s12083-020-00905-6.pdf (Archived version available via: https://archive.ph/XA0d0)

[206] NOFER, Michael, Peter GOMBER, Oliver HINZ a Dirk SCHIERECK. Blockchain [online]. Springer Fachmedien Wiesbaden 2017, 2017, 20 March 2017, 183 - 187 [cit. 2022-04-14]. Available at: https://link.springer.com/content/pdf/10.1007/s12599-017-0467-3.pdf (Archived version available via: https://archive.ph/ZNJFD)

[207] The network would simply notice such change and would not allow for the modification.

Blockchain such timeframe is about 10 minutes long[208]. The timeframe is of course fully programmable and in a different Blockchain the timeframe can be shorter (in seconds) or longer as needed.

The addition of new block is one of Blockchain's crucial features as there must be consensus within the network, whether such addition is valid. In classic systems, such consensus would be delegated to a trusted third party. To dispose of trusted third party Blockchain implements a proof of work or other consensus mechanism - game theory-based competition.[209] Proof of work concept can be among others also used as a mechanism to reach consensus.

4.3.5. Blockchain's Elements - Consensus mechanisms

As briefly argued above, in a database managed in classic centralized way, a trusted third party would review the state of the database, maintain it, and update it as needed. In public[210] Blockchains (permissionless blockchains) a more democratic solution is applied, and the single authority concept is abandoned for the benefit of distributed authority.

The consensus mechanism is then used to decide various matters. Generally speaking, it is a method used to keep information consistent.[211]Specifically, the Consensus Protocol can be used for processing transactions on the blockchain. Further, it can be used for voting or for creating new digital assets.

---

[208] KIM, Suah, Beomjoong KIM a Hyoung KIM. Intrusion Detection and Mitigation System Using Blockchain Analysis for Bitcoin Exchange [online]. Singapore: Association for Computing Machinery, October 29–31, 2018, 1-5 [cit. 2022-04-14]. Available at: https://www.researchgate.net/profile/Suah-Kim-3/publication/330205979_Intrusion_Detection_and_Mitigation_System_Using_Blockchain_Analysis_for_Bitcoin_Exchange/links/5e686005299bf1744f72cd20/Intrusion-Detection-and-Mitigation-System-Using-Blockchain-Analysis-for-Bitcoin-Exchange.pdf (Archived version available via: https://archive.ph/Yxir1)

[209] Liu ZIYAO, Luong NGUYEN CONG, Wang WENBO, Niyato DUSIT, Liang YING-CHANG a Kim DONG. A Survey on Applications of Game Theory in Blockchain [online]. IEEE, 15 March 2019 [cit. 2022-04-14]. Available at: https://arxiv.org/pdf/1902.10865.pdf (Archived version available via: https://archive.ph/xEBcr)

[210] As explained below.

[211] ZHU, Xingxiong. Research on blockchain consensus mechanism and implementation. IOP Conference Series: Materials Science and Engineering [online]. 2019, 1-6 [cit. 2022-04-20]. Available at: https://iopscience.iop.org/article/10.1088/1757-899X/569/4/042058/pdf (Archived version available via: https://archive.ph/vlMKd)

Any consensus mechanism faces certain challenges. The first problem is that the parties who are supposed to reach a consensus about an issue (state of the blockchain) usually do not know each other. Second, since such parties do not know each other, they likely do not trust each other and their acts. Third, it is likely that under such conditions any party will work only for her benefit, not for the benefit of the group. Therefore, any consensus mechanism must employ a way how to motivate and enforce users to act towards common goal. A consensus mechanism is a process in which a majority (or in some cases all) of network validators [nodes] come to agreement on the state of a ledger.[212] It represents a set of given rules that decides on the legitimacy of contributions made by the various participants (i.e., nodes or transactors) of the blockchain.[213]

The very basic motivation behind any consensus mechanism must appeal to any individual participating (node) within such network. Therefore, the chosen motivation is, of course, monetary. Further, to persuade the participants to work together or rather to follow the same goal, the monetary reward is accessible only through a fair competition. The goal of such competition can be in example the solution to mathematical equation. The first person to reach that goal will be rewarded by the protocol. As such, the protocol equally motivates all participants to take part in said competition. The participants are then essentially working towards the same goal, without the need to trust each other.

On important note, the blockchain protocol allows for mutual supervision between its users. Any blockchain user is able to verify the state of blockchain by herself by checking the results of said competition. However, for the main part the supervision is done automatically by the protocol itself. In case the provided solution would be incorrect, the protocol allows for its dismissal and the competition will continue.

[212] SWANSON., Ibid. at 204

[213] MANSA, Julius. Consensus Mechanism (Cryptocurrency). Investopedia.com [online]. 2021 [cit. 2022-04-14]. Available at: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp (Archived version available via: https://archive.ph/6a8TR)

4.3.5.1. Sybil Attack

Most consensus protocols also solve other issue associated with digital identities – the Sybil attack. "*Sybil attacks [are attacks] in which a small number of entities counterfeit multiple identities so as to compromise a disproportionate share of the system*".[214] The premise for this attack is that unless a central authority is verifying whether the digital entity is unique, anyone (a single entity) can create as many digital identities as possible and subsequently abuse them to gain unfair advantage in the network. To the network each fake entity will look like a normal participant, while all the fake entities will be governed by a single real entity.

An example of Sybil attack may be something very common such as a review at the Amazon website. An entity can create a large number of accounts, which then give selective negative reviews to products sold on the platform. Usually, to create a better standing for concurrent product. Similarly, a large number of fake accounts on the Facebook social network can commit Sybil attack, by spreading misleading information.

The term Sybil attack was first coined by J.R. Douceur. While describing it, Douceur added that without a central authority this problem is hardly solvable in peer-to-peer networks.[215] However, he also proposed a theoretical solution at that time[216]. "*This approach entails the following conditions:*

1. *All entities operate under nearly identical resource constraints.*
2. *All presented identities are validated simultaneously by all entities, coordinated across the system.*

[214] DOUCEUR, John R. The Sybil Attack. In: DRUSCHEL, Peter, Frans KAASHOEK and Anthony ROWSTRON. Peer-to-Peer Systems. Cambridge, MA, USA, March, 2002. pp. 251-261 Available also at: https://link.springer.com/content/pdf/10.1007/3-540-45748-8.pdf (Archived version available via: https://archive.ph/xUeFe)

[215] Id. at 5

[216] The article is from the year 2002 and at that point of time some solutions were unpractical, or not really possible yet.

3. *When accepting identities that are not directly validated, the required number of vouchers exceeds the number of system-wide failures.*

We claim that in a large-scale distributed system, these conditions are neither justifiable as assumptions nor practically realizable as system requirements."[217]

The consensus protocols have solved the Sybil Attack, by requiring every participant to expend resources. Therefore, honest participant or dishonest (fake entity) must both invest resources in the network. Mere existence does not give any advantage. In example in the Proof of Work based consensus protocols the nodes have to spend a computational power to participate in the network. To have any influence each fake entity would have to expend at detrimental amounts of resources and would be still working towards the same goal as honest entities. In Proof of Stake consensus mechanism each entity is required to possess some Digital Assets to have influence. Thus, even the fake entities would have to hold Digital Assets, which again makes it prohibitively expensive to conduct the Sybil Attack.

4.3.5.2. Proof of Work based Consensus Mechanism

While there are many different types of consensus mechanisms, the above-mentioned properties should be mutual to all of them. This solution allows for the absence of intermediary, who would normally be needed to authoritatively decide.

When Bitcoin was introduced, the Consensus Mechanism its Blockchain was using, was based on Proof-of-Work concept. Over the time, different Consensus Mechanisms were introduced. In example in 2012 Peercoin introduced other quire popular solution - the Proof of Stake Consensus Mechanism.[218] Each of its type may be suited better for a different type of Blockchain.

[217] Ibid. at 5

[218] KING, Sunny a Scott NADAL. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake [online]. 2012 [cit. 2022-04-20]. Available at: https://whitepaper.io/document/139/peercoin-whitepaper (Archived version available via: https://archive.ph/l2Mvp)

In example in Permissionless Blockchains it may be better to use Proof of Work Consensus Mechanism, as it requires no trust between participants.

Proof of Work Consensus Mechanism is associated with Digital Assets from their very beginning. It was first used by Satoshi Nakamoto in Bitcoin.[219] To this date it remains popular and widely used solution by other Digital Asset's Blockchains.[220]

As we have explained in the historic chapter, Proof of Work essentially proves that someone has spent computational power. In Proof of Work based Consensus Mechanism the node is required to solve a resource expensive mathematical operation. This process is often called mining. The first node to solve the mathematical operation is then allowed to post a new block.

The mathematical operation is designed in a way, which makes it very hard to solve, but very easy to verify, whether the solution was correct.[221] In other words, it is: "Easy to verify, but difficult to find."[222] Usually the concept is that the actual mathematical operation is very easy but has to be carried over and over. The difficulty of the mathematical operations can be decreased or increased as necessary. The actual number of operations taken by the nodes is too high in order to be fully appreciated. In March 2018, about 26 quintillion (26.000.000.000.000.000.000,00) hashing operations (attempts to solve the mathematical equation) were conceived every second.[223] The nodes are using a brute force approach, which

[219] NAKAMOTO., Ibid. 58.
[220] BAINS, Parma. Blockchain Consensus Mechanism: A primer for Supervisors [online]. International Monetary Fund, 2022, (Note 2022/003), 1-26 [cit. 2022-04-20]. Available at: https://www.elibrary.imf.org/downloadpdf/journals/063/2022/003/063.2022.issue-003-en.xml (Archived version available via: https://archive.ph/OKy0E)
[221] YAGA at all., Ibid. 164
[222] SRIMAN, B., GANESH, Kumar and SHAMILI, P. Advances in Intelligent Systems and Computing: Intelligent Computing and Applications Proceedings of ICICA 2019, in Blockchain Technology, Consensus Protocol Proof of Work and Proof of Stake [online]. Springer Nature Singapore Pte, 2021, 1-781, at 396 [cit. 2022-04-20]. ISBN: Available at: https://www.researchgate.net/profile/Saroj-Kumar-22/publication/345005910_Intelligent_Monitoring_of_Bearings_Using_Node_MCU_Module/links/6128 6be70360302a005f4941/Intelligent-Monitoring-of-Bearings-Using-Node-MCU-Module.pdf#page=395 (Archived version available via: https://archive.ph/CllcR)
[223] VRIES, Alex. Bitcoin's Growing Energy Problem. Joule [online]. Elsevier, 2018, May 16, 801-809 [cit. 2022-04-20]. Available at :

is very energetically demanding. Using Bitcoin as an example again, its electricity consumption is equal to Poland as of 2022.[224]

Proof of work uses two motivators to keep the participating nodes honest. Both of the motivators are monetary. Once participating node solves the mathematical operation and the rest of the network verifies that the solution was correct. The solving node is able to add a new block to the Blockchain. The data contents of such block are transactions that the node picked up from a pool of unconfirmed transactions. Those transactions are sorted by a transaction fee.[225] The higher the fee, the sooner the transaction is going to be picked up by a node.

The node, who solved posed mathematical operation will be awarded predefined number of Digital Assets. In example, on Bitcoin's blockchain the current reward for adding a new block is 6.25 bitcoins.[226] Additionally, the node will be awarded all the fees associated with the transactions such node has confirmed.

The practical solution in Proof of Work consensus protocol based on Bitcoin is very similar to the concept described in Bit Gold. The mathematical operation Bitcoin Nodes are trying to solve is also looking for a "valid" hash puzzle similar to Bit Gold. Once more the nodes are looking for a value that starts with a certain number of zeros. The nodes combine the nonce (as described above) and data from blockchain looking for a valid result on try and fail basis. In fact, the nodes are changing the nonce to find the valid hash, so technically the nodes are trying to guess the nonce.

---

https://reader.elsevier.com/reader/sd/pii/S2542435118301776?token=5EF3950165D72642454B31509AAB1C623722D6D5D43DA64494C534E31A92DEFF030114FF34EAA018F8620DCFE2EDD95C&originRegion=eu-west-1&originCreation=20220420210056 (Archived version available via: https://archive.ph/1Hms6)

[224] BAINS., Ibid. 220

[225] On most Blockchains associated with Digital Assets, the users are allowed to choose the transaction fee. In some cases, there is a coded minimum, but usually the user is able to choose 0 fee. Choosing higher fee should allow for a faster confirmation time, as the transaction will be selected in preference by the participating nodes.

[226] HAMDY, Abdulrahman. Explaining the Bitcoin Block Reward. Argoblockchain.com [online]. 2022 [cit. 2022-04-20]. Available at: https://argoblockchain.com/articles/explaining-the-bitcoin-block-reward (Archived version available via: https://archive.ph/iiZML)

Again, similar to Bit Gold, to offset the advances in computing power, the number of zeros can increase to raise the difficulty. Each increase in the number of zeros raises the difficulty substantially. In an experiment, the authors[227] describe that looking for a valid hash starting with "000000" it took a normal computer hardware about 11 million tries.[228] Looking for a hash starting with "0000000", with one more zero, the same hardware had to compute over 930 million separate tries.[229]

The Bitcoin protocol steadily raises the difficulty to keep the nodes finding solution about every 10 minutes, to keep the pace of 6 posted blocks every hour. The block is posted every time a node finds a correct nonce which in combination with the blockchain data gives the value of the correct hash.

It is worth mentioning that since the difficulty have risen so much that a normal computer does not have an actual chance of solving the issues. Nodes have started to unite in so called pools. In those pools the nodes share their computing power and invest it to solve the mathematical operation. Those mining pools are actually a Czech invention. If the pool is the first to solve the mathematical operation the node from the pool finding the solution will receive the reward, which will be then split among all of the participants of said pool based on the computing power they have invested. Since the pools usually split the work among the nodes according to certain rules, in example, 10% of the power of the nodes are looking for the first 10% possible nonce values, the mining is more effective than a single entity. Quoting the above-mentioned experiment in case of using a pooled computation power the 7 zeros has was found with "only" 90 million guesses. That is 1000% more effective than the single entity.

[227] YAGA., Ibid 164, at 20
[228] Id.
[229] Id.

4.4. Blockchain Technology stage of developments impacts

As of 2022 there are three generally recognized stages of Blockchain development. This division takes into account not only the technological aspect but also its influence on society. Those stages are aptly named Blockchain 1.0, Blockchain 2.0, and Blockchain 3.0.

With each stage the involvement of Blockchain in society grows. "The application of blockchain technology has extended from digital currency and into finance, and it has even gradually extended into health care, supply chain management, market monitoring, smart energy, and copyright protection."[230] Therefore, Blockchain 1.0 is said to represent the Digital Assets, Blockchain 2.0 then represents (financial) digital economy and Blockchain 3.0 shall grow to represent the digital society.[231]

4.4.1. Blockchain 1.0

As the name suggests, Blockchain 1.0 is the first generation and application of Blockchain technology.[232] We have basically described the whole Blockchain 1.0 stage above. This stage referrers to the creation of the intermediary-less payment system technology. "[Blockchain 1.0] refers to the underlying technology platform (i.e. mining, hashing, and the public ledger), the overlying protocol (i.e. transaction enabling software), and the [D]igital [Assets] (i.e. bitcoin or other digital tokens/coins) which represent a store of value as well as provide value to the protocol Itself."[233]

[230] XU, Min, Xingtong CHEN a Gang KOU. A systematic review of blockchain. Financial Innovation [online]. 2019, 5(27) [cit. 2022-05-08]. Available at: https://jfin-swufe.springeropen.com/articles/10.1186/s40854-019-0147-z (Archived version available via: https://archive.ph/GmSHn)

[231] EFANOV, Dmitry a Pavel ROSCHIN1. The All-Pervasiveness of the Blockchain Technology. 8th Annual International Conference on Biologically Inspired Cognitive Architecture, BICA [online]. 2018, 2018(123), 116-121 [cit. 2022-05-08]. Available at: https://reader.elsevier.com/reader/sd/pii/S1877050918300206?token=67C1D0ED992D918DEFCD6A4610C20160D3BE62479397C5805FDDBF51AC775EC013E60A1FAA63B4F9B6B40C77162C38D2&originRegion=eu-west-1&originCreation=20220508202227 (Archived version available at: https://archive.ph/PTE86)

[232] Id.

[233] Id.

Once again, the typical representant of Blockchain 1.0 is Bitcoin. However, other Digital Assets such as Litecoin[234] or DigiByte[235] could be used as prime examples. The comparative principle here is that those Digital Assets were only able to transfer value among its participants. No other specific functions would fit under the umbrella of Blockchain 1.0. Nevertheless, the trustless and decentralized aspects of the value transfer was completely new, sufficient enough to achieve its own category. For the sake of completeness this category has financial aspects.

4.4.2. Blockchain 2.0

Blockchain 2.0 is also a category, which resembles certain financial aspects. It refers to the penetration of Blockchain technology into areas, which have long established existence, but the addition of Blockchain technology makes them more effective. To give a financial example - supply chain finance, securities trading, banking instruments, payment clearing, establishing credit systems and other.[236] In other words, Blockchain 2.0 partly refers to the actual application of Blockchain technology to current areas of human development.

However, the Blockchain 2.0 also refers to the development of Blockchain based technology itself. "*Some of the terminology that broadly refers to the Blockchain 2.0 space can include Bitcoin 2.0, Bit- coin 2.0 protocols, smart contracts, smart property, Dapps (decentralized applications), DAOs (decentralized autonomous organizations), and DACs (decentralized autonomous corporations).*"[237] Therefore Blockchain 2.0 also encompasses the niche economy that revolves around the Blockchain technology.

[234] For more information please see: DigiByte Community Infopaper [online]. 2014, 1-17 [cit. 2022-05-08]. Available at: https://digibyte.org/docs/infopaper.pdf (Archived version available via: https://archive.ph/Cp0Rw)
[235] For more information please see: The Cryptocurrency for Payments: Based on Blockchain Technology [online]. [cit. 2022-05-08]. Available at: https://litecoin.org (Archived version available via: https://archive.ph/Jy7nw)
[236] XU at all., ibid 230
[237] SWAN, Melanie. Blockchain: Blueprint for a New Economy. USA: O'Reilly Media, 2015 pp 152(9). ISBN 978-1491920497.

4.4.3. Blockchain 3.0

Blockchain 3.0 is the most futuristic outlook on the Blockchain technology. Blockchain 3.0 is not directly related to finance per se, rather it should encompass the whole world. Authors assume that the technology will become integral part of human life. "It focuses on the regulation and governance of blockchain-based decentralization in every aspect of society."[238] "Blockchain 3.0 is a blueprint for popularizing the technology in fields other than cryptocurrency and finance, such as government, health, science, culture, and the arts."[239]

The futuristic outlook should be focused on trust. Blockchain 3.0 implementation should introduce the blockchain trustless-ness into so called system trust and subsequently replace the need for personal trust. System trust is a known concept of impersonal and indirect transactions, whereas personal trust is simply a bond between two know actors.[240] Nowadays, economic participants have minimal information about their transaction partner, yet most of the transactions are successful as the system is somehow working. Blockchain 3.0 society should be able of completely trustless yet functional economic interaction in all life aspects.

4.4.4. Synthesis

For the purposes of this Thesis, we are going to focus only on the Blockchain 1.0 aspects. Therefore, we are interested in the functionality of the Digital Assets that strive to provide monetary and investment functions.

[238] CHENG, Hsing Kenneth, Daning HU a J. Leon ZHAO. The landscape of Blockchain research: impacts and opportunities. Information Systems and e-business Management [online]. 2021, 749-755 [cit. 2022-05-09]. Available at: https://link.springer.com/article/10.1007/s10257-021-00544-1 (Archived version available at: https://archive.ph/Qfd3W)

[239] SWAN., Ibid 237.

[240] Based on the division established by Niklas Luhmann in Luhmann N (1968) Trust and power. John Wiley & Sons

5. Digital Assets in General Practice

5.1. Introduction

Thus far, we have written about the historic and technical aspects of Digital Assets. This part we dedicate to the actual use of Digital Assets, which then present a mix of social, theoretical, and also legal aspects.

This chapter is based on a few case studies[241], which all are mainly focused on the criminal abuse of Digital Assets. In this chapter we further address three of our research questions. The first one is what is the actual use of Digital Assets. Using this question, we are trying to present a case that the technology behind Digital Assets, the whole environment, but also dedicated services helps and even incentivizes criminals educated in computer science to carry out different financially related crimes. For this purpose, we are introducing the current Digital Asset environment and also certain aspects (characteristics) of Digital Assets that in our opinion serve best to its illicit use.

Further, we also address in this chapter the question whether Digital Assets and associated services used or abused for criminal activity. We are evaluating whether the Digital Assets services are developed intentionally to facilitate crimes. In this connection we present two main areas, we are introducing the so-called Dark Web Online Marketplaces, which are built with purpose to provide access to illegal substances and other illegal goods and the Digital Assets play a major role as a medium of exchange in such services. Additionally, we present the case of the abuse of Digital Asset Exchanges. Where we evaluate whether such abuse in relation to the Digital Asset Exchange service providers is intentional or whether such exchange is just caught in the middle of such crimes and their services are plainly abused.

[241] This part of the Thesis is based on our articles we have written mainly in 2018 and 2019 and thus provides a valuable inside into the use of Digital Assets before any comprehensive regulation took place. We have also revised some part to reflect the current approach.

Once we present the above-mentioned cases, we are also looking at the integration of Digital Asset under certain areas of law. We are thus looking at the approach of United States regulators. At the last part of the last section, we also highlight the issues of such approach and voice our opinion.

5.2. The broken promise of Digital Assets?

We have been involved with Digital Assets since 2013 as we have already mentioned in the introduction to this Thesis. Since then, but even before that Digital Assets embodied an immense technological promise to revolutionize payments (Blockchain 1.0), most of the other financial services (Blockchain 2.0), and in the end the whole society (Blockchain 3.0). The presence of the spirit of this revolutionary promise was definitely more obvious 9 years ago but it is still here. Blockchain and even Digital Assets are a revolution happening.

According to us, one of the Digital Assets most prominent promise was the financial inclusion. "*Blockchain technology can play a pivotal role when it comes to boosting financial inclusion toward the unbanked and underbanked, and there are significant opportunities on the horizon.*"[242] Quite large part of world's population is still unbanked or underbanked. "*Globally, about 1.7 billion adults remain unbanked—without an account at a financial institution or through a mobile money provider.*"[243] For those less fortunate people Digital Assets can represent a shortcut to twenty first century. Especially, as internet coverage is becoming

[242] LICHTFOUS, Marco, Vivek YADAV a Valentina FRATINO. Can blockchain accelerate financial inclusion globally? Inside Magazine [online]. 19(02) [cit. 2022-05-29]. Available at: https://theblockchaintest.com/uploads/resources/Deloitte%20-%20Can%20Blockchain%20Accelerate%20financial%20inclusion%20globally%20-%202019.pdf (Archived version available via: https://archive.ph/4ZUWQ)

[243] DEMIRÜÇ-KUNT, Asli, Leora KLAPPER, Dorothe SINGER a Jake HESS. The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution [online]. 2018 [cit. 2022-05-10]. ISSN 978-1-4648-1268-2. Available at: https://globalfindex.worldbank.org/sites/globalfindex/files/chapters/2017%20Findex%20full%20report_chapter2.pdf (Archived version available via: https://archive.ph/K2Mw7)

more accessible in less developed areas such as Middle East and Africa via Satellites.[244] Yet it seems that the society at large cares less about the above-described revolution. The users of Digital Assets now sidelined this revolution and exchanges if for a different promise. The promise to get rich and get rich quick.

The practice and approach to the Digital Asset is often described as follows: "*The "computer generation" sees crypto as an easy game that can be quickly profited from*"[245]. The numbers (see below) support this opinion. For most people Digital Assets represents the above-mentioned get rich quick scheme not a payment or societal revolution.

With time it was becoming clear to us that majority of Digital Assets are (unregulated) purely speculative assets in the colloquial sense. Further, we have shaken off the universal aura of Digital Asset's elusive promise to revolutionize payments. Interestingly not because the promise is a lie, it is because apart from a relatively small number of users, no one uses Digital Assets to carry out payments as we have shown above.

In our opinion, this does not motivate the developers to create actual payment systems and thus most of the new projects on the Digital Assets scene are only copies of each other aiming for monetary gain. Nevertheless, since Digital Assets are still a shiny new technology that sounds sophisticated, promising, thus it attracts large sums of money.

[244] GRAYDON, Matthew a Lisa PARKS. 'Connecting the unconnected': a critical assessment of US satellite Internet services. Media, Culture & Society [online]. SAGE, 2019, 1-17 [cit. 2022-05-29]. [online]. Available at: shorturl.at/fgmFJ (Archived version available via: [cit. 2022-05-29].

[245] Authors' translation from the Czech original "Počítačová generace" totiž krypto vnímá jako hru, na které lze snadno a dobře vydělat." Peníze a vzrušení ze hry. Mladé od kryptoměn neodrazují ani nekončící série krachů. Aktualne.cz [online]. [cit. 2022-05-22]. Available at: https://zpravy.aktualne.cz/finance/penize-hra-a-vzruseni-mlade-obchodniky-od-kryptomen-neodrazu/r~ce6a57c2d74b11eca873ac1f6b220ee8/?utm_source=www.seznam.cz&utm_medium=sekce-z-internetu (Archived version available via: https://archive.ph/foDbH)

5.2.1. The endless influx of money?

For the last 10 years Digital Assets are witnessing constant influx of money. Each cycle the market grows to new unprecedented and illogical heights. Which means that even more money is being poured in the Digital Assets and it seems that the money attracts more money. Creating sort of a bubble. Some even consider the whole Digital Asset economy to be a Ponzi scheme: "*[Digital Assets are] not merely a bad investment or speculative bubble, but something more akin to a decentralized Ponzi scheme"* [246]. Nevertheless, the money keeps flowing in, somehow recklessly.

At the beginning of 2018 Bitcoin was enjoying once again unprecedented interest from general public, soaring in its value to its new peak, reaching close to $20,000.00.[247] Just to subsequently keep losing value over the next year and half[248]. Reaching the bottom in under $4,000.00.[249] Then, as of May 2019, Bitcoin itself was again on the raise. The whole Digital Assets market had predominantly upward trend until November 2021, when the cycle has switched, and another decline has begun.[250] At the peak of the 2021 market growth (November 10, 2021) Bitcoin as the most valuable Digital Asset has reached value of $69,044.77.[251]

When another Bitcoin run began in the second half of 2019, we were already sort of skeptical. As the extreme valuation of Bitcoin and other Digital Assets simply does not make any sense. We also came across a study from the same year, which have shown that only 1.3% of the global

[246] ANDRUS MORTAZAVI, SOHALE. Cryptocurrency Is a Giant Ponzi Scheme. Jacobinmag.com [online]. [cit. 2022-05-30]. Available at: https://www.jacobinmag.com/2022/01/cryptocurrency-scam-blockchain-bitcoin-economy-decentralization (Archived version available via: https://archive.ph/5aYgz)

[247] From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited Coin Desk, Available at: https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited (last visited Jun 3, 2019) (Archived version available via: https://archive.ph/mkxzp)

[248] Bitcoin to USD Chart. Coinmarketcap.com [online]. [cit. 2022-05-08]. Available at: https://coinmarketcap.com/currencies/bitcoin/ (Archived version available via: https://archive.ph/tZKaI)

[249] Ibid.

[250] Bitcoin Price Chart (BTC). Coingecko.com [online]. [cit. 2022-05-16]. Available at: https://www.coingecko.com/en/coins/bitcoin (Archived version available via: https://archive.ph/ZMzFY)

[251] VACA, Inigo. While Bitcoin price starts 2022 with a slump, mining difficulty is on the rise. Cointelegraph.com [online]. [cit. 2022-05-29]. Available at: https://cointelegraph.com/news/while-bitcoin-price-starts-2022-with-a-slump-mining-difficulty-is-on-the-rise (Archived version available via: https://archive.ph/8Uit4)

volume of Bitcoin comes from the trade with merchants.[252] Those numbers seem relevant even in 2022, as the World Bank has published a very detailed working paper focusing on the use of Digital Assets.

This World Bank's paper evaluates whether Digital Assets are used predominantly as a risk asset rather than anything else.[253] While finding that Digital Assets are indeed used as a risk asset, it also highlights that out of all of the transactions that took place within Bitcoin network only 7 percent[254] reflects its use in domestic transaction and international payments.[255] Out of this 7 percent 20 percent then counts for international payments.[256]

While investing fiat money in Digital Assets was predominantly the domain of retail investors. Corresponding with the 2019 investment wave even the wholesale professional investors began to invest large sums of money. In example the American corporation MicroStrategy Incorporated owned (as of 2021) 129 218 bitcoin worth of billions.[257] Similarly, the automotive corporation Tesla, Inc. made initial investment worth of about 1.5 billion in early 2021, and still keeps the bitcoins.[258] Yet, it seems that nobody really uses them for payments. Is therefore the whole

[252] KHARIF, Olga. Bitcoin's Rally Masks Uncomfortable Fact: Almost Nobody Uses It [online]. [cit. 2022-05-29]. Available at: https://www.bloomberg.com/news/articles/2019-05-31/bitcoin-s-rally-masks-uncomfortable-fact-almost-nobody-uses-it?srnd=cryptocurrencies (Archived version available at: https://archive.ph/4CIiR)

[253] FEYEN, Erik, Yusaku KAWASHIMA a Raunak MITTAL. Crypto-Assets Activity around the World: Evolution and Macro-Financial Drivers. Policy Research Working Paper: Finance, Competitiveness and Innovation Global Practice & Information and Technology Solution Vice Presidency [online]. 2022, (9962) [cit. 2022-05-08]. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/37115/Crypto-Assets-Activity-around-the-World-Evolution-and-Macro-Financial-Drivers.pdf?sequence=1 (Archived version available via: https://archive.ph/1Xj13)

[254] Also confirmed by another study. For more information please see: GRAF VON LUCKNER, Clemens, Carmen M. REINHART a Kenneth S. ROGOFF. DECRYPTING NEW AGE INTERNATIONAL CAPITAL FLOWS. NBER WORKING PAPER SERIES [online]. 1-54 [cit. 2022-05-08]. Available at: https://www.nber.org/system/files/working_papers/w29337/w29337.pdf (Archived version available via: https://archive.ph/a9got)

[255] FEYEN at all., Ibid 253 at 2.

[256] Id.

[257] CRAWLEY, Jamie. MicroStrategy Buys $191M Worth of Bitcoin [online]. 2022 [cit. 2022-05-29]. Available at: https://www.coindesk.com/business/2022/04/05/microstrategy-buys-1905m-worth-of-bitcoin/ (Archived version available via: https://archive.ph/A3uqU)

[258] MONIACE, Paul R. La. Tesla still owns $2 billion in bitcoin, but crypto volatility has taken a toll [online]. [cit. 2022-05-29]. Available at: https://edition.cnn.com/2022/02/07/investing/tesla-bitcoin/index.htmlP (Archived version available via: https://archive.ph/TdWuG)

concept of Digital Assets based on extravagant and intensive promotion, in other words is the whole concept only based on endless hype?

5.2.2. Core characteristics and aspects of Digital Assets

So far, we have highlighted that Digital Assets have the promise of a digital revolution and constant influx of money. Just those two perks already create an interesting environment for criminal abuse, as both of them attracts numbers of people. Further, just couple pages above, we have argued that only about 7% of all bitcoin transactions are disconnected from investing. However, according to EUROPOL up to 23% of bitcoin transactions are associated with criminal activities.[259] Subsequently, we decided to find out what are the aspects that make Digital Assets the perfect cocktail for crime?

5.2.2.1. Technical complexity

As, the reader can judge from the technical part, Digital Assets are quite complex. In our personal opinion, we believe that majority of people, but even the Digital Assets users have a very little idea about how Digital Assets work or what could the technology behind them achieve. We don't even think they care about those aspects.

At this point, the reader could ask, how is that possible that you argue that Digital Assets are so complex that even people who use them do not understand how it works? How are they using it then? It is because the technology behind Digital Asset, the backend is hard to understand and very complex, however the frontend, the part the user actually sees is done in modern, sleek, and easy to use way. Transferring Digital Assets is easy, transferring them on a Digital Assets Exchange is easy, saving them to a personal wallet as well. Everything seem to be one click away.

[259] EUROPOL. Cryptocurrencies: Tracing the Evolution of Criminal Finances [online]. Luxembourg: Publications Office of the European Union, 2021, 1-20 [cit. 2022-05-30]. ISSN ISBN 978-92-95220-37-9. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf (Archived version available at: https://archive.ph/s8vgT)

However, that really is just its frontend. Just sending Digital Assets to a different wrong wallet or different version of it means losing it forever.[260]

This complexity combined with the limited understanding from the side of its users creates perfect environment for technologically well-versed criminals who can quickly abuse the technical flaws.

5.2.2.2. Lack of the trusted third party

As we have mentioned in the previous chapters one of the typical aspects of Digital Assets is its decentralized nature. Transactions and governance can be carried out without having to rely on any intermediary, as the transactions are conducted via peer-to-peer networks. Which is a breakthrough invention on one side, however a regulatory problem on another.

Regulation, in example anti-money laundering regulation, often depends on centralized "pressure points". "*Money laundering across national borders traditionally implicated large, multinational banks specialized in cross-border financial transactions. As such, global-level anti-money laundering (AML) efforts have traditionally "deputized" multinational banks as centralized "choke points" to report transactions suspected of laundering illicit funds*."[261] Since with permissionless Digital Assets there is usually no one in charge, using such pressure points approach against the payment system is practically impossible. It is therefore difficult to address the criminal activity both on the macro (regulatory) level as a new approach needs to be designed for the decentralized environment, but also on the micro (repressive) level, as it may be difficult to apply the current regulatory approach to this new decentralized phenomenon. We further address both of those problems below.

---

[260] BOOM VAN, Daniel. A Typo Sent $36 Million of Crypto Into the Ether. Cnet.com [online]. May 5, 2022 [cit. 2022-05-30]. Available at: https://www.cnet.com/personal-finance/crypto/a-typo-sent-36-million-of-crypto-into-the-ether/ (Archived version available via: https://archive.ph/Rxqf7) This actually happened not to a mere user of the technology but to a developer, showing just how prone to problems the Digital Assets are.

[261] CAMPBELL-VERDUYN, Malcolm. Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change [online]. Springer, 69(1), 1-30 [cit. 2022-06-02]. Available at: https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance (Archived version unavailable)

5.2.2.3. Partial anonymity (quasi-anonymity)

Partial anonymity is closely connected with the lack of trusted third party in blockchain based Digital Assets. Usually, to open an account that is able to hold funds a person must reveal personal information to the provider thus identifying herself and exposing herself to potential liability.

With Digital Assets user can simply open up an account with one click by creating a wallet.[262] In most cases, users are not required to provide any information, creating such wallet. As we have explained in the technical part users are identified only by the public key, which looks like this: 1AhTzKwpYmTjNwSjqJSf9xTBh927Ms5YNS, thus not directly revealing any information about its holder.

Analyzing IP addresses one could identify the holder of particular public key, thus the overall anonymity of wallet creation depends on the abilities of the creator. "*[Users] can avoid revealing any identifying information in connection with their public-keys; they can repeatedly send varying fractions of their bitcoins to themselves using multiple (newly generated) public-keys; and/or they can use a trusted third-party mixer or laundry*."[263] With some effort, Digital Asset users can become anonymous. It is also important to highlight that such anonymity can be achieved quite cheaply.[264] Even exchanging Digital Assets into fiat currency can be done anonymously (and cheaply), using stole identities, even if it may mean committing crimes such as identity theft, wire frauds etc.[265]

---

[262] In example using this service: https://www.bitaddress.org/bitaddress.org-v3.3.0-SHA256-dec17c07685e1870960903d8f58090475b25af946fe95a734f88408cef4aa194.html or you can even have some shipped https://bitcoinpaperwallet.com

[263] KETHINENI, Sesha, Cassandra DODGE a Ying CAO. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. American Journal of Criminal Justice [online]. Texas USA, May 2017, May 2017, 43(2) [cit. 2022-06-02]. Available at: https://www.researchgate.net/profile/Ying-Cao-25/publication/316655308_Use_of_Bitcoin_in_Darknet_Markets_Examining_Facilitative_Factors_on_Bitcoin-Related_Crimes/links/5c4503ec299bf12be3d79300/Use-of-Bitcoin-in-Darknet-Markets-Examining-Facilitative-Factors-on-Bitcoin-Related-Crimes.pdf (Archived version available via: https://archive.ph/iliFo)

[264] Most of the anonymous internet browsers can be obtained for free. In example: https://brave.com or https://www.epicbrowser.com.

[265] M.S. STEEL, Chad. Stolen Identity Valuation and Market Evolution on the Dark Web [online]. USA, 2019, 13(1) [cit. 2022-06-03]. Available at: https://www.cybercrimejournal.com/Steelvol13issue1IJCC2019.pdf (Archived version unavailable)

5.2.2.4. Borderless nature

Another aspect of Digital Assets is its borderless nature, which allows for a crime to be committed internationally. Existing on the Internet Digital Assets are accessible from anywhere and therefore are used for its ability to facilitate cross-border payments. As argued by the House of Commons Library research service: *"… in theory individual holding [Digital Assets] can transfer it to one another quite freely around the world at no or limited cost."*[266]

Further, this aspect closely relates to the decentralized structure of Digital Assets. The permissionless Digital Assets are without central intermediary and use open-source software. However, for proper functioning Digital Assets often need additional services. Such as Digital Asset Exchanges, Wallet Providers, payment processors, ATM providers etc. Those services then could be theoretically of interest in regulatory efforts. Yet, it is probably without surprise that those services abuse the borderless aspect of Digital Assets to establish themselves in jurisdictions, which have low bar for Digital Asset regulation.

This venue shopping then causes additional problems. This was aptly addressed by the Financial Action Task Force: *"[l]aw enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes ... [C]ustomer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them"*.[267]

5.2.2.5. The finality and irreversibility of transactions

The irreversibility of transactions in Digital Assets schemes is partially similar to cash instruments. "*Like cash, once a [Digital Asset] transaction has taken place, the exchange is final and there*

[266] BROWNING, Steve. Cryptocurrencies: Bitcoin and other exchange tokens. Briefing Paper [online]. United Kingdom, 2020(8780) [cit. 2022-06-07]. Available at: https://researchbriefings.files.parliament.uk/documents/CBP-8780/CBP-8780.pdf (Archived version available via: https://archive.ph/aIioe)

[267] FATF. Virtual Currencies Key Definitions and Potential AML/CFT Risks. FATF REPORT [online]. june 2014 [cit. 2022-06-07]. 1-15, p. 9 Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Archived version available via: https://archive.ph/ad7Lj)

is no recourse to undo the transaction, and there is no third-party like a bank to go to."[268] The difference, while not necessarily relevant, is that technically the transaction involving Digital Assets could be reversed. To reverse the transactions the whole Digital Asset project would have to be modified, which could cause a hard fork[269] of the underlining protocol. While possible, as such have been done in the past in the Ethereum Digital Asset blockchain following the DAO hack.[270]

It is important to note that from the business point of view such action have immense impact on the trust in such Digital Asset product. In case of Ethereum that action led to project duplicity -creation of the Digital Asset Ethereum Classic.[271] In sum, once transaction is initiated in blockchain based systems it is nearly impossible to reverse it. Such transaction therefore can be considered final.

5.2.2.6. The lack of sufficient regulation[272]

All of the above-mentioned core characteristics lead to one last, arguably the most important factor - the lack of sufficient regulation. This last factor is slowly overturning as most of the countries are taking some sort of statement regarding Digital Assets. Despite such efforts the providers of services associated with Digital Assets can, and as we show in later chapter, do chose venues where the regulation has more lax approach.

---

[268] BUTLER, Simon. Criminal use of cryptocurrencies – a great new threat or is cash still king?. Information Security Group [online]. 2019, 1-23, p.7 [cit. 2022-06-07]. Available at: https://pure.royalholloway.ac.uk/portal/files/42792707/Accepted_Manuscript.pdf (Archived version available via: https://archive.ph/B8b0N)

[269] Essentially splitting the blockchain.

[270] MEIER, Julia a Benedikt SCHUPPLI. The DAO Hack and the Living Law of Blockchain. DAL MOLIN-KRÄNZLIN, Alexandra, Anne Mirjam SCHNEUWLY a Jasna STOJAVIC. Digitalisierung - Gesellschaft - Recht: Analysen und Perspektiven von Assistierenden des Rechtswissenschaftlichen Instituts der Universität Zürich. s. 27-44. ISBN 978-3038910817. Chapter available at: https://www.researchgate.net/profile/Benedikt-Schuppli/publication/348419598_The_DAO_Hack_and_the_Living_Law_of_Blockchain/links/5ffe286f92851c13fe09c754/The-DAO-Hack-and-the-Living-Law-of-Blockchain.pdf (Archived version available via: https://archive.ph/mSFBI)

[271] KIFFER, Lucianna, Dave LEVIN a Alan MISLOVE. Stick a fork in it: Analyzing the Ethereum network partition. HotNets-XVI: Proceedings of the 16th ACM Workshop on Hot Topics in Networks [online]. 2017, 94-100 [cit. 2022-06-07]. Available at: https://dl.acm.org/doi/pdf/10.1145/3152434.3152449 (Archived version available via: https://archive.ph/wip/UFhmN)

[272] We are going to address the regulatory and legal part in more details in the following chapters.

As of the writing of this Thesis, there is still need for major improvements in regulatory approach to Digital Assets and the legislative holes are making Digital Assets interesting to criminal use.

One would assume that most of the criminals would abuse the partial anonymity and transactions irreversibility and just steal the Digital Assets. While this assumption is not wrong, there are many other possibilities how to use and abuse Digital Assets. For one-part, Digital Asset serve as an essential piece making the whole criminal scheme work – such as Dark Web markets. For the other, Digital Markets just revolutionize the old system – such as money laundering schemes. Finally, at some point Digital Assets are used as the criminal medium itself.

In the section below we therefore highlight some of the known and less known abuses of Digital Assets. In short, we argue that besides investing Digital Assets belonging to Blockchain 1.0 division mainly serve as a tool for criminal abuse.

5.3. The early abuse of Digital Assets – the Silk Road

Some believe that the motivation to use Digital Assets for payments must stem from political believes. The historical part of this Thesis has shown most of the developers of the associated technology believed in detachment from governments and financial oversight. Further, as we have written in the first chapter, most of the developers of the Digital Asset predecessor identified themselves as libertarians and shared such beliefs.

While we have argued numerous times that Digital Assets are predominantly used as a risk asset investment. In certain situations, Digital Assets are nevertheless used as a means of payment. While such use can be perfectly legitimate, such as the use of Digital Assets to carry out micropayments or international remittance, in other cases the use is purely illegitimate

and intentionally criminal. The following part is based on one of our articles, which we have modified for the purposes of this Thesis.[273]

A good view of the criminal use of Digital Assets is presented by the notable case of *U.S. v. Ulbricht*, 31 F. Supp. 3d 540 (S.D.N.Y. 2014). Not only it is one of the first successfully tried cases against Digital Assets abuse, but it is also one of the most influential cases even if not necessarily in the legal sense of things. The Silk Road case, which began in 2011, just few years after Bitcoin was introduced, have shown the capabilities of the new unregulated medium of exchange and sort of paved the way for more elaborate scams.

This case involved Ulbricht, the defendant, who engaged in narcotics trafficking, computer hacking, and money laundering conspiracies by designing, launching, and administering a 'website' called Silk Road as an online marketplace for illicit goods and services.[274] Silk Road was a Dark Web online point which served as a marketplace which allowed for exchange of illicit goods for bitcoins. Before we begin with Silk Road description, we will quickly describe the Dark Web.

5.3.1. The Dark Web

Internet became so common that everyone who is going to read this Thesis will do it over the internet. However, what most users refers to as the internet is just one of its parts also called Surface Web.[275] The Surface Web is easily accessible via search engines such as the most popular Google. Next to Surface Web, or below if you please, is so called Deep Web a part of the Internet

[273] KOHAJDA, Michael - MORAVEC, Jiří. The Illicit Use of Bitcoin. Daně a finance. 2020, 28 (1-4), 43-50. ISSN 1801-6006.
[274] *U.S. v. Ulbricht*, 31 F. Supp. 3d 540, 546 – 547 (S.D.N.Y. 2014) Available at: https://casetext.com/case/united-states-v-ulbricht-11 (Archived version available via: https://archive.ph/MQIbV)
[275] CHERTOFF, Michael. A public policy perspective of the Dark Web. Journal of Cyber Policy [online]. 2017, 2(1) [cit. 2022-05-22]. Available at: https://www.tandfonline.com/doi/pdf/10.1080/23738871.2017.1298643?needAccess=true& (Archived version available via: https://archive.ph/5qj3X)

that has not been indexed.[276] That means that the crawlers[277] search engine use either cannot access or intentionally do not access such online locations. The Deep Web is larger than the Surface Web. *Estimating the size of the Deep Web is challenging, but researchers estimate that it is between 4000 and 5000 times larger than the Surface Web. The Deep Web accounts for 90% of the traffic on the internet [...].*[278] Finally part of the Deep Web is so called Dark Web. *The furthest corners of the Deep Web, segments known as the Dark Web, contain content that has been intentionally concealed.*[279]

The Dark Web is not that easily accessible as the Surface Web. As opposed to the Surface Web, Dark Web is often not navigated by search engines or at least not by those each of uses in daily life, but the online points are reached by knowing the exact address. The online points (websites) are purposefully hidden and anonymous.[280] Those online points (websites) might require passwords or permissions to reveal its contents.[281] However software like The Onion Router or Invisible Internet Project makes the experience quite feasible to anyone. *The access of users anonymously is essential for the Dark Web […] [u]sers are accessed on the Dark Web to share data with little risk and to be undetected (anonymous).*[282] Where Dark Web and The Onion Router made the access and contents of Silk Road anonymous, Bitcoin has taken care of the anonymous transactions. This combination has proved to be quite effective in protecting the identity of Ross Ulbricht, the creator of Silk Road.[283]

---

[276] FINKLEA, Kristin. Dark Web. Congressional Research Services informing the legislative debate since 1914 [online]. March 10, 2017, 1-16 [cit. 2022-05-22]. Available at: https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf (Archived version unavailable)

[277] Crawlers are computer programs that access online location and check information to index such places into search engines.

[278] CHERTOFF., Ibid 275, at 27.

[279] FINKLEA., Ibid 276, at 3, The Dark Web technically can be used for legitimate purposes, however it gains public recognition for the fact that it often hides illegal activities.

[280] BESHIRI, Arbër S. a Arsim SUSURI. Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. Journal of Computer and Communications [online]. Scientific Research Publishing, 07(03) [cit. 2022-05-22]. Available at: https://www.scirp.org/html/4-1730998_91242.htm (archived version available via: https://archive.ph/oifvg)

[281] FINKLEA., Ibid 276,

[282] BESHIRI at all., Ibid 280, at 31.

[283] CBS, Interactive Inc. Inside the FBI takedown of the mastermind behind website offering drugs, guns and murders for hire. Cbsnews.com [online]. Nov. 10, 2022 [cit. 2022-05-22]. Available at: https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/ (archived version available via: https://archive.ph/WCMsR)

5.3.2. The Silk Road Online Marketplace

Silk Road Online Marketplace, was, as the name suggests, a marketplace accessible via The Onion Router using silkroad6ownowfk.onion and later silkroad7rn2puhj.onion. It was first open to customers in February 2011 and at its best days it had about 150 000 active customers.[284] The original Silk Road was then shut down by Federal Bureau of Investigation in 2013 and its copy Silk Road 2.0 was shut down in 2014.

Silk Road was the black market of its time. It was modern, online, international, and anonymous.[285] As a market it did not provide or sell its own goods, rather it facilitated infrastructure to connect sellers to buyers. The goods and services offered for sale were predominantly illegal. [286] On Silk Road a person could buy books describing hacking and conspiracy theories, apparel, weapons, but mainly controlled substances and illegal narcotics, predominant of which was marijuana.[287]

To pay for the illicit goods from the internet marketplace, buyers were required to use Bitcoin. Bitcoin was chosen due to its lack of regulation and partial anonymity. [288] Since bitcoin transactions are irreversible and probably because there might be no honor between criminals Silk Road Online Marketplace was acting as an escrow. Bitcoins were released from the escrow once the buyer have informed via Silk Road online forum that she received the goods.[289]

---

[284] CHRISTIN, Nicolas. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace [online]. November 30, 2012 [cit. 2022-05-24]. Available at: https://arxiv.org/pdf/1207.7139.pdf (Archived version available via: https://archive.ph/uuAJM)

[285] PHELPS, Amy a Allan WATT. I shop online – recreationally! Internet anonymity and Silk Road enabling drug use in Australia. Digital Investigation [online]. December 2014, 11(04), 261-272 [cit. 2022-05-24]. Available at: https://www.sciencedirect.com/science/article/pii/S1742287614000930 (Archived version available via: https://archive.ph/2havz)

[286] MARTIN, James. Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. Criminology & Criminal Justice [online]. Sage, 2014, 14(3), 351-367 [cit. 2022-05-24]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.838.8982&rep=rep1&type=pdf (Archived version not available)

[287] CHRISTIN., Ibid 284

[288] Id.

[289] Id.

The delivery of the illicit goods itself was then carried out via post, usually delivering to the post offices itself.

While the crimes committed are numerous, as according to the state, the defendant: "*conspired with narcotics and hackers to buy and sell illegal narcotics and malicious computer software and to launder the proceeds using [b]itcoin.*"[290] We will be more interested in the role of Digital Assets, how it relates to the Dark Web Online Marketplaces and the last crime - money laundering. More specifically how Digital Assets influences such process.

5.3.3. The crucial role of Digital Asset in Dark Web Online Marketplaces

Dark Web Online Marketplaces are relatively new phenomenon. Interestingly, the Internet drug trade can be traced literally to the Internet's inception as according to the Guardian: "*the very first thing bought and sold on the net was a bag of marijuana – over [5]0 years ago*."[291] Who in fact quotes Prof. John Markoff's book: *"In 1971 or 1972, Stanford students using Arpanet[292] accounts at Stanford University's Artificial Intelligence Laboratory engaged in a commercial transaction with their counterparts at Massachusetts Institute of Technology. Before Amazon, before eBay, the seminal act of e-commerce was a drug deal. The students used the network to quietly arrange the sale of an undetermined amount of marijuana.*"[293]

The Silk Road concept was not all new. Similar marketplace existed already. First operated via encrypted electronic email 'Adamflowers@Hushmail.com' starting in the summer 2006[294].

---

[290] U.S. v. Ulbricht., Ibid. 274., at 547

[291] POWER, Mike. Online highs are old as the net: the first e-commerce was a drugs deal [online]. 2013 [cit. 2022-06-07]. Available at: https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal (Archived version available at: https://archive.ph/iToGH)

[292] ARPANET was the first public computer network operating from 1969 and decommissioned in 1989. For more information please see: HAUBEN, Michael. History of ARPANET: Behind the Net - The untold history of the ARPANET [online]. 1-20 [cit. 2022-06-08]. Available at: https://www.jbcoco.com/Arpa-Arpanet-Internet.pdf (Archived version available via: https://archive.ph/mEotQ)

[293] JOHN, Markoff. What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry. Penguin Books; Annotated edition, (28 Feb. 2006), 352 s. ISBN 978-0143036760.

[294] US DISTRICT COURT. United States District Court for the Central District of California September 2011 Grand Jury Indictment [online]. [cit. 2022-06-08]. Available at: https://www.wired.com/images_blogs/threatlevel/2012/04/WILLEMSIndictment-FILED.045.pdf

Subsequently, with the introduction of TOR moving to the Dark Web rebranding as "The Farmer's Market.[295] However this market did not and technically speaking could not use Digital Assets as a payment medium. "*The on-line marketplace has accepted Western Union, Pecunix, PayPal, I-Golder, and cash as payment for illegal drug sales.*"[296] However, the use of those payment systems, and frankly the plead of Marc Peter Willems, have proven to be terminal for the marketplace.[297] The modern Dark Web Markets decided upgraded the anonymity be using Digital Assets.

In example as of 2019 the Wall Street Market[298] and Dream Market was using exclusively Bitcoin as a medium of payment for illicit goods.[299] Apart from Bitcoin Nightmare Market was using Bitcoin Cash, Litecoin, Monero, Zcash and Dash.[300] Berlusconi Market allows payments in Litecoin and Bitcoin.[301] And the list goes on.

The actual revolution in those Markets actually came about 40 years after the ARPANET incident, with the involvement of a key component – Digital Assets. Therefore, when the Silk Road Marketplace introduced the Bitcoin escrow services it revolutionizes the whole "industry". Any other similar concept of a Dark Web Marketplace now uses Digital Assets to carry out payments. The reason is of course the dissociative anonymity, which Digital Assets can provide if used correctly. Digital Assets thus became one of the integral parts of those Dark Web Marketplaces.

---

[295] Id

[296] Id. at page 4 line 8 – 9.

[297] Ibid., and KIM, Victoria. Dutch national pleads guilty to running online marketplace for drugs. Latimes.com [online]. September 3, 2014 [cit. 2022-06-08]. Available at: https://www.latimes.com/local/la-me-online-drug-marketplace-20140904-story.html (Archived version available via: https://archive.ph/PHWKF)

[298] The Wall Street Market was taken down. For more information please see: COLDEWEY, Davin. How German and US authorities took down the owners of darknet drug emporium Wall Street Market [online]. 2019 [cit. 2022-06-08]. Available at: https://archive.ph/GJwgM.

[299] KERMITSIS, Emmanouil, Demitrios KAVALLIEROS, Demitrios MYTTAS, Euthimios LISSARIS a Gerogios GIATAGANAS. Dark Web Markets. AKHGAR, Babak, Marco GERCKE, Stefanos VROCHIDIS a Helen GIBSON. Dark Web Investigation [online]. 85 - 118 [cit. 2022-06-08]. ISBN 978-3-030-55343-2. Available at: https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Tor/Dark%20Web%20Investigation.pdf#page=99 (Archived version available via: https://archive.ph/DgXtM)

[300] Id.

[301] Id.

Even if Digital Assets are widely used on such marketplaces, its anonymity is not without a mistake. As we have explained in the technical part, each and every transaction carried via blockchain is recorded. This fact combined with context discovery (combining information from different data sets) potentially affects the dissociative anonymity.

Already in 2011 Dan Kaminsky have proven that one could connect IP addresses to public keys in the Bitcoin network, unless its users are using TOR while creating such public keys.[302] Further research was conducted on Bitcoin's anonymity with similar results. The authors of one of the most prominent research papers on this topic have stated: "*Using an appropriate network representation, it is possible to associate many public-keys with each other, and with external identifying information. With appropriate tools, the activity of known users can be observed in detail.*"[303] In other words it means that even using Digital Assets, the users could be theoretically identified by the good old paper trail, unless they employ other measures to cover their tracks. One of such measure to cover the paper trail is called Digital Asset Mixer.

5.3.4. The Digital Assets Tumblers

We have said that Digital Assets have certain aspects that makes them interesting for criminal use. Further, we have explained that even so, Digital Assets by itself do not offer 100% anonymity.[304] Using certain methods one can therefore track the paper trail that Digital Asset

[302] D. Kaminsky. Black Ops of TCP/IP Presentation. Black Hat, Chaos Communication Camp, 2011. Available at: https://dankaminsky.com/2011/08/05/bo2k11/ (Archived version unavailable)

[303] REID, Fergal a Martin HARRIGAN. An Analysis of Anonymity in the Bitcoin System [online]. Clique Research Cluster, May 2012, 1-26 [cit. 2022-06-08]. Available at: https://arxiv.org/pdf/1107.4524.pdf?ref=https://githubhelp.com (archived version available via: https://archive.ph/oa4tb)

[304] This statement needs a small redaction, because it is not entirely correct. Some Digital Assets specialize on providing a high level of anonymity. One Such case is Monero. However, as we are trying to introduce a general picture of Digital Assets and the interconnected services, it is not the aim of this Thesis to describe each Digital Asset specifically. Nevertheless, if the reader is interested to read about one of the best anonymous Digital Asset in its class, we recommend this article, which actually describe how to decode the anonymous Digital Asset, thus evaluating its anonymity aspect thoroughly: WIJAYA, Dimaz, Joseph LIU, Ron STEINFELD a Dongxi LIU. Monero Ring Attack: Recreating Zero Mixin Transaction Effect [online]. Faculty of Information Technology, Monash University, 1-9 [cit. 2022-06-08]. Available at: https://eprint.iacr.org/2018/348.pdf (Archived version available via: https://archive.ph/BtqQt)

transactions leave. However, we are going to illustrate that it does not mean that the Digital Asset transactions cannot be further anonymized. Going back to the case of Ross Ulbricht and his Silk Road Market.

In an interview with Forbes Ulbricht said: "*we employ an internal tumbler for when vendor withdraw their payments, and a more general mix for all deposits and withdrawals. This makes it impossible to link your deposits and withdrawals and makes it really hard to even tell that your withdrawals came from Silk Road*".[305] Here, Ulbricht describes a service that allows for further anonymization of Digital Asset transactions. Those services usually operate with the Digital Asset Bitcoin as it is the most frequently used one and has the widest network of third-party services. For that this type of services is often called Bitcoin Tumbler or Bitcoin Mixer.

Bitcoin Tumbler is a service that mixes bitcoins belonging to different people together in order to lose the connection, the paper trail, between the bitcoins and its respective owner.[306] Less specifically such services combine same type of Digital Assets, but of different origin to conceal its source. It is quite easy to explain how those Mixers work. The easiest is to compare Bitcoin Tumbler with rice: "*It can be thought of as throwing three grains of rice in a very large bowl of rice, shaking the bowl for several hours, and then taking out any three of the identical grains.*"[307]

The point of those mixers therefore is to change the transaction history associated with the input funds. It uses the classical fungibility concept of money and simply switches the input Digital Asset for one with different transaction history. Such output Digital Asset has nothing in common with the one, which was inserted in the service in the first place. Additionally, the user of Digital Asset

[305] An Interview With A Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A) Forbes, https://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/#42e590c95732 (last visited Jun 4, 2019) (Archived version available via: https://archive.ph/B1Wh5)
[306] Carmine DiPiero, Deciphering Cryptocurrency: Shining A Light on the Deep Dark Web, 2017 U. Ill. L. Rev. 1267, 1273 (2017)
[307] Ibid.

Mixers can usually choose a delay between the input of Digital Assets to receiving the output. The longer the user is able to wait, the harder might be for anyone to connect the user to the inputted Digital Assets.

For the sake of completeness, the use of Digital Asset Mixers might be easy, but it is not without risk. Other authors have identified the following risks:

1. Permutation Leak. Third party can obtain the database regarding the link between input and output public keys, this essentially decoding the Digital Asset Mixer.
2. Digital Asset Theft. Third party gains unauthorized access to the Digital Assets, or public addresses routing. Further, the operator generally has access to the Digital Assets in the Mixing set (the pool of Digital Assets used for its mutual exchange, or using the above mentioned example – the bowl of rice), thus the operator can steal the Digital Assets.
3. Dropping of participants. Operator of the Digital Asset Mixer service can disallow access of the legitimate users of the service to lower the overall level of anonymity.
4. Small Mixing Set Size. The larger the mixing set (the more rice in the rice bowl) of the Digital Assets the higher the level of anonymity. Using small mixing set thus can lead to the detection of the public key associated with input of Digital Assets.
5. Join-Then-Abort. A third party can negatively influence the mixing process by leaving the Digital Asset mixer before it's the mixing round is completed.[308]

[308] The above division is based on: M. Tran, L. Luu, M. Suk Kang, I. Bentov, and P. Saxena, "Obscuro: A Bitcoin Mixer using Trusted Execution Environments," in ACSAC '18 (Annual Computer Security Applications Conference), ser. ACSAC '18, vol. 18. New York, NY, USA: ACM, 2018, pp. 692–701. [Online]. Available at: https://dl.acm.org/citation.cfm?id=3274750{\%}0A (Archived version available via: https://archive.ph/a20Qg) and PAKKI, Jaswant. Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask). University Thesis - Arizona State University [online]. April 2020 [cit. 2022-06-08]. Available at: https://keep.lib.asu.edu/_flysystem/fedora/c7/224575/Pakki_asu_0010N_19863.pdf (Archived version available via: https://archive.ph/E9ImK)

Naturally, the use of Bitcoin Tumblers and similar services[309] makes Digital Assets even more interesting platform for crimes such as money laundering. Yet, it is important to keep in mind that those mixers can still fulfil legitimate services: "*[…] for example, with the mixing of bitcoins with the purpose of better protecting and hiding public access by third parties to virtual wallet content or even personal data, with a view to enhance privacy and also prevent third party attacks."*[310] Despite this notion we will be more interested in the role of tumblers in regard to its criminal use such as money laundering.

5.3.5. Court's opinion on using Digital Assets in money laundering schemes

Such process concerned with the legitimization of the money despite its source is called money laundering and is viewed upon as: "*The act of transferring illegally obtained money through legitimate people or accounts so that its original source cannot be traced*"[311], or more generally without the use of the word money "*the process by which one conceals the existence, illegal source, or illegal application of income, and then disguises that income to make it appear legitimate.*"[312]

Once again coming back to the Ulbricht case as the main melody of this part, the Court here evaluated, whether Digital Asset can be used in money laundering. However, because the very basic fact of money laundering is that it is concerned with 'money', Ulbricht argued that "*because [b]itcoins are not monetary instruments, transactions involving Bitcoins cannot form the basis for a money laundering conspiracy*"[313] Thus raising in essence the same argument as the lawyers for Dr. Douglas Jackson in the E-Gold case. Needless to say that this argument is strictly formalistic

[309] See, in example the above-mentioned https://www.torproject.org. (Archived version available via: https://archive.ph/9V1Va) TOR is an internet addon to explorer, or explorer itself that allows for anonymous web browsing and communication. When used and executed correctly TOR can make a Bitcoin user completely anonymous.

[310] RAMALHO, David a Nuno MATOS. What we do in the (digital) shadows: anti-money laundering regulation and a bitcoin-mixing criminal problem. ERA Forum [online]. Springer, 2021, 2021(22), 487-506 [cit. 2022-06-08]. Available at: https://link.springer.com/content/pdf/10.1007/s12027-021-00676-4.pdf (Archived version available via: https://archive.ph/dw3q0)

[311] MONEY-LAUNDERING, Black's Law Dictionary (10th ed. 2014)

[312] Kevin Scura, *Money Laundering*, 50 Am. Crim. L. Rev. 1271, 1271 (2013)

[313] U.S. v. Ulbricht., Ibid. 274, at 569

and could hardly succeed – in both cases. Ulbricht at least supported his argument with the Internal Revenue Service's notice stating that bitcoins are property.[314] Contrary to Ulbricht's argument the court had held that bitcoins transactions are able to facilitate money laundering stating that: "*One can lauder money using bitcoin*."[315]

The analysis of the argument asserted by Ulbricht is governed by the Money Laundering Control Act of 1986.[316] This act is divided into two sections, the first one - 18 U.S.C. § 1956 addresses prohibited financial transactions, prohibited financial transportation, and authorizes government sting operations, while 18 U.S.C. § 1957 covers transactions involving property exceeding $10,000 derived from the specified unlawful activities.[317]

The first section further provides; "*[w]hoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity…"*[318] As such the offenses under the first sections are called transaction money laundering.[319]

The court in *Ulbricht* focused on the term financial transaction, stating that it is broadly defined.[320] According to the court the term 'financial transaction': "*captures all movements of "funds" by any means, or monetary instruments. "Funds" is not defined in the statute and is therefore given its ordinary meaning.*"[321] Funds itself sees the court as anything that can be used to pay for things in colloquial sense.[322] The court argues that bitcoin can be used as a form of payment directly, or can be exchanged into legal tender, and that its only value lies

[314] Id.
[315] Id. at 570
[316] SCURA., Ibid 312, at 1272
[317] Ibid. at 1277
[318] 18 U.S.C.A. § 1956 (West) Available at: https://www.law.cornell.edu/uscode/text/18/1956 (Archived version available via: https://archive.ph/oQMUZ)
[319] SCURA., Ibid 312, at 1277
[320] U.S. v. Ulbricht., Ibid. 274, at 570
[321] *Ibid.*
[322] *Ibid.*

in the ability to pay for things.[323] The court concludes that since the narcotics sold on Silk Road were exchanged for bitcoin, which as mentioned above is capable of holding value, the sale satisfies the term financial transaction as required by the Money Laundering Control Act.[324]

The Court therefore concludes that bitcoins can be used and indeed were used for money laundering. "*The money laundering statute is broad enough to encompass use of Bitcoins in financial transactions. Any other reading would—in light of Bitcoins' sole raison d'etre—be nonsensical. Congress intended to prevent criminals from finding ways to wash the proceeds of criminal activity by transferring proceeds to other similar or different items that store significant value."*[325]

Ross Ulbricht, aka Dread Pirate Roberts, was sentenced to life in federal prison (without parole) for creating and operating the Silk Road.[326] Following the trial, the Silk Road Online Market Place was shut down.

5.3.6. Synthesis regarding the research question

As at the very beginning we have asked the question whether some of the services associated with Digital Assets exists solely for the purpose of facilitating crime. In relation to this question, we have presented the case of Dark Web Online Marketplaces – hidden marketplaces that facilitate the sale of prohibited substances and illegal services. Those marketplaces utilize Digital Assets as a medium of exchange due to its characteristics such as technical complexity, lack of the trusted third party, partial anonymity, borderless nature, the finality and irreversibility of transactions and the lack of sufficient regulation.

---

[323] *Ibid.*
[324] *Ibid.*
[325] Ibid.
[326] U.S. Immigration and Customs Enforcement, Ross Ulbricht, aka Dread Pirate Roberts, sentenced to life in federal prison for creating, operating 'Silk Road' website. Ice.gov [online]. [cit. 2022-06-09]. Available at: https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating (Archived version available via: https://archive.ph/KV0Z7)

The existence of Dark Web Online Marketplace alone should confirm that there are purely criminal services, which depend on the use of Digital Assets as Digital Assets itself are prone to abuse, however we also show the existence of Digital Asset Mixer Services or so-Called Tumblers. Those services serve as a anonymization tool for Digital Currency, it essentially launders dirty money for a fee and it is created for this only reason. It could be argued that those services have a legitimate use, such additional anonymity on the internet, but the reality is that those services are only used for money laundering, therefore we conclude that there are services, which were developed only to make committing crimes easier.

In the next part, we are going to look into other possible roles of Digital Asset abuse and see if services such as Digital Exchanges also exist only purely to facilitate crime.

5.4. Other possible abuses in the Digital Asset's environment

Looking at the headlines of internet use, we can see that the general abuse of Digital Assets is omnipresent. Just withing the Digital Asset niche economy, we have found a statistic that shows the development of Digital Asset hacks and thefts and monitors its rising tendency. In 2011 there was 8 document incidents, which caused the damage of about $1 000 000.[327] In 2012 and 2013 the number of incidents rose to about 30 in total causing damage over $ 19 000 000.[328] By 2014 the damage was already in hundreds of million.[329] In 2019 the damage rose to multi billions and as of 2021 it keeps rising.[330] Since the acquired value of such stole Digital Assets is so high, we are looking at what are the possibilities of the actors of such crimes to legitimize the scores.

[327] CRYSTALBLOCKCHAIN. Map of Security Breaches and Fraud Involving Crypto 2011-2021. Crystalblockchain.com [online]. [cit. 2022-06-11]. Available at: https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/ (Archived version available via: https://archive.ph/ESIlG)
[328] Id.
[329] Id.
[330] Id.

It is now a well-established fact that the process of money laundering essentially consists of three stages: (1) the placement of money, (2) the layering of money, and (3) the integration of money.[331] While Digital Assets might play important role in every of those stages in the following chapter, we will be concerned with the placement part. *"The placement stage involves the physical movement of currency or other funds derived from illegal actives to a place or into a form that is less suspicious to law enforcement authorities and more convenient to the criminal. The proceeds are introduced into traditional or nontraditional financial institutions or into the retail economy."*[332]

As argued above Digital Asset can introduce new concepts of placement. In example the "dirty money" can be placed in a financial system through creating new Digital Assets with computer equipment purchased with illegal proceeds (purchased with Digital Assets), subsequently and subsequently sold as legitimate proceeds of so-called mining.

We have also chosen to focus on the placement stage, as according to some authors, the process of placement of money is the most suspectable to authorities.[333] One reason being that the liability is switched from the criminal himself to participating institutions who shall have higher incentive to participate with authorities. It is then further argued that the placement stage of money laundering is possibly the one, where it the regulation might have the highest success of reaching its goal.

Looking at any payment system, there are two important points in connection with the flow of money. Where the fiat money enters into such system and where it leaves such system. Now if such money is of questionable origin, it is best to evaluate as such at the point where such

[331] Duncan E. Alford, *Anti-Money Laundering Regulations: A Burden on Financial Institutions*, 19 N.C. J. Intl. L. & Com. Reg. 437, 439 (1994) Available at: https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1535&context=ncilj (Archived version available via: https://archive.ph/rEZqB)

[332] Peter Reuter & Edwin M. Truman, Chasing dirty money: the fight against money laundering, 25 (Institute for International Economics) (2004), https://piie.com/publications/chapters_preview/381/3iie3705.pdf (Archived version available via: https://archive.ph/I5vx2)

[333] Ibid.

money enters given payment system. Around the world the legislators therefore established so called Know Your Customer systems.

Know your customer, usually abbreviated as KYC, refers to the requirement for banks and other financial institutions to monitor, audit, collect, and analyze relevant information about their customers (or potential customers) before engaging in financial business with them.[334] In other words before the protentional customer is able to place the funds to the electric payment systems via a bank, such bank will have to identify the customer to verify, whether it can allow the customer to do so. The objectives of Know Your Customers are (1) identify who the customer is, (2) review and verify the source of customer's funds (3) monitor banking activities, after establishing the relationship with the customer.[335] The last point, number three, means that even if a person already somehow have illegitimate funds at her disposal, the bank will very likely restrict the access and handling of such funds.

The reader probably already knows, where we are going with this introduction. The main issue here is that the Know Your Customer system was designed for a financial system composed of banks.[336] In other words for a financial system, where the payment system, banks, and other financial institutions are governed by intermediaries. The difference between bank and any blockchain based Digital Asset is that Digital Assets are self-sustaining and self-governing systems without the need for a central authority. Thus, also mostly without anyone to aim the regulatory pressure on, or who to held liable for abetting to crimes.

For a simple transaction to occur within the classic banking system a bank must not only debit the funds from one account and credit them to another.[337] But the funds must even be accepted

[334]Genci Bilali, *Know Your Customer-or Not*, 43 U. Toledo L. Rev. 319 (2012) Available at: https://heinonline.org/HOL/Page?handle=hein.journals/utol43&div=15&g_sent=1&casa_token=&collection=journals (Archived version available via: https://archive.ph/VOSlq)
[335] Ibid. at 322 - 323
[336] Ibid. at 319
[337] U.S. Congress, Office of Technology Assessment, *Information Technologies for Control of Money Laundering*, 19 OTA-ITC-630 (Washington, DC: U.S. Government Printing Office, September 1995) Available at:

to by the bank in the first place. As previously stated, Digital Assets do not concern with those steps. This situation makes the placement of money especially easy, because mostly no-one verifies who owns what public key with Digital Assets, nor what is the origin of them.

5.4.1. Placement via mining?

We have already mentioned above that one way to introduce illegitimate money in the Digital Asset economy without notifying any authority is by generating new Bitcoins. We are now going to quickly evaluate whether such approach would be reasonable compared to using Digital Asset Exchanges, with its current regulatory approach, by which we hope to highlight certain problems with current regulatory measures. As this part is based on our articles that were concerned mainly with the USA's approach, we are going to base this part on US laws.

The process of generation new Digital Assets is often called bitcoin mining, given such Digital Asset is using the Proof-of-Work concept.[338] Taking bitcoin as an example once more - its mining rewards the participants with bitcoins for the allocation of computational power. At the moment the rewards is 12.5 bitcoin every 10 minutes.[339] As of the date of writing of this article, which is May/June 2019 the price of one bitcoin fluctuates around $8 400 [340] That means that every 10 minutes, the Bitcoin network by itself facilitates around $105 000 worth of bitcoins, that are completely clean and can be send anywhere in the world as long as there is internet connection.[341]

---

https://www.princeton.edu/~ota/disk1/1995/9529/9529.PDF (Archived version available via: https://archive.ph/sjCXE)

[338] Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 Ind. L.J. 441, 446 (2014) Available at: https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj (Archived version available via: https://archive.ph/ShrUs)

[339] Controlled supply Controlled supply - Bitcoin Wiki, https://en.bitcoin.it/wiki/Controlled_supply (last visited Jun 5, 2019) (Archived version available via: https://archive.ph/vfMiY)

[340] Bitcoin (BTC) price, charts, market cap, and other metrics CoinMarketCap, https://coinmarketcap.com/currencies/bitcoin/ (last visited Jun 5, 2019) (Archived version available via: https://archive.ph/bqQ2s)

[341] Technically, it is possible to transfer bitcoin even without internet using so called paper wallets. For more information about Paper Wallets see Paper wallet - Bitcoin Wiki, https://en.bitcoin.it/wiki/Paper_wallet (last visited Jun 5, 2019). (Archived version available via: https://archive.ph/gpsmg). The transfer would work in the same way as giving cash in exchange for goods.

Revisiting this part in the middle of 2022. The current situation is following. The value of Bitcoin oscillates around $30 000[342]. However as of May 11, 2020 the reward for adding a block to blockchain was halved. This means that currently the network rewards 6.25 bitcoin per connected block. Since the time of block creation is hard coded to the protocol, each block is still added about every 10 minutes. The computation thus remains the same. Every 10 minutes the Bitcoin network now produces about $187 500.

5.4.1.1. Partial synthesis of placement via mining

Therefore, one could place illegitimately obtained funds in Bitcoin network simply by using such funds to purchase or rent the equipment and use to mine bitcoins. Subsequently, one could sell those Bitcoins and legitimately declare it came from mining, which is completely legal. This remains true even about 3 years later. Nowadays it would be similarly easy to do so even using illegitimate Digital Assets as the shops which sell equipment used for mining often accept Digital Assets as a means of payment.[343] Still, as we have already noted in 2019 the convenience of this approach is somehow questionable.

However, because the mining is becoming extensively more expensive. Less profitable and it is a complex operation that nowadays requires a lot of equipment and cheap electricity. We are therefore going to conclude that this strategy is possible and unregulated but seems like it does not use the full protentional of Digital Assets in this sense. In the end such approach is just purchase of goods.[344]

---

[342] Bitcoin price. Coinbase.com [online]. [cit. 2022-06-10]. Available at: https://www.coinbase.com/price/bitcoin (Archived version available via: https://archive.ph/M49lV)

[343] In example the vendor eastshoremining.com(https://www.eastshoremining.com/checkout/)allows for payment in bitcoins, so does the vendor blockforge.com (https://blokforge.com/product/bitmain-antminer-l7-9500mh/) – after we checked about 5 other online shops, which all accept either bitcoin or different Digital Assets. We can safely conclude that majority of vendors selling equipment used for generating new Digital Assets accepts Digital Assets in return for such equipment.

[344] Peter Reuter & Edwin M. Truman, Chasing dirty money: the fight against money laundering, 25 (Institute for International Economics) (2004), https://piie.com/publications/chapters_preview/381/3iie3705.pdf (Archived version available via: https://archive.ph/rxTpA)

While we understand that this is not the best idea how to launder money, we at least can conclude that the mining itself is not mainly an illicit activity as it does not seem to be reasonable. Digital Asset mining thus seems to be a normal use of Digital Assets.

5.5. The abuse of Digital Asset Exchanges

In this part, which we have based on our published article[345], we address two issues in connection with Digital Asset Exchanges. We are again trying to find out, whether the Digital Asset Exchanges are existing primarily to facilitate crime or whether such service is used incidentally by the criminals. The first issue is again held in light of the basic view on money laundering as we believe that a more convenient placement strategy is the use of Digital Asset Exchanges compare to the above-mentioned mining. The second issue, which we are going to summarize later in this subchapter will be focused on so called wash trading.

Digital Asset Exchanges are not financial exchanges per se, rather it is a service that allows for exchange of Digital Assets like Bitcoin into different Digital Assets like Ethereum and at some exchanges into legal tender.[346] In 2018 we have stated, that the use of Digital Assets exchanges is convenient, because they are vastly unregulated.[347] We are going to address this statement more thoroughly in the next sub chapter. However, we now can reveal that that is not the case anymore as at least when to comes to money laundering there is an improvement even if there are still some problems associated with the use of Digital Asset Exchanges.

This part of Thesis gives us an opportunity not only to introduce and briefly describe what a "Digital Assets Exchange" is and later also to review the associated regulation in the United

[345] KOHAJDA, Michael - MORAVEC, Jiří. Contemporary Development of Criminal Activity in Cryptocurrency Environment. Daně a finance. 2019, 27 (1-2), 55-60. ISSN 1801-6006.

[346] Allison Caffarone & Meg Holzer, "*Ev'ry American Experiment Sets A Precedent": Why One Florida State Court's Bitcoin Opinion Is Everyone's Business,* 16 J. Intl. Bus. & L. 6, 9 (2016) Available at: https://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=2124&context=faculty_scholarship (Archived version available via: https://archive.ph/2Ew5c)

[347] CipherTrace, *Cryptocurrency Anti-Money Laundering Report (*2018), 2, https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf (last visited Jun 5, 2019) (Archived version available via: https://archive.ph/JSCSI)

States of America. *A [Digital Assets] Exchange is a platform that provides users with the possibility to trade [Digital Assets] for other [Digital Assets] or fiat money*.[348] The distributed ledger technology allows for different concepts of Digital Assets Exchanges regarding its centralization and thus also liability. *There are three types of [Digital Assets] Exchanges: centralized exchanges (CEX) which is governed by a company or an organization, decentralized exchanges (DEX) which provide automated process for peer-to-peer trades, and hybrid exchanges which combine both of the above*.[349] Given the Decentralized exchanges would need additional technical introduction, for the purposes of this Thesis we are going to limit our interest primarily to the Centralized exchanges.

5.5.1. Using Digital Asset Exchanges for money laundering?

Should the illicit Digital Asset originate in the Digital Asset system in example due to a hack or theft as we mentioned above then uploading Digital Asset on Digital Asset should be quite easy. As we have explained in the technical part to send the Digital Assets the sender needs to know only the public key, which shall receive the Digital Assets.

Of course, the first thing any criminal would need to have, is an account with the given Digital Exchange. While now most of the exchanges employs KYC, back the beginning of 2021 one could still create an account using only anonymous email address even on one of the biggest exchanges Binance.[350] Creating an account then substantially helps with placement, because once one creates account the Digital Asset Exchange automatically creates and assigns a wallet for such user, and they are able to send Digital Assets on the Exchange. Further, as we have

[348] GROENEWEG, Nikolaj. Evaluating Cryptocurrency Exchanges in the Absence of Governmental Frameworks: - A multiple criteria scoring model - [online]. Switzerland, 1-28 [cit. 2022-05-10]. Available at: https://deliverypdf.ssrn.com/delivery.php?ID=739098086122105021068114015106124011123049028029039027085068064111098103126097115094055034030123018059015112077097064110093120038013054059039029117103065082004122092022035014117081026107102025012094025085103110077125121083029121030122015108095005022085&EXT=pdf&INDEX=TRUE (Archived version available via: https://archive.ph/fTvdp)

[349] XIA, Pengcheng. Characterizing Cryptocurrency Exchange Scams [online]. China, 2020, 1-15 [cit. 2022-05-10]. Available at: https://arxiv.org/pdf/2003.07314.pdf (Archived version available via: https://archive.ph/xdkJ8)

[350] Please see: https://accounts.binance.com/en/register We have tried to create account again in 2022 and this approach is still possible, however AML measures apply later.

mentioned above the Dark Web Online Markets sell stolen identities, which can be used in the process of account creation.

For the layering process Digital Asset Exchanges seems to serve the criminals very well. *"The layering stage involves the separation of proceeds from their illegal source by using multiple complex financial transaction (e. q., wire transfers, monetary instruments) to obscure the audit trail and hide the proceeds."*[351] In our opinion this process could be done in example by trading different Digital Asset against each other. Trading one Digital Asset for a different one shall completely obscure the transaction trail as two different blockchains will be involved. Further, those trade may go to different owner. In example the criminals may choose such Digital Asset which have low liquidity and either set automated programs to trade among each other, or just buy from each other using specific prices.

The next step will be the integration stage of money laundering: "*During the integration stage, illegal proceeds are converted into apparently legitimate business through normal financial or commercial operation.*"[352] Now this step of course will be problematic, however the criminals can now again use the Digital Asset Mixers to obscure their paper trail even more, The proceeds of the placement on the Digital Asset Exchange already look like a legitimate business and commercial operation, so the criminal can simply argue that the proceeds come from trading on the exchange.

Further, it is necessary to add that as long as the Digital Assets are not sold into fiat currency using the Digital Asset Exchange, there are usually quite high limits to withdraw Digital Assets. Those limits are often denominated in Bitcoin. In example: KuCoin a centralized exchange still allows for withdrawal of up to 5 bitcoin per 24 hours, without the need for KYC, with

[351] Peter Reuter & Edwin M. Truman, Chasing dirty money: the fight against money laundering, 25 (Institute for International Economics) (2004), https://piie.com/publications/chapters_preview/381/3iie3705.pdf
[352] Id.

KYC it is up to 100 bitcoin.[353] Then there is a number of decentralized exchanges, which try to not employ KYC at all.

However, as Digital Assets could be theoretically used anywhere with sufficient internet connection, which is now even Africa, as we have argued above, the criminal perpetrators often select for the placement of illicitly obtained funds those Digital Asset Exchanges that are seated in such jurisdictions where the Anti-Money Laundering Laws and KYC laws are lacking either completely or in quality. In fact, the use of unregulated Digital Asset Exchanges was so extensive in 2018 that only about 3% of all Bitcoin transactions was happening on the regulated Digital Asset Exchanges.[354] This report subsequently provides some additional data: "*The analysis also identified 380,155 bitcoins that were received by [Digital Asset Exchanges] directly from criminal sources between January 9, 2009 and September 20, 2018. In other words, 36 times more criminal bitcoin was received by [Digital Asset] exchanges in countries where AML is either lax or lacking."*[355] This issue has been addressed by the Financial Action Task Force[356] and there are already emerging voices calling for regulation on international level.[357] When we were writing this part of the article in 2018 there was no sign of international regulation, now when we review those parts in 2022, there are certain developments, but the main one is the European Markets in Crypto Assets, which we will address in separate chapter. In this sense, we further shall add that during the time we were reviewing those parts of the Thesis Reuters have uncovered that the above mentioned Binance Digital Asset Exchange was part of large money laundering

[353] KOINLY. Top 7 No-KYC Exchanges [online]. Jan 2022 [cit. 2022-06-17]. Available at: https://koinly.io/blog/top-no-kyc-crypto-exchanges/

[354] Q3 2018 Cryptocurrency Anti-Money Laundering Report [online]. 2018 [cit. 2022-06-17]. Available at: https://ciphertrace.com/q3-2018-cryptocurrency-anti-money-laundering-report/ (Archived version available via: https://archive.ph/Jhy4z)

[355] *Ibid.*

[356] Financial Action Task Force, *Virtual Currencies Key Definitions and Potential AML/ CFT Risks* (June 27, 2015), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Archived version available via: https://archive.ph/ad7Lj)

[357] Steven Mnuchin, Sec'y, U.S. Dep't of Treasury, Panel Discussion at the World Economic Forum: The Remaking of Global Finance (Jan. 25, 2018)

scheme.[358] *"For five years, the world's largest cryptocurrency exchange Binance served as a conduit for the laundering of at least $2.35 billion in illicit funds..."*[359]

5.5.1.1. Partial synthesis of abuse of Digital Asset Exchanges

With Digital Assets Exchange it is more difficult to reach the decision, whether such third-party service is used purely for criminal endeavors or whether it is just abused, as we simply do not have enough relevant data, however what is worse, we do not even have the skill to do a proper data analysis and thus, we can leave this part for further research. However, in our opinion there is a couple points that can be derived from the above-mentioned example.

First, we believe that there is number of Digital Asset Exchanges that wishes to function as a legit business. Given we keep the discussion in the US environment, there are now Digital Asset Exchanges that register with the states using state issued licenses. In example the Digital Asset Poloniex, which is incorporated in Boston, Massachusetts.[360] Similarly, Gemini Digital Asset Exchange that is registered in New York, New York.[361] Especially Gemini takes the regulatory approach very seriously.

However, when we compare the volume, meaning the trades that have occurred the above-mentioned Digital Asset Exchanges– Polonies and Gemini with Digital Asset Exchanges that are established outside of the United State, we will see that:

---

[358] BERWICK, Angus a Tom WILSON. How crypto giant Binance became a hub for hackers, fraudsters and drug traffickers. Reuters [online]. June 2022 [cit. 2022-06-18]. Available at: https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirtymoney/ (Archived version available via: https://archive.ph/NoqOS)

[359] Id.

[360] See https://poloniex.com, and its license may be seen here https://poloniex.freshdesk.com/support/solutions/articles/1000276567-us-state-licenses,

[361] Please see: https://www.gemini.com/legal/user-agreement#section-applicable-laws-and-regulations (Archived version available via: https://archive.ph/UTHhv)

1. Regarding Poloniex Digital Asset Exchange the average volume for the past 6 months is around $100 000 000, with a few volume spikes reaching over $200 000 000.[362]
2. Regarding Gemini Digital Asset Exchange the average volume for the past 6 months is about $150 000 000, with few volume spikes reaching over $300 000 000 or even over $400 000 000.[363]
3. Regarding Kucoin Digital Asset Exchange the average volume for the past 6 months is about $1 500 000 000, with a number of volume spikes over $2 000 000 000.[364]
4. Regarding Binance Digital Asset Exchange the average volume for the past 6 months is about $12 000 000 000, with a few volume spikes over $25 000 000 000.[365]

Which lead us to partial conclusion that Digital Asset Exchanges that are less regulated, attracts much larger volume of trades. While this does not directly support our argument that many of the Digital Asset services exists solely for the purpose of facilitating illegal activities. It still in our opinion could support that those services are abused for criminal purpose. As we have said above without a good technical analysis this may be only an educated guess however, we have a follow up question regarding this issue.

The question is whether the Digital Assets Exchanges know about its (alleged) abuse and decided to remain unregulated for purpose? Such as if say Binance or Kucoin would intentionally self-regulate more would that mean that those exchanges would lose the volume? In such case we could then side with the argument that some Digital Asset Exchanges serve rather for criminal purposes as they would willingly abet crimes by allowing for them happening on their platforms.

---

[362] Poloniex Exchange: Overall Exchange volume [online]. [cit. 2022-06-18]. Available at: https://www.cryptocompare.com/exchanges/poloniex/overview (Archived version available via: https://archive.ph/dq6rx)

[363] Gemini Exchange: Overall Exchange volume [online]. [cit. 2022-06-18]. Available at: https://www.cryptocompare.com/exchanges/gemini/overview (Archived version available via: https://archive.ph/16i7x)

[364] Kucoin Exchange: Overall Exchange volume [online]. [cit. 2022-06-18]. Available at: https://www.cryptocompare.com/exchanges/kucoin/overview (Archived version available via: https://archive.ph/ZpwXr)

[365] Binance Exchange: Overall Exchange volume [online]. [cit. 2022-06-18]. Available at: https://www.cryptocompare.com/exchanges/binance/overview (Archived version available via: https://archive.ph/9YCR0)

Well first off, some the Digital Asset Exchanges themselves face the allegation of massive wash trading frauds and potential money laundering issues.[366]

5.5.2. The term Wash Trading explained

In the previous subchapter we were discussing the Digital Asset Exchanges. We have shown that Digital Asset Exchanges that are incorporated and operate in jurisdictions where the AML and KYC laws are less straight thrive more than those incorporated in example in the United States. We have further posed a question, whether Digital Asset Exchanges willingly abuse the situation.

Pursuant to the study enacted by the Blockchain Transparency Institute[367] substantial number of Digital Asset Exchanges is involved in a process called wash trading. Wash trading is a recognized concept originating outside of the phenomenon of Digital Assets.

Practically speaking wash trading is a process that involves a number of trades; however, all of those trades are orchestrated by one person or colluding people. It could be that a person places an order on an exchange and then executes the order himself acting as a different entity. Alternatively, the wash trading can be sone one a large-scale using algorithms or automated programs that are issuing and executing orders among themselves. Wash trading is prohibited by law, as it can lead to tax avoidance and frauds, but also to market manipulation.

Wash trading also known as wash sale can be defined: "*Within meaning of Commodity Exchange Act section prohibiting entering into, offering to enter into, or confirming execution of a wash sale, "wash sales" involve the use of techniques designed to give the appearance*

[366] Wash Trading Bitcoin: How Bitfinex benefits from fraudulent trading Medium, https://medium.com/@bitfinexed/wash-trading-bitcoin-how-bitfinex-benefits-from-fraudulent-trading-8bd66be73215 (last visited Jun 4, 2019) (Archived version available via: https://archive.ph/Rj6kS)

[367] According to the description on Blockchain Transparency institute's twitter is: "…a group of blockchain data researchers and enthusiasts looking to bring more transparency and trust to the crypto sphere." Please see the corresponding website: [cit. 2018-12-18], https://twitter.com/bti (Archived version available via: https://archive.ph/u04MD)

of submitting trades to the open market, while negating the risk or price competition incident to the market; wash trading produces a virtual financial nullity because the resulting net financial position is near or equal to zero, and such transactions are considered harmful because they create illusory price movements in the market."[368]

In the United States there is a dual approach to wash trading depending on the jurisdiction of the competent agency. Legal definition is therefore provided by the Internal Revenue Service, Security Exchange Commission, and Commodity Futures Trading Commission[369]. The duality is in the aim of the definition SEC and IRS are more focused on individual whereas CFTC is focused more on the market makers. Wash trading resp. Wash Sale defined by IRS as: "*A wash sale occurs when you sell or trade stock or securities at a loss and within 30 days before or after the sale you:*

1. *Buy substantially identical stock or securities,*
2. *Acquire substantially identical stock or securities in a fully taxable trade,*
3. *Acquire a contract or option to buy substantially identical stock or securities, or*
4. *Acquire substantially identical stock for your individual retirement account (IRA) or Roth IRA."*[370]

Accordingly, SEC defines wash trading by referring to the IRS definition mentioned above.[371] However, CFTC has a slightly different purpose in its definition: "*A wash trade is a transaction made without an intent to take a genuine, bona fide position in the market, such as a simultaneous purchase and sale designed to negate each other so that there is no change in financial position. Wash trades may be used, inter alia, to avoid margin requirements, to rearrange gains and loss for tax purposes, or to manipulate prices*."[372] CFTC definition's

[368] *Wilson v. Commodity Futures Trading Commn.*, 322 F.3d 555 (8th Cir. 2003) Available at: https://scholar.google.com/scholar_case?case=17618803477312186888&q=Wilson+v.+Commodity+Futures+Trading+Commn.,+322+F.3d+555+(8th+Cir.+2003)&hl=en&as_sdt=2006 (Archived version available: https://archive.ph/sq6Uq)

[369] We address all of those authorities in the next subchapter, please look below for further information.

[370] IRS. Investment Income and Expenses [online]. 2021, 1-77 p. 56 [cit. 2022-06-22]. Available at: https://www.irs.gov/pub/irs-pdf/p550.pdf (Archived version available via: https://archive.ph/yz06c)

[371] Id., for more information please see: https://www.sec.gov/answers/wash.htm (https://archive.ph/Abxnx)

[372] Reddy v. CFTC, 191 F.3d 109 (2d Cir. 1999)

purpose servers more Brokers, Exchanges, and Platforms rather than an individual. From the definitions above we can see that wash trading has harmful effect on both the individual and market. We will be further addressing the legal details in the next subchapter. We will also explain, why under then current regulation the above-mentioned regulators could only provide very limited response to the Wash Trading in relation to Digital Assets.

5.5.3. Wash Trading on the Digital Asset Exchanges

While we will address the above-mentioned research in the next few paragraphs, it is worth mentioning that we have personal experience with the Wash Trading. In our experience the Wash Trading was used as a part of a bigger scam. Starting at the beginning of 2017 until its fall[373] in 2019, we were monitoring an ongoing project of a new Digital Asset Exchange called COSS, which stands for Crypto One Stop Solution[374].

The promise of the project was, to develop a Digital Asset Exchange, which would offer a wide variety of services such a payment gateway, market cap rankings, dedicated marketplace, electronic wallet system and other.[375] While there was already a number of Digital Exchanges in 2017 offering basically the same services, the selling point of the COSS, was their Digital Asset, which was aptly also called COSS.

Apart from other Digital Asset Exchanges, COSS offered to share its revenue with owners of the COSS Digital Asset. In short, the principle was that from the overall volume of the COSS Digital Asset Exchange the holders of the COSS Digital Asset would be entitled to 50% of the fees, which were spent on trades. We found this promise interesting and bought some of those Digital Assets.

---

[373] Due to its exist scam. The whole project just disappeared and that remains is the website.

[374] ATTENTION – since the whole project has turned out to be a scam, please access with consideration (the archived version should be safe). For more information, please see: Crypto One Stop Solution. Coss.io [online]. 2021 [cit. 2022-05-08]. Available at: https://www.coss.io (Archived version available at: https://archive.ph/G5mYE)

[375] COSS. Coss: Crypto-one-stop-solution made easy [online]. 2017, 1-50 [cit. 2022-06-18]. Available at: https://cryptorating.eu/whitepapers/COSS/coss-whitepaper-v3.pdf (Archived version available via: https://archive.ph/6S78y)

At first the development of the whole platform continued quite well. The project had a working platform, which was able to connect sellers and buyers and allow for exchange of wide variety of Digital Assets. However, as the time progressed it was becoming obvious that the development team is stuck, as the exchange itself was having problems with uptime and none of the other promised functions were being added. The overall volume of the exchange was not even a million of dollars, which in comparison of the volume we have shown above is laughable amount.

Suddenly, without any major update the volume rose to about $5 millions and sometimes even to $10 million. Interestingly, the amount we were receiving due to our ownership of the COSS Digital Asset did not change. We therefore begun to monitor the trades on the platform.

While the system indicated and showed trades, those trades were specific. There were about 3 different amounts that kept repeating. The trades were not showing on the order book only on the digital field showing trades that have already happen. Further, those trades were occurring always in after certain time from each other. There was no doubt that the platform was either subject to Wash Trading or was Wash Trading herself. Given the low volume the fact that the Wash trading is going on was obvious.

Presuming, it would be highly unlikely that this Digital Exchange did not know about it, the question becomes more of do the exchanges do it on purpose rather than unknowingly allowing it? Further, would such ignorance be a single event?

While our method of simply checking the trades worked, it was mainly because the volume on the COSS Digital Asset Exchange was so low. Blockchain Transparency Institute approached the problem more professionally and evaluated the web traffic leading to the scrutinized

exchanges, which subsequently compared with the trade data collected from the actual exchanges.[376]

Comparing the traffic, which basically shows the connection to the server, where the Digital Asset Exchange is operated with the data from the exchanges itself is very important. As we show below the promoted volume on given Digital Asset Exchanges was large, but if the internet traffic would not be sufficient, who would have caused such large volume? Who would be behind the trades? The results of the Blockchain Transparency institute revealed that majority of the exchanges are reporting volume that is greatly inflated.[377] The study shows that up to 99% of the volume may not be real.[378] With great emphasis we would like to point out that it means that only 1% of the reported volume is natural.

For example, on a trading pair BTC/USDT of Digital Asset Exchange called OKEx[379], reported trading volume of over $180 000 000 where, according to the report the actual trading volume was just $20 000 000 making it only 11% of real volume. When we were reviewing this part in 2022, we have checked the OKEx (OKx) Digital Asset Exchange volume using a specialized service messari.io[380], which using its special methodology[381] verifies the reported volume, and we found out that the volume was inflated again. This time however, it was merely doubled. Similar, example using the same trading pair, but on different could be derived from the Digital Asset Exchange called Coinbene reported over $222 000 000 where the actual trading volume was only about $3 000 000 making it less than 2% of the whole volume traded.[382]

[376] December 2018 - Exchange Volume Report. Blockchain transparency [online]. 2018 [cit. 2018-12-18]. Available at: https://www.blockchaintransparency.org (data also available via: https://blogs.airdropalert.com/best-airdrops-newsletter-week-15/)
[377] Id.
[378] Id.
[379] For more information please see: https://www.okx.com. The Digital Asset exchange have rebranded itself.
[380] For more information please see: https://messari.io/exchanges
[381] https://messari.io/article/messari-proprietary-methods
[382] As of 2022, Coinbene Digital Asset exchange does not exist anymore.

If the above mentioned three Digital Asset Exchanges would not provide enough evidence, about ongoing Wash Trading and volume manipulation, already in 2017, a medium post warned about the ongoing manipulations.[383] As a side note here, we would like to add that we have again revised this part in 2022 and the specialized service messari.io we have used to verify the volume in the previous examples does not warn about ongoing Wash Trading it still shows the volume on Bitfinex to be lower than what Bitfinex reports. The author of this medium article raises serious allegations against the Digital Asset Exchange Bitfinex[384] arguing that it engages in Wash Trading. The author further claims that Bitfinex knew about the ongoing Wash Trading on its platform and actively supported it by developing a matching engine[385] that allowed a single person to bid on their own orders.[386] "*Someone writing an exchange trading engine on a normal exchange, one of the very first things the trade engine will do, is ensure your orders don't match one of your own.*"[387] In other words, the author says that every exchange that want to have a normal trading mechanism sets the matching engine in a way it does not allow such trades. He further gives an example of Digital Asset Exchange called LedgerX[388], where he analyzes the code of its matching engine to show that it will reject trades that originate and end with the same account (entity). Needless to say, that LedgerX is fully regulated by CFTC.[389] On this regulatory note however, we have to add that LedgerX operates with options and futures, in other words with derivates and as we will show that is the whole difference, why such Digital Asset Exchange is behaving differently.

We believe that by the previous paragraphs we have sufficiently proven that the some of the Digital Asset Exchanges engage in Wash Trading practices and intentionally report inflated

[383] Unknown. Wash Trading Bitcoin: How Bitfinex benefits from fraudulent trading [online]. 2018, October 21, 2017. Available at: https://medium.com/@bitfinexed/wash-trading-bitcoin-how-bitfinex-benefits-from-fraudulent-trading-8bd66be73215 [cit. 2018-12-18]
[384] For more information about the exchange itself please see: https://www.bitfinex.com/
[385] Matching engine is a complex program that allows the customers of given exchange to fulfill their posted orders. In principle a good matching engine does not allow for fulfilling your own bids.
[386] Unknown. Wash Trading Bitcoin: How Bitfinex benefits from fraudulent trading [online]. 2018, October 21, 2017. Available at: https://medium.com/@bitfinexed/wash-trading-bitcoin-how-bitfinex-benefits-from-fraudulent-trading-8bd66be73215 [
[387] Id.
[388] Please see: https://derivs.ftx.us
[389] Id.

volume. Such conduct leads us to partial conclusion that at least some of the Digital Asset Exchanges are used for illegitimate purposes or at least allow its abuse. Next, we are going to evaluate what are the impacts of such conduct and why the Digital Asset Exchanges allow or perpetrate such activity.

5.5.4. The impact of Wash Trading

In the previous subchapter we have described a number of Digital Asset Exchanges that intentionally engage in potentially criminal activities, however we still haven't show why we believe such exchanges would do that. In this subchapter we therefore present some of the reasons, why we believe the Digital Asset Exchanges may be motivated to do so.

One example in the Digital Asset Environment could be the is the admittance of new trading pairs on given Digital Asset Exchange. The apparent practice is that if developers of a project such a new Digital Asset wants for such Digital Asset to be admitted on a Digital Exchange for trading, they are required to pay a listing fee. The listing fee depends on the popularity of the Digital Asset Exchange. The more popular the Digital Asset Exchange is the higher the listing fee can be. It is no coincidence that the popularity of Digital Asset Exchange is determined by the overall trading volume of the pairs traded on the exchange. Due to the fact that the higher the (real) volume the safer it is to trade on such exchange as it is more likely your trades will be executed. According to the Business Insider the listing fee charged by the Digital Asset Exchanges can be up to $1 000 000.[390] At such high prices for listing there is a clear incentive to inflate the popularity of the platform.

[390] The cost to list tokens on cryptocurrency exchanges: Crypto exchanges are charging up to $1,000,000 for ICO to list tokens: It is a Pure Capitalism. Businessinsider.com [online]. 2018, March 12, 2018. cit. [2018-12-18] Available at: https://medium.com/@bitfinexed/wash-trading-bitcoin-how-bitfinex-benefits-from-fraudulent-trading-8bd66be73215 (Now also available here: https://uk.news.yahoo.com/crypto-exchanges-charging-1-million-064500807.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAA-KMd_Hc-jpFEus723Bt3Cjzf9ZDY-I-waoI9Cb5EDScy4rwzjcNUVCdTkznQarG-v5lJjR2PWxf1iw9r2Am9GWBsVUnm-8QeCzuS9BpajniZMFYHYh4ax_cKX2HtC3QR-bNPy6GR0jO0tFpvunqCDvtCkYV-BSfXOELpwSPTls) Archived version available via: https://archive.ph/yjswr)

This is a root of even larger problem that borderlines with a Ponzi scheme. Because if a Digital Asset that is otherwise useless is admitted on a new Digital Asset Exchange its value usually rises, therefore even the developers of such Digital Asset have incentive to pay those ridiculous admittance fees as they usually hold large numbers of the Digital Asset they develop. "*The positive effect of being listed on a popular exchange has been quite substantial for altcoins and newly-issued ICO tokens as it not only provides the digital asset with a certain level of industry approval but it also allows a much larger investor base to invest in it. Naturally, a listing on a major international digital currency exchange usually results in a price boost for the token.*"[391]

Additionally, some Digital Asset Exchanges, such as the above-mentioned COSS issued their own Digital Asset, which value is directly derived from the success of the exchange. For the most part, the success is measured by the Digital Asset Exchange use, and the extent of the use is again measured by the volume. Other reason can be very simple, to attract new business. We have said above that the volume is important decisive factor for potential customers.

The readers probably already realize the gravidity of the problem. Below we provide a very basic overview of the legal aspects of this activity under the United States jurisdiction. We believe that at minimum the manipulation with volume amounts to misrepresentation of information. With further analysis we would found even elements of fraud. According to US Common law fraud connotes perjury, falsification, concealment, misrepresentation."[392] Additionally, the fourth Circuit found that: "*fraud is a broad term, which includes false representations, dishonesty and deceit.*" [393] Since the substantive law in the US is usually defined on the state level, fraud under the New York law is defined as follows:

[391] LIELACHER, Alex. How exchange listings affect cryptocurrency prices [online]. 2018 [cit. 2022-06-18]. Available at: https://bravenewcoin.com/insights/how-exchange-listings-affect-cryptocurrency-prices (Archived version available via: https://archive.ph/WTMnf)
[392] Knauer v. United States, 328 U.S. 654, 657, 66 S.Ct. 1304, 90 L.Ed. 1500 (1946)
[393] United States v. Grainger, 701 F.2d 308, 311 (4th Cir. 1983), cert. denied, 461 U.S. 947 (1983).

"*The elements of a cause of action alleging fraud are a representation of fact, which is either untrue and known to be untrue or recklessly made, and which is offered to deceive the other party and to induce them to act upon it, causing injury; moreover, the plaintiff must show not only that he or she actually relied on the misrepresentation, but also that such reliance was reasonable*."[394][395]

Looking at the elements of fraud above, we would conclude that the actions of certain Digital Asset Exchanges would likely satisfy them. We have established that the volume reported by different Digital Asset Exchanges is different than the actual volume those Digital Asset Exchanges experience.

Further, it is not relevant whether the Digital Asset Exchanges know explicitly about the Wash Trading practices, as the mere negligence is sufficient to satisfy this element. In other words, if the Digital Asset Exchanges know about the Wash Trading practices, they satisfy the element, should they only tolerate it they are negligent and also satisfy the element. Additionally, as we have argued most of exchanges employ the matching engine, which verifies whether the person making trade is not essentially trading with herself. Therefore, we assume that the Digital Asset Exchanges must know about the ongoing Wash Trading.

We further believe that the fake volume is offered to attract more business for given Digital Asset Exchanges. We have also summarized that it is a common practice for developers and customers to look for a Digital Asset Exchange with higher volume. Therefore, showing that the volume is higher than it actually is, must be done with the intent to deceive the developers or customers and induce them to act upon it. In other words, to pay the listing fee.

[394] McMorrow v. Dime Sav. Bank of Williamsburgh, 852 N.Y.S.2d 345, 347 (N.Y. App. Div. 2d Dept. 2008)

[395] Compare also with the Florida definition of Fraud: "Fraud" is generally defined as "(1) a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment, and (2) misrepresentation made recklessly without belief in its truth to induce another person to act". Please see: Kish v. A.W. Chesterton Co., 930 So. 2d 704, 707 (Fla. 3d Dist. App. 2006), The actions taken by the Digital Asset Exchanges amounts to fraud, in our opinion, under the Florida Law as well.

Given that the volume on such Digital Asset Exchanges is then lower, the customers and developers are caused injury. As such the listing fee was incomparably high to the volume or the risk that the trade order will not be fulfilled.

As we have also summarized above, the volume is often the only thing that shows the success of a Digital Asset Exchange and therefore it is reasonable to rely on such information. Even if we show that it is probably not reasonable to rely on such information alone. However, we argue in line with the mentioned technical complexity aspect of Digital Asset and its services that the common user is not able to verify the honestness of given Digital Asset Exchange. Thus the volume can still be a decisive factor.

To support the analysis above, we quickly reference to two international cases of volume inflation. It can be therefore seen that the Wash Trading and generally the conduct of Digital Asset Exchanges is not only problem of the western regulators, but also to the Asian regulators. In South Korea this activity has its first convicts. According to a news report[396] on the Korean website Blockinpress, the CEO of Komid, a Korean crypto exchange, has received a three-year prison sentence for committing fraud against investors by artificially inflating the exchange's actual trading volume. Another company executive also received a sentence of two years for his role in these crimes.[397]

5.5.4.1. Potential securities fraud

To be more specific, under normal circumstances, the above described may even be a securities fraud. However, the jurisdiction of the Security Exchange Commission is limited in those cases as we show in the next subchapter. Further, the rules and law regarding the securities fraud are complicated. "Securities fraud" is an umbrella term for several causes of action, some

[396] For more information, in Korean, please see: https://blockinpress.com/archives/12614.

[397] Please see: https://bitcoinmagazine.com/articles/top-officials-two-korean-cryptocurrency-exchanges-face-fraud-indictments/

of which are for forms of core fraud and some of which are for forms of misrepresentation."[398] However, the laws and rules regarding the securities fraud are also very broad.[399] Simplified, one way to understand securities frauds is by the conduct that is prohibited by SEC:

(1) Schemes or artifices to defraud,

(2) False statements of fact or omissions that make truthful affirmative statements misleading, and

(3) Acts or practices that operate as frauds or deceits.[400]

Here it seems that the wash trading and associated problems may amount to securities frauds depending on what kind of product is being traded. We will address this issue more thoroughly in the next subchapter. Where we show the regulatory response.

5.5.5. Conclusion to the abuse of Digital Asset Exchanges

We dedicated a part of this Thesis to the abuse of Digital Asset Exchanges. We were once again evaluating service that associated with Digital Asset to determine what is the actual use of Digital Assets and also whether such services are used or only abused for committing criminal activity. We summarize that Digital Assets Exchanges can be used in both ways. However, we show that none of the activities we describe are happening without the knowledge of the associated services such as Digital Asset Exchanges.

Whether it is money laundering or Wash Trading it is obvious that the Digital Asset Exchanges are creating environment where those activities are possible. Since the Digital Asset environment is multinational, the Digital Asset Exchanges often choose jurisdiction where the regulatory response is lax or lacking completely. We further summarize that by doing so their transactional

[398] BUELL, Samuel. WHAT IS SECURITIES FRAUD? Duke Law Journal [online]. 2011, 512 - 581 [cit. 2018-12-20]. Available at: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1518&context=dlj
[399] Id.
[400] Section 10 of the Securities Exchange Act of 1934, Rule 10b-5, the SEC's principal exercise of authority under Section 10, 17 C.F.R. § 240.10b-5

volume is much higher compared to those Digital Asset Exchanges that choose to incorporate in jurisdictions that regulate KYC and AML.

We therefore conclude that not only some Digital Asset Exchanges tolerate the ongoing criminal activities, but such also themselves are indulging in criminal activities. The scale of those frauds and other crimes is rather extensive as we had no problem locating a number of Digital Asset Exchanges that were misrepresenting their volume or committing other crimes.

We therefore infer that Digital Asset Exchanges themselves participate on the criminal activities ongoing in the Digital Asset environment. Further, the scale of the abuse must be immense, some of the sources we have quoted evidence that overwhelming majority of the Digital Asset Exchanges participate in criminal activity. Further, given the data from this chapter we must conclude that some of the Digital Asset Exchanges commit crimes intentionally and thus must be clasified as a service that is used to commit illegal activities.

On the other hand, certain Digital Asset exchanges such as the above mentioned LedgerX voluntarily submit themselves towards the existing regulation in anticipation of a broader regulatory action. That means that even in the Digital Asset environment there are Digital Asset Exchanges that are trying to play by the rules, but those are outnumbered by those who just blatantly break the most basic rules. As we will show in the next chapter the regulatory response to the state of the Digital Asset market is overly complicated and thus does not fully encompass the ongoing issues.

5.6. The regulatory response regarding Digital Assets in United States of America Regulation

5.6.1. Introduction

This part of the Thesis is based on an article we have published in 2018 and enhanced with new developments for the purposes of this Thesis.[401] Since United States of America still does not have a comprehensive regulation regarding Digital Assets on federal level this analysis should be relevant. Back in 2018, we were trying to encompass then actual regulation relating to the concept of Digital Assets. Back then, we have chosen three independent actors that each have a different regulatory approach to what Digital Assets might be. Each of those actors approaches Digital Assets within the scope of its power and verifies, under what conditions they would have jurisdiction over them.

We have chosen the following actors. First is the Security Exchange Commission also known as the SEC. As we will explain further below SEC would be concerned with Digital Assets primarily if it finds that Digital Assets or some of them amounts to securities. Second, we chose the Commodity Futures Trading Commission also known as the CFTC. CFTC would be able to assert jurisdiction over Digital Assets if it would find that such amounts to commodities. The last one we have chosen is the Internal Revenue Service also known as the IRS. While IRS is a rather different actor compared to SEC and CFTC, we believed it would be interesting to uncover how IRS approaches Digital Assets.

5.6.2. Security Exchange Commission

In reaction to the famous Wall Street Market Crash of 1929, and as a part of the New Deal the American Congress enacted the Securities Exchange Act of 1934[402]. This Act embodies provision § 78d, 5 U.S.C.A., that established the Security Exchange Commission.

[401] KOHAJDA, Michael - MORAVEC, Jiří. Elemental Analysis of the U.S. Regulation of Cryptocurrencies. Daně a finance. 2018, 26 (4), 23-28. ISSN 1801-6006.
[402] Please see here: https://www.law.cornell.edu/wex/securities_exchange_act_of_1934

SEC is an independent federal agency. According to the website Investor.gov and similarly on the official SEC's website, SEC serves a three-part mission; (1) to protect the investors, (2) maintain fair, orderly, and efficient markets, and (3) facilitate capital formation[403]. In other words, its core function is to enforce and manage securities legislation. SEC's authority is derived especially from the following federal laws: the Securities Act of 1933, Securities Exchange act of 1934, Trust Indenture Act of 1939, and others[404]. To serve well, SEC was given quite wide range of powers, among which are the Executive power, Legislative power, and even Judicial power.

5.6.2.1. The Securities Act of 1933 and the Securities Exchange Act of 1934

Given our purposes, we can say that SEC under the Securities Act is mainly concerned with the primary introduction of securities – its offering and sales. Further, for us the most important part of the Securities Act is its section 5, which is concerned with registration of new securities. Especially 15 U.S. Code § 77e - Prohibitions relating to interstate commerce and the mails:

(a) Sale or delivery after sale of unregistered securities

Unless a registration statement is in effect as to a security, it shall be unlawful for any person, directly or indirectly—

(1) to make use of any means or instruments of transportation or communication in interstate commerce or of the mails to sell such security through the use or medium of any prospectus or otherwise; or

[403] The Role of the SEC [online]. [cit. 2022-05-22]. Available at: https://www.investor.gov/introduction-investing/investing-basics/role-sec (Archived version available via: https://archive.ph/2KP49)

[404] Investment Company Act of 1940, Investment Advisers Act of 1940, Sarbanes-Oxley Act of 2002, Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, and Jumpstart Our Business Startups (JOBS) Act of 2012

(2) to carry or cause to be carried through the mails or in interstate commerce, by any means or instruments of transportation, any such security for the purpose of sale or for delivery after sale.[405]

The secondary sales of securities are then regulated by the Security Exchange Act of 1934. For our purposes it is important that the Exchange Act also cover the regulation of securities exchanges.

It shall be unlawful for any broker, dealer, or exchange, directly or indirectly, to make use of the mails or any means or instrumentality of interstate commerce for the purpose of using any facility of an exchange within or subject to the jurisdiction of the United States to effect any transaction in a security, or to report any such transaction, unless such exchange (1) is registered as national securities exchange under section 78f of this title, or (2) is exempted from such registration upon application by the exchange because, in the opinion of the Commission, by reason of the limited volume of transactions effected on such exchange, it is not practicable and not necessary or appropriate in the public interest or for the protection of investors to require such registration.[406]

It is further worth noting that while the regulation of securities in the United States is predominantly federal, all of the state securities commissions' regulation was expressly preserved by the Securities Act of 1933:

Preservation of authority

(1) Fraud authority

[405] 15 U.S. Code § 77e available at: https://www.law.cornell.edu/uscode/text/15/77e (Archived version available via: https://archive.ph/CLmwO)
[406] 15 U.S. Code § 78e available at: https://www.law.cornell.edu/uscode/text/15/78e (Archived version available via: https://archive.ph/6mYHg)

Consistent with this section, the securities commission (or any agency or office performing like functions) of any State shall retain jurisdiction under the laws of such State to investigate and bring enforcement actions, in connection with securities or securities transactions

(A) with respect to—

(i) fraud or deceit; or
(ii) unlawful conduct by a broker, dealer, or funding portal; and

(B) in connection to a transaction described under section 77d(6) of this title, with respect to—

(i) fraud or deceit; or
(ii) unlawful conduct by a broker, dealer, funding portal, or issuer.[407] It therefore remains, significant part of securities law practice.[408]

5.6.3. Digital Assets as a security?

In this part we are going to address the SEC's position on Digital Assets. As Digital Assets, specifically Bitcoin and Ethereum became popular, it has breached within its jurisdictional border. SEC then had to look into the legal relationships that Digital Assets facilitates. Thus, what does SEC says about Digital Assets? Does the SEC consider that Digital Assets are a security or something similar?

We will again try to add a practical example and thus we will evaluate the infamous DAO incident. The DAO incident is an example of ICO. ICO stands for Initial Coin Offering. The History of ICO's

[407] 15 U.S. Code § 77r (c)(1) Available at: https://www.law.cornell.edu/uscode/text/15/77r (Archived version available via: https://archive.ph/9zUAM)
[408] MACEY, Jonathan a Geoffrey MILLER. Origin of the Blue Sky Laws. Texas Law Review [online]. USA, 1991, 70(2) [cit. 2022-06-11]. Available at: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/884/Origin_of_the_Blue_Sky_Laws.pdf?sequence=2&isAllowed=y (Archived version available via: https://archive.ph/6CaPq)

started in 2013, but it became a widespread phenomenon in 2017 and 2018.[409] By initial coin offerings new blockchain based project were rising monetary funds usually in exchange for Digital Assets, which in connection with ICO are called tokens. "*The tokens […] that are offered typically exhibit the characteristics of a digital voucher and grant the participants a right of some kind. The particular right represented by the token varies. A token may represent a license to use a software program (usage token), a membership in a community (community token) or a financial asset.*"[410]

In short while ICOs offered some benefits, such as lower costs, increased transparency and additional liquidity, they were characterized by uncertainty on many different levels.[411] In example as the Initial Coin Offering happens at the very inception of a venture its future remains uncertain. Further, there is a considerable information asymmetry between ventures and investors.[412] It goes without saying that this novel fund raiser was also uncertain from the point of view of its regulation and was rooted with various scams.

[409] LIU, Hannah. Why do People Invest in Initial Coin Offerings (ICOs)?. Joseph Wharton Scholars [online]. 2019, (5) [cit. 2022-06-11]. Available at: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1073&context=joseph_wharton_scholars (Archived version available via: https://archive.ph/YEVXl)

[410] ZETZSCHE, Dirk, Douglas ARNER a Linus FÖHR. The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators. Law Working Paper Series Paper number 2017-011 [online]. 1-39 [cit. 2022-06-11]. Available at: https://www.researchgate.net/profile/Ross-Buckley/publication/321381542_The_ICO_Gold_Rush_It%27s_a_Scam_It%27s_a_Bubble_It%27s_a_Super_Challenge_for_Regulators/links/5bb6d1a6a6fdcc9552d3ddd0/The-ICO-Gold-Rush-Its-a-Scam-Its-a-Bubble-Its-a-Super-Challenge-for-Regulators.pdf (Archived version available via: https://archive.ph/DkJoo)

[411] BELLAVITIS, Cristiano, Christian FISCH a Johan WIKLUND. A Comprehensive Review of the Global Development of Initial Coin Offerings (ICOs) and Their Regulation. Journal of Business Venturing Insights [online]. 2020 [cit. 2022-06-11]. Available at https://www.researchgate.net/profile/Christian-Fisch/publication/346413693_A_Comprehensive_Review_of_the_Global_Development_of_Initial_Coin_Offerings_ICOs_and_Their_Regulation/links/5fc0b33c92851c933f65077e/A-Comprehensive-Review-of-the-Global-Development-of-Initial-Coin-Offerings-ICOs-and-Their-Regulation.pdf (Archived version available via: https://archive.ph/z0JCu)

[412] Id.

On a separate note, the Authors have personal experience with the historical development on ICOs and actually participated in the DAO incident itself. We therefore think it may be worthwhile to draw a little illustration here in the footnote[413].

5.6.3.1. The DAO incident:

DAO stands for Decentralized Autonomous Organization. The DAO was a decentralized, crowdfunded, direct- management (or direct-democracy) organization and investment platform.[414]

According to the SEC's Release No. 81207: DAO is a term used to describe a:" *[…]"virtual" organization embodied in computer code and executed on a distributed ledger or blockchain."*[415] The Purpose of the very first DAO, which was back then simply named DAO, was to create a unique entity encoded into blockchain that would control funds denominated in the Digital Asset Ethereum and act like an independent investor or an authority in the Digital Asset environment. Its investors would then share profits should there be any.

[413] ICOs were not always a thing in the Digital Asset economy. Before it started there were different ways how to raise money for the development team. Some of them were pure scams some of them did help the developers to raise money. There were two ways how to solve the lack of funds in the beginning of this era. In the very beginning the developers would finish writing the code and put the coin online, but the process of generating new coins – so called mining - would not be open to the general public, rather to the development team only. Later on, someone realized that you can pre-mine the coins by hard coding it in the whole product. Of course, the coins would get credit based on how big the pre-mine would be. The bigger the pre-mine was the less credit and respect would the coin and the developers team receive from the community. Some developers would go completely opposite way by developing a process that was called airdrop. Airdrop was a process when the developers gave time to the general public to claim an address and the pre-mined coins would be sent to the addresses. At some point the developers realized that easiest way how to obtain money for the project would be to have them before the project would even start. The developers started to sell numbers of coins before the project development began and would be selling them in phases. In the first phase the price would be very low, in the second phase the price would be a little higher and the last phase would have the highest price. The inspiration came from the real world Initial Public Offerings.

[414] DUPONT, *Quinn. Experiments in Algorithmic Governance*: A history and ethnography of "The DAO," a failed Decentralized Autonomous Organization. (ed. Malcolm Campbell-Verduyn) Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance (forthcoming). [online]. 1-18 [cit. 2022-06-11]. Available at: https://moodle.epfl.ch/pluginfile.php/2861870/mod_resource/content/1/DUPONT-2017-Preprint-Algorithmic-Governance.pdf (Archived version available via: https://archive.ph/ohUOQ)

[415] SEC. *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934*: The DAO [online]. 2017, July 25, 2017, 2017(Release No. 81207), 1 [cit. 2022-06-11]. Available at: https://www.sec.gov/litigation/investreport/34-81207.pdf (archived version available via: https://archive.ph/kv05f)

To obtain funds for the activities DAO held a public sale of DAO tokens. During the sale DAO sold over 1 billion of so-called DAO tokens for approximately $150 000 000. The public sale of the DAO tokens is the core of our interest.

There were basically two problems that caught the attention of the SEC. The first is that when anyone organizes a $150 million public offering that lasts 30 days and broadcasts it all over the internet, but does not invite the SEC, they should likely expect the SEC to be knocking on their door. Yet when about fourteen days later someone steals from them one quarter of the raised funds (worth about $ 70 000 000 at that time)[416] anyone can be sure that the SEC is going to open that door fairly quickly. On serious note the SEC suspected that the DAO broke the above-mentioned federal laws as it did not register the DAO tokens as securities while raising the capital and became investigating the DAO tokens public offering.

"*The investigation raised questions regarding the application of the U.S. federal securities laws to the offer and sale of DAO Tokens, including the threshold question whether DAO Tokens are securities.*"[417] In order for SEC to assert jurisdiction over the sale of the DAO token it would have to amount to a security.

SEC first broadly argued that section 5(a) and 5(c)[418] of the Securities Act prohibits the unregistered offer or sale of securities in the interstate commerce.[419] SEC quoted Section 2(a)(1) of the Securities Act[420] and Section 3(a)(10) of the Exchange Act, highlighting that

[416] FALKON, Samuel. The Story of the DAO — Its History and Consequences. Medium.com [online]. [cit. 2022-06-11]. Available at: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee (Archived version available via: https://archive.ph/YgyVQ)
[417] SEC., *supra*. 415
[418] 15U.S.C. §77e (a) and (c)
[419] SEC., *supra*. 415
[420] Pursuant to the definitions: The term "security" means any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share**, investment contract**, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate

according to the definition of the Securities even an investment contract is considered security. Investment contract is then properly defined by precedents. "*An investment contract is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.*"[421]

The investment contract as defined by the Supreme Court of the Ununited States of America gave rise to the Howey Test. Howey Test is used when one is evaluating whether an asset could amount to security. If such asset satisfies all four prongs than it shall fall within the broad definition of investment contract. The four prongs of the Howey test are:

1. an investment [of money] – the scope of the investment is quite large. As argued in Reves v. Ernst & Young: "*Congress' purpose in enacting the securities laws was to regulate investments, in whatever form they are made and by whatever name they are called.*"[422]
2. [in a] common enterprise. While the courts are split on whether the commonality should be horizontal or vertical, the horizontal approach is the majority view.[423] Horizontal approach is then viewed by the courts as "*a type of commonality that involves the pooling of assets from multiple investors so that all share in the profits and risks of the enterprise.*"[424]

---

for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing. Available at: https://www.law.cornell.edu/uscode/text/15/77b#a_1 (Archived version available via: https://archive.ph/44scw)

[421] SEC., *supra* 415, and SEC v. Edwards, 540 U.S. 389, 393 (2004); SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946)

[422] Reves v. Ernst & Young, 494 U.S. 56, 61 (1990) Available at: https://scholar.google.com/scholar_case?case=18068523124125938239&q=494+U.S.+56&hl=en&as_sdt=2006 (Archived version available via: https://archive.ph/Sdkq2)

[423] In example see the following cases: SEC v. Infinity Group Co., 212 F.3d 180, 187-88 (3d Cir.2000), cert. denied, ___ U.S. ___, 121 S.Ct. 1228, 149 L.Ed.2d 138 (2001); SEC v. Life Partners, Inc., 87 F.3d 536, 543 (D.C.Cir.1996); Wals v. Fox Hills Dev. Corp., 24 F.3d 1016, 1018 (7th Cir.1994); Revak v. SEC Realty Corp., 18 F.3d 81, 87 (2d Cir.1994); Curran v. Merrill Lynch, Pierce, Fenner & Smith, 622 F.2d 216, 222, 224 (6th Cir.1980), aff'd on other grounds, 456 U.S. 353, 102 S.Ct. 1825, 72 L.Ed.2d 182 (1982).

[424] SEC v. Sg Ltd., 265 F. 3d 42, 50 - Court of Appeals, 1st Circuit 2001 Available at: https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1335&=&context=umblr&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Den%2526as_sdt%253D0%25252C5%2526q%253Dhowey%252Btest%2526btnG%253D#search=%22howey%20test%22 (Archived version available via: https://archive.ph/8paNX)

3. reasonable expectation of profits. The investment in common enterprise shall be done with the expectation of gaining profits. The expected return on the investment must come from earnings of the enterprise, not merely form additional contributions, and this return must be the principial motivation for the investment.[425]
4. [solely] the effort of others. The rigidity of the fourth prong was alleviated in United Housing Foundation v. Forman, where the Court states: *The touchstone is the presence of an investment in a common venture premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.*[426]

When SEC was evaluating whether DAO token amounts to security it relied on the relationship between DAO and the holders of the DAO token, who had the right to govern the DAO operations and were entitled to the share of profits if the entity would generate any[427]. The next problem that SEC faced, was the fact that the investment contract's definition is: […] "*an investment of money in a common enterprise […]*" While the DAO token seems to satisfy everything of the above outlined definition the investment into the DAO entity was conducted via Ethereum and Ethereum similarly to Bitcoin Digital Asset fails to fully satisfy the definition of money, as we have outline at the beginning of this Thesis.

Strictly formally speaking, the DAO token would not be a security. To bypass the money requirement SEC argued *Uselton v. Comm. Lovelace Motor Freight, Inc., 940 F.2d 564, 574 (10TH CIR. 1991)*. This case provides that: "[…] *it is well established that cash is not the only form of contribution or investment that will create an investment contract."*

[425] ALBERT, Miriam. The Howey Test Turns 64: Are Courts Grading This Test on a Curve: Are Courts Grading This Test on a Curve. 2 Wm. & Mary Bus L. Rev. 1 (2011) [online]. [cit. 2022-06-12]. Available at: https://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=1184&=&context=faculty_scholarship&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Den%2526as_sdt%253D0%25252C5%2526q%253Dhowey%252Btest%252Bprongs%2526btnG%253D#search=%22howey%20test%20prongs%22 (Archived version available via: https://archive.ph/Oj4KQ

[426] United Hous. Found., Inc. v. Forman, 421 U.S. 852 (1975) Available at: https://scholar.google.com/scholar_case?case=11168754825085710379&q=421+us+837+1975&hl=en&as_sdt=2006 (Archived version available via: https://archive.ph/uqc8n)

[427] SEC., *Ibid*. 415

In other words, the US law is familiar with multiple instruments that could serve to raise a capital for a business entity. Such as other securities, real estate know how etc. Therefore, it does not matter that the investment contract was not sponsored from one side in the exact form of fiat money. As long as the Digital Asset, in this case Ethereum is able to serve as a vehicle carrying value it shall be regarded in the same way as if it would be real estate, stock or in the end fiat money.

SEC thus argued that Ethereum is: "[…] *the type of contribution of value that can create an investment contract under Howey*.[428] Further sealing the argument with the following: "*the investment may take form of goods and services or some other exchange of value*.[429]

To fully determine whether the actions taken by the DAO would breach federal laws SEC also had to figure out the satisfaction of the reasonable expectation of profits and the fact whether it was derived from the managerial efforts of others. The last prong that SEC needed to resolve to be able to assert its authority over the problem was the comprehension of an issuer. However, the definition of the issuer was not hard to satisfy: *[…] is broadly defined to include "every person who issues or proposes to issue any security" and "person" includes "any unincorporated organization."*[430] Since SEC at that point already determined that DAO token was a security the definition of an Issuer was satisfied.

Within this reasoning we can therefore recognize that DAO Token Digital Asset is considered a security by the SEC. From the point of this incident SEC monitors all of the ICOs and requires a proper registration. However, a Digital Asset is a security only if it fulfills all the four prongs of the Howey test, which would be true only for a small part of Digital Assets. In example Bitcoin or Ethereum does not pass the Howey Test.

[428] SEC., *supra.* 415
[429] Id.
[430] SEC., *supra.* 415 Quoting the U.S.C. par 77b(a)(4).

The problems are especially the last two prongs. As with the Digital Assets decentralized nature there is hardly any enterprise and there are no common earnings. Fact is that the value actually rises only from the contributions of others – from new investments in the Digital Assets. Further, it is questionable, whether the Digital Assets are managed at all in order to satisfy the fourth prong, which requires the entrepreneurial or managerial efforts of others.

5.6.4. The Commodity Futures Trading Commission

The Security Exchange Commission is not the only regulator who has authority over the subject of our interest. In fact, the area of securities is divided between the above-mentioned SEC and other agencies such as the Financial Industry Regulatory Authority, which belongs under the so called self-regulatory organizations, and of course in relation to the Blue-Sky Laws state securities commissioners and officials. Nevertheless, we are now going to look at the approach of yet another federal commission. Now we are going to evaluate, whether Digital Assets could be considered to be commodities.

Commodity Futures Trading Commission is also an independent agency of the US government. U.S. Congress formed the CFTC in 1974 by enacting the Commodity Futures Trading Act of 1974 and the Commission assumed responsibilities that had previously belonged to the Department of Agriculture[431].

According to the CFTC's website its mission is to: [*…] foster open, transparent, competitive, and financially sound markets. By working to avoid systematic risk, the Commission aims to protect market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices related to derivatives and other products that are subject to the Commodity Exchange Act.*[432] In other words, CFTC regulates commodity futures trading (derivates relating to commodities) in the United States. The Commodity Futures Trading Commission is also

[431] CFTC. CFTC Mission Statement [online]. [cit. 2022-05-22]. Available at: https://www.cftc.gov/About/MissionResponsibilities/index.htm (Archived version available via: https://archive.ph/fEr9g)
[432] Id.

one of the most vocal and active authority in the US regarding Digital Assets, as already in 2014, its Chairman Timothy Massad said: "*We are also monitoring developing issues, including the increasing use of automated trading strategies and virtual currencies like bitcoin.*"[433]

The core of CFTC power is embodied in the Commodity Exchange Act of 1936. The Commission shall have exclusive jurisdiction […] with respect to accounts, agreements (including any transaction which is of the character of, or is commonly known to the trade as, an "option", "privilege", "indemnity", "bid", "offer", "put", "call", "advance guaranty", or "decline guaranty"), and transactions involving contracts of sale of a commodity for future delivery (including significant price discovery contracts)[…][434] CFTC is therefore charged with administering the CEA and has exclusive jurisdiction over transactions involving commodity interest.[435]

Luckily, the concept of a commodity in the United States is understood broadly under the Commodity Exchange Act. First the act lists a wide variety of agriculture products, with the exception of onions and then adds more " *[…] goods and articles […] and all services, rights, and interests […] in which contracts for future delivery are present or in future dealt in.*"[436] Under this definition commodity can be all sort of things (except the above mentioned onions and also movie tickets). Nevertheless, as we mentioned above, even if commodity is involved, the CFTC can assert jurisdiction over only if a commodity interest is based on such commodity.[437] Commodity interest is then defined as:

---

[433] Senate Hearing 113-640 [online]. [cit. 2022-06-13]. Available at: https://www.govinfo.gov/content/pkg/CHRG-113shrg94366/html/CHRG-113shrg94366.htm (Archived version available via: https://archive.ph/jJ6O4)

[434] 7 U.S.C § 2 (a)(1)(A).

[435] KLUCHENEK, Matthew. BITCOIN AND VIRTUAL CURRENCIES: WELCOME TO YOUR REGULATOR. Harvard Business Law Review Online [online]. 2016(7) [cit. 2022-06-13]. Available at: https://www.hblr.org/wp-content/uploads/sites/18/2016/12/M.-Kluchenek_Bitcoin-and-Virtual-Currency-Regulation-1.pdf

[436] 7 U.S.C. §. 1a(9) (2017) - The term "commodity" means wheat, cotton, rice, corn, oats, barley, rye, flaxseed, grain sorghums, mill feeds, butter, eggs, Solanum tuberosum (Irish potatoes), wool, wool tops, fats and oils (including lard, tallow, cottonseed oil, peanut oil, soybean oil, and all other fats and oils), cottonseed meal, cottonseed, peanuts, soybeans, soybean meal, livestock, livestock products, and frozen concentrated orange juice, and all other goods and articles, except onions (as provided by section 13–1 of this title) and motion picture box office receipts (or any index, measure, value, or data related to such receipts), and all services, rights, and interests (except motion picture box office receipts, or any index, measure, value or data related to such receipts) in which contracts for future delivery are presently or in the future dealt in.

[437] KLUCHENEK., supra at 435.

(1) *Any contract for the purchase or sale of a commodity for future delivery. – in other words, futures contract.*

(2) Any contract, agreement or transaction subject to a Commission regulation under section 4c or 19 of the Act. – in other words, commodity options and leveraged contracts.

(3) Any contract, agreement or transaction subject to Commission jurisdiction under section 2(c)(2) of the Act; - in other words, retail foreign exchange and commodity transactions.

(4) Any swap as defined in the Act[438]*, by the Commission, or jointly by the Commission and the Securities and Exchange Commission.*[439] In conclusion, the CFTC is able to assert jurisdiction over Digital Assets interests if Digital Assets amount to commodities.

5.6.5. Digital Asset as a Commodity?

The conclusion to the posed question could have been already derived from the statement of T. Massad, when he said in 2014: "*Derivative contracts based on a virtual currency represent one area within our responsibility.*"[440] Therefore, it is no surprise that CFTC subsequently argues that under the Commodity Exchange Act Digital Assets amount to commodities. The reasoning for the CFTC's statement comes from in the Coinflip Inc., case that dates to 2015.[441]

On the factual basis of the case, the Respondents (Coinflip Inc.) developed a platform called Derivabit that facilitated connection between the buyers and sellers of standardized Bitcoin

[438] 7 U.S.C. § 1(a)47 (Definition is too extensive to add) available at: https://www.govinfo.gov/content/pkg/USCODE-2010-title7/html/USCODE-2010-title7-chap1-sec1a.htm (Archived version available via: https://archive.ph/wip/NdfbT)

[439] 17 C.F.R. § 1.3 (yy) Available at https://www.govinfo.gov/content/pkg/CFR-2011-title17-vol1/xml/CFR-2011-title17-vol1-sec1-3.xml (Archived version available via: https://archive.ph/jpgJL)

[440] CFTC. Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry [online]. 2014 [cit. 2022-06-13]. Available at: https://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6 (Archived version available via: https://archive.ph/wip/71IMK)

[441] UNITED STATES OF AMERICA, COMMODITY FUTURES TRADING COMMISSION. ORDER INSTITUTING PROCEEDINGS PURSUANT TO SECTIONS 6(c) AND 6(d) OF THE COMMODITY EXCHANGE ACT, MAKING FINDINGS AND IMPOSING REMEDIAL SANCTIONS: In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, [online]. 2015, Sept 17, 2015, 2015(15-29), 2 [cit. 2018-11-21]. Available at: https://www.cftc.gov/sites/default/files/2018-06/enfsocietegeneralesaorder060418.pdf (Archived version available via: https://archive.ph/VbE1K)

options contract as eligible for trading on the Derivabit Platform[442].The Platform was using Bitcoin Digital Asset as a medium of exchange for premiums and settlements of the option contracts.[443] Users were communicating through the platform posting bids and offers regarding the designed options contract, while Respondents would confirm the bid or offer by communication it to all users through the platform.[444]

On the legal side of the case, the Commission first determines that Digital Assets (Bitcoin) are not a currency. Stating: Bitcoin and other virtual currencies are distinct from "real" currencies, which are the coin and paper money of the United States or another country that are designated as legal tender, circulate, and are customarily used and accepted as a medium of exchange in the country of issuance.[445] Subsequently without further explanation concludes that Bitcoin is a commodity. "*Bitcoin and other [Digital Assets] are encompassed in the definition and properly defined as commodities.*"[446] Importantly then, the Commission related the commodity approach to all of the Digital Assets not just to Bitcoin or Ethereum.

Further having established the jurisdiction, the CFTC held that in 2014 Respondents Francisco Riordan and Coinflip, Inc., violated Sections 4c(b) and 5h(a)(l) of the Commodity Exchange Act. Section 4c(b) of the Commodity Exchange Act provides that it is unlawful for any person to: " *[…] offer to enter into, enter into or confirm the execution of, any transaction involving any commodity […] which is of the character of, or is commonly known to the trade as, an 'option' [...] , 'bid', 'offer', 'put', [or] 'call' [...] contrary to any rule, regulation, or order of the Commission prohibiting any such transaction.*"

The posed question thus was, is Bitcoin Futures of the character as an 'option' etc.? In this sense, the Commodity Exchange Act further provides that the "option contract" which is outlined

[442] Id.
[443] Id. at. 357
[444] Id. at. 357
[445] Id.
[446] Id.

in the above definition as an option, includes the definition of swap[447] The violated section 5h(a)(1) of the Commodity Exchange Act prohibits anyone from operating: "*a facility for the trading or processing of swaps unless the facility is registered as a swap execution facility or as a designated contract market […].*"[448] CFTC argued that since the respondents were operating platform that allowed trading of swaps, the Respondent should have had register such facility looking for authority in the act 17 C.F.R. par 37.3(a)(1): "[*p]erson operating a facility that offers a trading system or a platform in which more than one market participant has the ability to execute or trade swaps with more than one other market participant on the system or platform shall register the facility as a swap execution facility under this part […].*"Where given the previous reasoning Bitcoin Futures fits right in the definition.

In conclusion, because the platform in question was not registered with the CFTC and because the Digital Assets fits the definition of Commodity so aptly, the Respondents breached the law. CFTC ordered the respondents to stop operating the platform.[449] Respondents subsequently settled.

5.6.6. Internal Revenue Service

For the sake of completeness, different approach to the definition of the Digital Assets can be found in the materials provided by the Internal Revenue Service. The IRS was created based on Revenue Act of 1862 during the American Civil War. It has also a constitutional dimension in the 16th amendment. "*The Congress shall have power to lay and collect taxes on incomes, from whatever source derived, without apportionment among the several States,*

[447] Section 1a(47)(A)(i) of the Commodity Exchange Act.
[448] Section 7 U.S.C. par. 7b-3(a)(1)
[449] UNITED STATES OF AMERICA, COMMODITY FUTURES TRADING COMMISSION. ORDER INSTITUTING PROCEEDINGS PURSUANT TO SECTIONS 6(c) AND 6(d) OF THE COMMODITY EXCHANGE ACT, MAKING FINDINGS AND IMPOSING REMEDIAL SANCTIONS: In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, [online]. 2015, Sept 17, 2015, 2015(15-29), 6 [cit. 2021-11-21]. Available at: https://www.cftc.gov/sites/default/files/2018-06/enfsocietegeneralesaorder060418.pdf

and without regard to any census or enumeration."[450] However since taxation is not within the scope of the interest of this Thesis, we will just briefly introduce on of the relevant materials prepared by the Internal Revenue Service.

Most notorious material provided by the IRS is the Notice 2014-21[451]. This report relies highly on the FinCEN's Guidance on the Application of FinCEN's Regulation to Persons Administering, Exchanging, or Using Digital Assets.[452] This report generally sees Bitcoin (Digital Assets) as a: *[…] decentralized convertible virtual currency (1) that has no central repository and no single administrator, and (2) that person may obtain by their own computing or manufacturing effort.*[453]

The IRS' material provides that Digital Assets are a digital representation of value that functions as a medium of exchange, a unit of account and/or a store of value.[454] Further the material argues that even though the digital currency technically is able of the same as a fiat currency is not a legal tender in any jurisdiction.[455] Since Bitcoin and similar is on the markets denominated to United States Dollar and may act as a substitute for the fiat currency the IRS refers to it as a convertible currency, and the sale or exchange of the convertible currency may impose a tax liability, similarly to its use to purchase goods.[456] Without any further reasoning the IRS sees Bitcoin and Digital Assets as a property and therefore as a subject to Federal Income Tax.[457]

---

[450] The 16th Amendment, March 15, 1913; Ratified Amendments, 1795-1992; General Records of the United States Government; Record Group 11; National Archives Available at: https://www.archives.gov/milestone-documents/16th-amendment (Archived version available via: https://archive.ph/rLmSj)

[451] INTERNAL REVENUE SERVICE. Notice 2014-21 [online]. 1-6 (Cited at Nov 1, 2018). Available at: https://www.irs.gov/pub/irs-drop/n-14-21.pdf (Archived version available via: https://archive.ph/xy1jc)

[452] DEPARTMENT OF THE TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK. Guidance FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies [online]. March 13, 2013, 1 Cited at Nov 5, 2018). Available at: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

[453] Id at 6.

[454] INTERNAL REVENUE SERVICE. Notice 2014-21 [online]. 1 (Cited at Nov 1, 2018). Available at: https://www.irs.gov/pub/irs-drop/n-14-21.pdf (Archived version available via: https://archive.ph/xy1jc)

[455] Id.

[456] Id.

[457] Id at 2.

5.6.7. Synthesis

In conclusion we can see that the United States agencies does not regulate to prohibit the use of the Digital Assets but understand that there are ongoing issues such us money laundering, tax evasion, and illegal raise of capital and others. We are sort of skeptical of its approach because it still feels rather incidental.

To illustrate some of the problems specifically (even if simplified), in example we have talked about the Wash Sales. We have also said that there is a dual approach where the securities and stocks are subject to prohibition by such rule. This area is regulated by SEC and IRS, in fact as we have said SEC derives the definition from the IRS's approach, however according to IRS Digital Assets are properties and properties are not subject to the Wash Trading regulation.

Similarly, as we have spoken about CFTC and its approach to Digital Assets. CFTC can regulate and oversee trading of derivates of Commodities, however not spot trading. Thus, even if Digital Assets are considered commodities the reach of CFTC is substantially limited. This is the same case with SEC, which argues that certain Digital Assets are securities, if such assets pass the Howey test, however in example Bitcoin, which is the most used Digital Asset does not pass Howey test and thus cannot be considered security. Such approach then again limits the powers of SEC. In synthesis this means that the Digital Asset Exchanges are not properly regulated on the federal level and usually register with States.

We believe that the proper response should be a federal regulation of Digital Assets. However, this seems to be generally problematic in the United States. Two bills have already been proposed. First being the "Virtual Currency Consumer Protection Act of 2018"[458] addressing price manipulation and protection of the investors and also suggesting CTFC's supervision over the market and the second being the "Virtual Currency Market and Regulatory Competitiveness

[458]For more information please see: https://soto.house.gov/sites/soto.house.gov/files/documents/SOTO_133_xml.pdf

Act of 2018"[459] talking about the general regulation of Digital Assets, clarification of their legal status and most importantly giving CFTC more rights to improve the growth of the adoption of Digital Assets. In 2022 none of those Bills have been passed.

Further, other regulation was proposed such as the Build Back Better Act, which was addressing the above-mentioned loophole with Wash Trading.[460] While this act has passed in the House of Representative, it did not pass in the Senate. Therefore, there was no change in this matter. Recently in connection with Digital Asset Exchanges the US have passed Infrastructure Investment and Jobs Act, which requires Digital Asset Exchanges to provide additional tax related reporting[461][462] Most recently the President of United States have enacted an Executive Order on Ensuring Responsible Development of Digital Assets.[463] However, this Executive Order has been enacted too late (March 2022) for us to provide any insight, we believe that it would serve as an interesting starting point for further research.

In conclusion we believe that any federal law[464] that would regulate the Digital Asset in the United States should focus on the problems outlined above, but also create a new authority with exclusive jurisdiction over the Digital Assets, as the division

[459] For more information please see: https://soto.house.gov/sites/soto.house.gov/files/documents/SOTO_162_xml.pdf

[460] For more information please see: https://www.congress.gov/bill/117th-congress/house-bill/5376

[461] Section 80603 of the Act, Information Reporting for Brokers and Digital Assets, modifies the definition of broker as set forth in Section 6045(c)(1) of the Internal Revenue Code of 1986, as amended, to include "any person who (for consideration) is responsible for regularly providing any service effectuating transfers of digital assets on behalf of another person." The term "digital asset" is defined by Code Section 6045(g)(3)(D) to mean "except as otherwise provided by the Secretary [of the Treasury], any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology as specified by the Secretary." MANATT, PHELPS a PHILLIPS. Crypto Reporting Rules in the Biden Infrastructure Deal [online]. 2022 [cit. 2022-06-18]. Available at: https://www.jdsupra.com/legalnews/crypto-reporting-rules-in-the-biden-1784927/ (Archived version available via https://archive.ph/bqQ2s)

[462] WALKER, Jones. Cracking the Crypto Code: New Reporting Obligations (Current Developments in the World of Blockchain and Cryptocurrency). Natlawreview.com [online]. [cit. 2022-06-18]. Available at: https://www.natlawreview.com/article/cracking-crypto-code-new-reporting-obligations-current-developments-world-blockchain (Archived version available via: https://archive.ph/Cx2wU)

[463] Available here: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

[464] A bill providing for the regulation of Digital Assets and for their other purposes, which shall cover some of the topics argued below was proposed, however as of 2022 it is not getting any substantial recognition. The Bill is available here: https://www.congress.gov/117/bills/hr4741/BILLS-117hr4741ih.pdf

between SEC, CFTC, and IRS apparently causes problems. Define Digital Assets in federal law using technical analysis, because once again the current regime is too complicated and there are likely examples when Digital Asset satisfies each of the prongs of the above-mentioned agencies meaning being Security, Commodity, and Property. The above-mentioned new authority should also have exclusive jurisdiction over the secondary trading of Digital Assets.

6. Stable Digital Assets and MiCA

6.1. Stable Digital Assets

6.1.1. Introduction

So far, we have raised argument that majority of the Digital Assets limited use. We further argue that most of Digital Assets are used only for speculation or criminal activity. While there are certain branches of Digital Assets that promise for a different potential. In example, such Digital assets that serve as a platform for a software development, such as Ethereum, or have a single utility function inside larger systems such as the Gas token in the Neo ecosystem[465]. We are still of the opinion that the classic concept of Digital Assets is problematic and frankly not needed.

We believe that what other see as a good aspect is one of the problems. The usual limited supply of Digital Asset motivates people to spend horrendous sums of money, which as we have argued above then attracts the criminal element. That is in our opinion however, not the only problem. Since the limited supply in combination with the influx of money motivates people to hold such Digital Asset rather then spent them, those Digital Assets are not used as they were initially intended.[466] The following part will be based on our article that we have modified for the purposes of this Thesis.[467]

In the recent years, one type of digital assets, so called Stablecoins, shows a steady growth in its user base and utility. As such this concept is getting traction not only in the Digital Assets economy, but also among the big tech companies, and therefore also regulators.

[465] For more information on the Neo project please see its home webpage: https://neo.org

[466] Given there was any general intention to use them as a medium of exchange, which was proclaimed by all the developers, but we have shown that the reality is completely different.

[467] MORAVEC, Jiří - KOHAJDA, Michael. Legal Issues of Stablecoins. Daně a finance. 2021, 28 (1-4), 93-98. ISSN 1801-6006.

6.1.2. Brief introduction to stablecoins history

One of the defining elements of the Digital Assets' speculative economy is its instability. For good or worse the volatility, has attracted large number of speculators and investors who brought a substantial amount of money into said economy. Ironically, a niche economy largely build on instability, became lacking stability. In other words, it was lacking a stable asset, that would be easily transferable, denominated in a known currency, and would serve as a haven for the acquired value. In the late 2014 a group called Tether Limited came with a solution.[468]

They developed and presented the first digital asset, which value was pegged to an existing real-world fiat currency. In case of tether, then known as Realcoin, it was the United States Dollar. Because of its relative stability Tether and similar assets became generally known as stablecoins.

Right after tether was introduced to general public, its market capitalization was around $250 000 in April, 2015.[469] Ever since then the market capitalization and its global use was growing exponentially. The users have heavily relied on the promised stability as for the first time it was possible to exchange your funds into an asset that worked in the same way as Bitcoin, however had also a promise that it would not lose its value completely overnight.

In January 2017 the market capitalization has crossed the $10 million for the first time[470]. However, on December of the same year the market capitalization was already over one billion USD.[471] As of now, in May 2022 the capitalization is over sixty billion USD, and it seems to be still growing.[472] Not to mention that pooling together the top three stablecoins their market is near to one hundred billion USD.[473]

---

[468] The Rise of Stablecoins: The Rise of Tether [online]. USA, 2020, s. 1-20, page 3, [cit. 2021-11-21]. Available at: https://f.hubspotusercontent00.net/hubfs/5264302/The%20Rise%20of%20Stablecoins.pdf (Archived version available via: https://archive.ph/O1Pfq)

[469] Coin Market Cap: Tether price today [online]. USA, 2021 [cit. 2021-11-21]. Available at: https://coinmarketcap.com/currencies/tether/ (Archived version available via: https://archive.ph/Br2fh)

[470] *Id*.

[471] *Id*.

[472] *Id*.

[473] *Id*.

6.1.3. Stablecoins generally

"*Stablecoins are an attempt to address the high volatility of "traditional" [Digital Assets] by tying the stablecoin's value to one or more other assets, such as sovereign currencies."*[474] Stablecoins, including Tether, are Digital Assets that are designed in a way that allows them to maintain a stable value against a target price. In the words of the European Central Bank "*Stablecoins are digital units of value that are not a form of any specific currency (or basket thereof) but rather, by relying on a set of stabilization tools, try to minimize fluctuations in their price in such currencies*."[475]

Financial Stability Board sees stablecoins similarly to European Central Bank: "*A crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.*"[476]Even though there are now different types of stablecoins, the unifying factor between them is the existence of a mechanism that allows for a stable value. Based on the technological difference between the stabilization mechanisms, we can establish technical taxonomy of stablecoins. The technical taxonomy of stablecoins is important for subsequent legal qualification. Importantly, stablecoins generally do not represent an entirely new type of asset, rather it mirrors a real-world value, in example a fiat currency. This type of a "off-chain" collateral is the most popular one.[477] as we will show later, such technical solution brings stablecoins close to the classic concept of electronic money.

---

[474]Financial Stability Board: Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document [online]. April 14, 2020, page 1, 1-62 [cit. 2021-11-21]. Available at: https://www.fsb.org/wp-content/uploads/P140420-1.pdf (Archived version available via: https://archive.ph/A138I)

[475] BULLMANN, Dirk, Jonas KLEMM a Andrea PINNA. Occasional Paper Series: In search for stability in crypto-assets: are stablecoins the solution? [online]. August 2019, 1-53 [cit. 2021-11-21]. ISSN 1725-6534. Available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf (Archived version available via: https://archive.ph/Q3XSt)

[476] Financial Stability Board: Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document [online]. April 14, 2020, page 4, 1-62 [cit. 2021-11-21]. Available at: https://www.fsb.org/wp-content/uploads/P140420-1.pdf (Archived version available via: https://archive.ph/A138I)

[477] Stablecoins: an overview of the current state of stablecoins [online]. 2020, 1-31 [cit. 2021-11-21]. Available at: https://download.blockdata.tech/blockdata-stablecoin-report-blockchain-technology.pdf (Archived version available via: https://archive.ph/JePwl)

Besides offering and bringing stability to the Digital Asset economy it seems that Stablecoins might have quite a few of innovative characteristics, some of which it partially shares with other distributed ledger technology based Digital Assets and some that it brings on its own. A fully functioning and legal concept of Stablecoin could introduce so called smart money (programable money), higher efficiency in payments through its 24/7 availability, borderless character, ability to employ smart contracts, micropayments, and fractioning[478]. As well as financial inclusion for less developed regions in the world. As we have said above, we believe that the main difference from the above-described Digital Assets such as Bitcoin, which makes Stablecoins interesting is that Stablecoins are not conceived with limited supply. Therefore, do not motivate its user to hold them and wait for value increase, but rather actually use them.

6.1.4. Technical taxonomy of stablecoins

General dividing line between Stablecoins could be draw based on the fact, whether such stablecoins are backed by assets and if so, by what kind of asset. However other approaches are also possible, depending on the actual kind of the stabilizing asset a Stablecoin may be or does not have to be directly linked to the already existing financial system. Stablecoins relying on other than real world assets may be functioning completely without the need of established external financial system. For the purposes of this Thesis we decided to divide stablecoins depending on its stabilization mechanism.

A Stablecoin using an asset as a collateral or a part of its stabilization mechanism is referred by Financial Stability Board to as: "*A stablecoin that purports to maintain a stable value by referencing real or financial assets or other crypto-assets."*[479]

[478] ARNER, Douglas, Raphael AUER a Jon FROST. BIS Working Papers No 905: Stablecoins: risks, potential and regulation [online]. 2020, page 7, 1-31 [cit. 2021-11-21]. Available at: https://www.bis.org/publ/work905.pdf (Archived version available via: https://archive.ph/GQMqB)
[479] FSB., supra 474 at 9.

Asset-Backed Stablecoins can be further divided based on whether the collateralized asset is a traditional asset or rather a Digital Asset such as Bitcoin, or whether such collateral is mixed. Therefore, Asset-Backed Stablecoins based on its collateral can be divided as follows:

1. Asset-Backed, where the collateral is a real-world asset for example gold[480];
2. Fiat-Backed, where the collateral is a fiat currency for example USD. Actual example would be Tether Dollar, USDT[481]; or Saga, which is now delisted.
3. Asset-Fiat-Backed, where the collateral is a combination of fiat currency and a real-world asset, for example USD and Gold;
4. Digital Asset-Backed, where the collateral is a Digital Asset, such as Ethereum. Actual example would be DAI[482];
5. Digital Asset and Fiat-Backed, where the collateral is a Digital asset and a fiat currency, for example Ethereum and USD.[483]

Apart from having the stabilization mechanism relying on real or financial asset or other Digital Asset, some stablecoins projects promise a working solution based on an algorithm. According to Financial Stability Board the Algorithm-based Stablecoin is: "*a stablecoin that purports to maintain a stable value via protocols that provide for the increase or decrease of the supply of the stablecoins in response to changes in demand.*"[484]

While algorithm-based stablecoin is technically possible, we are still not sure as of the time of writing this Thesis, whether there are such stablecoins that would be reliable and functional (as we show below on an example). "*The idea behind algorithmic stablecoin initiatives is to adjust*

[480] For more information on the Digix gold token project please see it's home webpage: https://digix.global/#/ (Archived version available via: https://archive.ph/Zdfec)
[481] For more information on the Tether project please see it's home webpage: https://tether.to (Archived version available via: https://archive.ph/quMGp)
[482] For more information on the Dai project please see it's home webpage: https://makerdao.com/en/ (Archived version available via: https://archive.ph/EYtEV)
[483] The current approach of Digital Asset-Backed stablecoins is to overcollateralize in order to offset the volatility of the digital asset that is used as a collateral. Therefore, the actual ratio is not one to one as is in case of Tether but rather six to one or higher.
[484] FSB., ibid 474 at 9

the supply of stablecoin units in order to maintain their price stability in the currency of reference and to guide users' expectations on its future value."[485]

One of the main differences between asset-backed stablecoins and algorithm stablecoins is the absence of even a theoretical redeemability in algorithmic stablecoins. While the users should be at least theoretically capable of redeeming the stablecoins for the stabilizing asset in case of algorithm stablecoins projects such exchange is not even a theoretical option.

As an example, we can introduce the stablecoin "Fei Protocol[486]". Fei is built upon the cooperation of two different digital assets a Fai stablecoin and a so called "Tribe", which is a governance token.

The stabilization algorithm itself shall work upon a self-regulating market principle. Any time the value of Fei rises above the desired value (1 USD) the algorithm mints more Fei, which it sells for a digital asset such as Ethereum to lower Fei's value. Should Fei lose its value under the desired value the algorithm shall sell a digital asset such as Ethereum and issue orders for more Fei[487]. For the past five months Fei stablecoin is relatively stable, oscillating around the desired value of one USD[488]. However, in the beginning of its launch for the first two months the peg was broken and the value of the stablecoin was under one USD. Further, while speculative, it is questionable what would in rapid market crash. It is unsure whether the algorithm would be able to upkeep the established peg.

[485] BULLMANN at all., ibid at 475 at 23

[486] For more information on the Fei project please see its home webpage: https://fei.money (Archived version available via: https://archive.ph/bOnfe)

[487] Fei Protocol White Paper [online]. 2020, 1-18 [cit. 2021-11-21]. Available at: https://fei.money/static/media/whitepaper.7d5e2986.pdf (Archived version available via: https://archive.ph/AYPP5)

[488] Coin Market Cap: Fei price today [online]. USA, 2021 [cit. 2021-11-21]. Available at: https://coinmarketcap.com/currencies/fei-usd/ (Archived version available via: https://archive.ph/w6URF0)

About one year after, when we added this part, which was published as an article, we can answer the previous sentence. Let us briefly introduce the Stablecoin TerraUSD[489], which is algorithmic Stablecoin using arbitrage as a stabilizing mechanism. As the sell-off of Digital Asset begun to intensify TerraUSD has lost its peg and the algorithm stopped working properly. TerraUSD started losing value, and then in the spam of 10 days lost literally 99.99% of its value, thus effectively crashing to nothing.[490] We thus derive that algorithmic Stablecoins still have room for improvement.

6.1.5. Sporadic regulation of Stablecoins under EMD2

Under the current (European) regulatory framework some stablecoins might be regulated under the directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, as amended (EMD) as some types of stablecoins might fall under the definition of electronic money.

Under EMD2 the electronic money is defined as: *electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC ('payment transaction' means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee), and which is accepted by a natural or legal person other than the electronic money issuer*[491].

Whether a stablecoin could fall under the EMD2 definition of electronic money depends on the technical background (back end) of such stablecoin. The decisive factor seems

[489] For more information please see here: https://www.terra.money (archived version available: https://archive.ph/TazZq)
[490] The investors lost $ 40 billion. NEWBERY, Emma. Binance CEO Says LUNA Collapse Left Him 'Poor Again [online]. [cit. 2022-06-21]. Available at: https://www.fool.com/the-ascent/cryptocurrency/articles/binance-ceo-says-luna-collapse-left-him-poor-again/ (Archived version available via: https://archive.ph/16i7x)
[491] Article 2(2) of EMD2

to be whether such stablecoin represents a contractual relationship between the issuer and a customer amounting to IOU.

The fiat (one type of fiat) backed type of stablecoin follows the characteristics of electronic money definition. In example Tether is electronically stored monetary value, as Tether is a representation of tokenized USD which is logged on blockchain technology.

Further, at least, according to official statements of the tether group, the individual coins are issued against a receipt of funds (USD)[492] and should amount to IUO relationship additionally the purpose of Tether is to allow for transactions as defined in article 4(5)(f) of Directive 2007/64/EC. Therefore, Tether could be considered electronic money under EMD2, and the provider of Tether might be under certain obligations. However, since Tether can also be used as a form of investment transferred over blockchain, where the contractual relationship between issuer and customer could be diminished, it could be also considered e-money token under the below mentioned regulation.

However, other types of stablecoin, while having the exact same purpose (to facilitate payment transactions as defined above) seem to be out of scope of the e-money definition. Asset backed stablecoins are not issued against receipt of funds, which makes them standout of the definitions.

Similarly, should the stablecoin be backed by a basket of fiat currencies, rather than just one, it seems it would not follow the definition under EMD2. Further, algorithmic stablecoins, which promise not to be backed by anything else than the algorithm itself, cannot meet the definition either as such coins should be stabilized only by responding to supply and demand.

[492] Tether.to: Assurance Opinion Confirms Tether's Reserves Fully Backed; Company Shares as Part of Ongoing Transparency Commitment [online]. USA, 2021 [cit. 2021-11-21]. Available at: https://tether.to/assurance-opinion-mar-21/ (Archived version available via: https://archive.ph/ZxJLE)

6.2. The MiCA proposal

As shown above certain technological solutions are taking stablecoins out of the scope of electronic money and to completely unregulated space. European Union therefore came with a plan for a new regulation of the European Parliament and the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA), which should be a general response to the quickly developing Digital Asset technology and more importantly a prime regulation on stablecoins. MiCA introduces new definition of stablecoins and additional obligations for stablecoins issuers depending on its type and significance.

While we do not intent to provide full review of the MiCA in this Thesis, we are going to introduce certain areas of the regulation itself.

EU is quite serious with its approach to Digital Assets and thus it chosen a regulation instead of directive, as there shall be no national exception regarding the issuer and service providers. It should be noted however that the proposal is still under development and subject to alternations and changes. The MICA proposal has been enacted with four general and related objectives.

1. Legal certainty;
2. Support innovation;
3. Instill appropriate levels of consumer and investor protection;
4. Ensure financial stability.[493]

While the objectives seem to promote primarily digital asset consumer protection, according to the MiCA explanatory memorandum the financial stability itself is also an important part of its intended purpose: *a relatively new subset of crypto-assets – the so-called 'stablecoins' – has recently emerged and attracted the attention of both the public and regulators around the world.*

[493] Explanatory memorandum of MiCA, available at: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF (Archived version available via: https://archive.ph/dxxME)

While the crypto-asset market remains modest in size and does not currently pose a threat to financial stability, this may change with the advent of 'global stablecoins', which seek wider adoption by incorporating features aimed at stabilizing their value and by exploiting the network effects stemming from the firms promoting these assets.[494]

As of now it is often argued that stablecoins do not present danger to the existing financial system. Similarly argued by the Financial Stability Board: *At present, stablecoins are being used primarily as bridge between traditional fiat currencies and other crypto-assets, which in turn are primarily held and traded for speculative purposes*[495].

However, under certain conditions the situation may quickly change: *Increased participation by retail investors could give rise to broader financial stability issues through an erosion of trust in the financial system. In the event that a stablecoin does enter the mainstream of the financial system as a means of payment and/or a store of value in multiple jurisdictions, with the potential to achieve substantial volume, it could become a global stablecoin. The emergence of global stablecoin would pose greater risks to financial stability than existing stablecoins and may challenge the comprehensiveness and effectiveness of existing regulatory, supervisory and oversight approaches.*[496]

In other words, should stablecoins become a global phenomenon or should firms like Facebook (Meta Inc.) or Apple create their own Digital Assets (currency) as proclaimed[497]. MiCA should be there to help assure the financial stability as we know it. Stablecoins as such therefore seem to be one of the central focus points of MiCA.

[494] Id.
[495] FSB., ibid 474 at 3
[496] Id. at 4
[497] DILLET, Romain. Facebook scales back its crypto ambitions once again. TechCrunch.com [online]. [cit. 2021-11-21]. Available at: https://techcrunch.com/2021/10/19/facebook-scales-back-its-crypto-ambitions-once-again/ (Archived version available via: https://archive.ph/bhYux)

6.2.1. The MiCA proposal's subject matter, scope, and its approach to Digital Assets

MiCA represents the first EU general regulatory response to Digital Assets. We are now going to describe MiCA's subject matter, its scope and the definition of Digital Assets, which MiCA addresses as "Crypto-Assets".

Crypto-Asset is then defined as *"[…] a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology."*[498] Therefore choosing a broad general definition and diverging from the misleading term virtual currency that was then used in anti-money laundering directives 4 and 5. Which provided that virtual currency means: "*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."*[499] The term Crypto-Asset is then further specified in MiCA. Crypto-Asset is divided in three subcategories.

1. Asset-Referenced Token, according to MiCA "*means a type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets.*"[500]
2. Electronic Money Token or E-money Token according to MiCA means a type of crypto-asset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender.[501]

[498] Article 3(1)(2) MiCA
[499] Art. 3(18) of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
[500] Article 3(1)(3) MiCA
[501] Article 3(1)(4) MiCA

3. Utility Token according to MiCA means a type of crypto-asset which is intended to provide digital access to a good or service, available on DLT, and is only accepted by the issuer of that token.[502]

We can see that MiCA draws difference between different types of Digital Assets and Stable Digital Assets. In terms of Asset-Referenced Token and E-Money token MiCA draws difference between them based on what such Digital Assets use for its stabilization. Further based on this division MiCA also provides different set of rules for such Digital Assets. Crypto-Assets different than asset-referenced token or e-money tokens are regulated under the Title II. Asset-referenced tokes are regulated in Title III. Electronic money tokens are then regulated in Title IV of MiCA[503]. More as an interesting point the algorithmic stablecoins we mention above do not fall within the specific Title III and Title IV Stable Digital Assets and rather: "*So-called algorithmic 'stablecoins' that aim at maintaining a stable value, via protocols, that provide for the increase or decrease of the supply of such crypto-assets in response to changes in demand should not be considered as asset-referenced tokens, provided that they do not aim at stabilizing their value by referencing one or several other assets."*[504]

The scope of MiCA is not established only by what amounts to Crypto-Assets, but also by an exclusion of certain other Digital Assets that may fall under existing EU regulation. Specifically, MiCA provides, that it does not apply to crypto-assets that qualify as:

(a) financial instruments as defined in Article 4(1), point (15), of Directive 2014/65/EU;

(b) electronic money as defined in Article 2, point (2), of Directive 2009/110/EC, except where they qualify as electronic money tokens under this Regulation;

[502] Article 3(1)(5) MiCA
[503] For a part also in EMD2.
[504] Recital 26 MiCA

(c) deposits as defined in Article 2(1), point (3), of Directive 2014/49/EU of the European Parliament and of the Council;

(d) structured deposits as defined in Article 4(1), point (43), of Directive 2014/65/EU;

(e) securitization as defined in Article 2, point (1), of Regulation (EU) 2017/2402 of the European Parliament and of the Council.[505]

We find this part a little problematic as MiCA does not provide any guidance on the relationship of MiCA and does not provide any instructions on such qualifications, which could be a source of problems in the future. In example in the case of the above-mentioned Tether.

Further pursuant to article 2(3) MiCA also does shall not apply to certain entities and persons. Among those listed are the European Central Bank, national central banks of the Members States, but only when acting in their capacity as monetary authorities or other public authorities, persons who provide crypto-asset services exclusively for their parent companies, for their subsidiary or for subsidiaries of their parent companies, the European investment bank, the European Financial Stability Facility and the European Stability Mechanism, and others.[506]

According to article 2(1) of MiCA the regulation then applies to persons that are engaged in the issuance of crypto-assets or provide services related to crypto-assets in the Union.[507] For the sake of completeness, *"'crypto-asset service provider' means any person whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis."*[508] We find this broad approach correct as MiCA should apply on the Digital Asset service provides as well as issuers for which we have made case above that

[505] Article 2(2) MiCA
[506] Article 2 (3) MiCA
[507] Article 2(1) MiCA
[508] Article 3(1)(8)

both of those use and abuse the Digital Asset environment. Further, given the international and borderless nature of Digital Assets MiCA is likely to have even broader territorial influence.

6.2.2. Quick overview of some of the rules pertaining to Stable Assets and Crypto-Assets

As we have said above this part should not be a thorough review of the MiCA regulation however, we find that despite the different regulator approach to different types of Stablecoins, MiCA set some generally applicable rules to Stablecoins, which we feel are worthy of mentioning. In some cases, such as the following the requirement are the same even for Crypto-Assets. However, MiCA creates a set of new rules especially regarding the asset referenced tokens, in some other cases it links to existing regulation. In example regarding e-money tokens it often references to EMD2.

Issuers for each Crypto Asset must prepare and publish a White Paper, even if its contents are different for each of the issuer respectively.[509] While the contents of White Papers are quite specific under MiCA, we can summarize it as providing sufficient information about the project, information on the issuer, technologies, and standards, but also information relating to the functioning of the projects and rights of the asset or token holders and so on. We believe this will be important addition to the transparency of the Digital Asset environment as potential users will have necessary information to evaluate the quality of the product and the issuers should be liable for the contents of the White Papers.[510]

Further the issuers of Stablecoins must be authorized to offer such Digital Assets to the public. In case of an issuer of Asset-referenced tokes the competent authority is the corresponding EU member state: "*No issuer of asset-referenced tokens shall, within the Union, offer such tokens to the public, or seek an admission of such assets to trading on a trading platform for crypto-assets, unless such issuers have been authorized to do so in accordance with*

[509] Article 4(1)(d), Article 16(2)(i), and Article 46(1)
[510] Article 14, Article 22, and Article 47.

Article 19 by the competent authority of their home Member State."[511] In case of Issuers of e-money tokens, article 43(1)(a) provides: "*No electronic money tokens shall be offered to the public in the Union or shall be admitted to trading on a trading platform for crypto-assets unless the issuer of such electronic money tokens: is authorized as a credit institution or as an 'electronic money institution' within the meaning of Article 2(1) of Directive 2009/110/EC."*

In case of the catch all category – Crypto Asset no registration seems to be necessary, however: "*Issuers of crypto-assets, other than asset-referenced tokens or e-money tokens, shall publish their crypto-asset white paper, and, where applicable, their marketing communications, on their website, which shall be publicly accessible, by no later than the starting date of the offer to the public of those crypto-assets or the admission of those crypto-assets to trading on a trading platform for crypto-assets. The crypto-asset white paper, and, where applicable, the marketing communications, shall remain available on the issuer's website for as long as the crypto-assets are held by the public."*[512] Therefore the issuer of Crypto Assets must publish the White Paper, for which contents is responsible for the public to see, before offering Digital Assets to the public or before seeking admission to trading on a trading platform.

Issuers of asset-referenced tokes are further required to keep the higher of at least EUR 350 000 or 2% of the average amount of the reserve assets[513], which the issuer of shall keep in accordance with the article 32 of MiCA. Regarding the issuer of e-money token the MiCA does not explicitly provide any requirements, but EMD2 in its article 5 imposes similar requirements on electronic money institutions. We think this requirement is also very good as even the Stablecoins proved to be problematic and therefore the minimum own funds requirement will most probably prove worthy.

[511] Article 15(1)
[512] Article 8(1) MiCA
[513] Article 31(1) MiCA

6.2.3. Quick overview of some of the rules pertaining to Crypto-Asset service providers

Crypto-asset services are defined quite broadly MiCA: means any of the services and activities listed below relating to any crypto-asset: (a) the custody and administration of crypto-assets on behalf of third parties; (b) the operation of a trading platform for crypto-assets; (c) the exchange of crypto-assets for fiat currency that is legal tender; (d) the exchange of crypto-assets for other crypto-assets; (e) the execution of orders for crypto-assets on behalf of third parties; (f) placing of crypto-assets; (g) the reception and transmission of orders for crypto-assets on behalf of third parties; (h) providing advice on crypto-assets.[514]

Once again, we must judge the broad scope of MiCA in regard to Crypto Asset services providers positively, because as we have shown in the previous chapters the unregulated services providers are causing incentives for criminals unless such providers are committing the crimes themselves.

The crypto-asset services shall be provided only by legal persons.[515] Further, such person have registered office in a Member State of the Union and must have been properly authorized.[516] The authorization will be provided by the competent authority of the Member State where they have their registered office.[517] Further, the competent authorities shall inform the European Securities and Market Authority of awarded authorizations. "*Competent authorities shall inform ESMA of all authorizations granted under this Article. ESMA shall add all the information submitted in successful applications to the register of authorized crypto-asset service providers.*"[518] Thus strengthening the supervision. Under certain conditions, the competent authorities can, of course, withdraw the granted authorization to operate as crypto-asset services provider.[519]

[514] Article 3(1)(9) MiCA
[515] Article 53 (1)
[516] Article 53 (1)
[517] Article 54(1) MiCA
[518] Article 55(6) MiCA
[519] Article 56(1) MiCA

Besides the authorization requirement and other provision what we find as needed addition to the regulation of crypt-asset services providers some of their other obligations found in Title V, Chapter 2. In light of the evaluation of Digital Asset service providers in the previous chapter the article 59 stands out:

1. Crypto-asset service providers shall act honestly, fairly and professionally in accordance with the best interests of their clients and prospective clients.
2.Crypto-asset service providers shall provide their clients with fair, clear and not misleading information, in particular in marketing communications, which shall be identified as such. Crypto-asset service providers shall not, deliberately or negligently, mislead a client in relation to the real or perceived advantages of any crypto-assets.
3.Crypto-asset service providers shall warn clients of risks associated with purchasing crypto-assets.
4.Crypto-asset service providers shall make their pricing policies publicly available, by online posting with a prominent place on their website.

We also find very relevant the additional requirements such as the prudential requirement under the article 60 of MiCA regarding capital safeguard, article 63 of MiCA safekeeping of client's crypto-assets and funds, but also the article 65 of MiCA that requires the disclosure of conflict of interest.

6.2.4. Synthesis

While we find the MiCA regulation generally good, it would require more time to evaluate, and we leave that to further research, as MiCA regulation was revealed after we have done most of our research and we have added it for the sake of completeness. Further, we can generally state that the comprehensive regulation offered by MiCA would resolve majority of the above-mentioned problems associated with Digital Assets. Especially, the mentioned market manipulation and misrepresentation of Digital Assets. Additionally, we believe that the MiCA presents strong case of protection to customers and also new supervision to Digital Assets both on national and Union lever. We are pleased with the broad and strict approach as otherwise

we do not feel the Digital Assets generally would be worthy of keeping legal. In short, we have basically only two issues with the regulation, even if there might be more under specific research.

We believe that the regulation should have been completely dedicated to the Digital Assets (crypto assets) as any reference and connection with the existing regulatory regime may be problematic, due to the novelty of the issue at hand, which have proven in the chapter with American approach. Second, the regulation does not address or provide regulatory response to the ongoing decentralized finance, which we see as a future issue, as we believe that the criminal element could migrate towards decentralized platforms.

7. Thesis Summary and Conclusion

7.1. Summary

In this Thesis we address still quite a recent phenomenon of Digital Assets in general fashion. In the simplistic way of a statement, we ask, whether Digital Assets serve any purpose. The motivator for such question is derived from aspects that were somehow intrinsic to Digital Assets when we started composing this paper. We are talking about technologically complex digital solution of trustless payment systems functioning over the Internet that promised revolution in payment technology, however, are widely abused by criminal element. Further, the questionably legitimate use of Digital Assets that prevailed was not the payments, but rather unregulated and risky investments.

In those thoughts in mind, we have begun the research and composure of this Thesis. As we have understood Digital Assets more thoroughly, we have determined the areas of research, which we have presented in the Thesis introduction.

Before we have approached the factual areas of research, we had to present to the readers the very basics of this Thesis, to help them ease into the fairly complex topic. We therefore added a chapter called General Explanations, where we mainly discuss, why we are using the connotation Digital Assets.

In the chapter we argue that the view on Bitcoin and similar projects as a “Virtual Currency” is unfitting, for wide variety of reasons. We further continue to describe such reasons. Besides the reason that we feel that the word virtual is not fitting for what Digital Assets encompass, we make other more relevant points. We argue that since Bitcoin and most of the similar projects does not satisfy the basics definition of money, but also because only a very limited number of its users actually uses it for payments, it should be looked upon in different light. Further we argue that the use of the word “currency” is then misleading and confusing. We therefore propose the connotation Digital Assets. For which we are pleased to recognize that the current

regulatory approaches use either “Crypto-Assets” in the European environment and “Digital Assets” in the regulatory environment of the United States of America. Therefore, we believe it was a correct method to approach Bitcoin and similar projects in a broad way.

Since, at the beginning of the research the whole Digital Asset environment was still at the early developments, as the inception happened less then 10 years ago, we decided to dedicate a part of the thesis to historical development of Digital Assets. Therefore, we have posed the first research question. Can the history of Digital Assets help us with its understanding and with regulatory approach?

To this question we can generally answer yes, providing the specifics below. We have researched the previous attempts to develop private payment systems. Founding that there was a wide variety of such projects. Therefore, the invention of Bitcoin was not a revolution, but rather a stable evolution. From those above mentioned attempts we have chosen four, which we believed to have impacted and influenced the developer of the first Digital Asset – Bitcoin. Those projects were E-Gold, eCash, B-Money, and Bit Gold.

We subsequently described those projects with accent on its technical solutions and where possible also on the authoritative response. Further, we have noticed that all of the described projects had have in common a political aspect. The creators and developers behind the projects believed that then current financial system is conceptually wrong, they disagreed among others with fiat money inflation, central banking, the use of intermediaries in commerce and finance, and the lack of anonymity generally and in transactions specifically.

While evaluating the historical concepts, we have found that even before the private payment systems were decentralized, it was already an interesting environment for criminal minded users. The case of E-Gold has proven that a functioning private payment system, without a sufficient regulation will be immediately abused. Since E-Gold itself, apart from using the Internet, did not

present any revolutionary technical ideas, there was no sufficient regulatory response, and the project was only discontinued following court's proceedings.

Using the following projects as examples, we then continue to describe the evolution of decentralized payment system, with accent on transactional functioning and money creation. In the projects called eCash we describe how the cryptography allows for completely anonymous transactions. Further, we use the two purely theoretical concepts of B-Money and Bit Gold, to introduce the technology that allows for decentralization. We focus on the Hash function and Proof-of-Work function. Especially, the Proof-of-Work function is relevant as it allows for creation of valuable digital files, which then could be used a medium of exchange. Which is then the case of the first Digital Asset – Bitcoin. We derive, that the developer of Bitcoin must have been aware of the previous technological development and use some of it in his creation. In this sense, at the end of the chapter we provide a short overview of the Bitcoin functionality.

To answer the posed question, we summarize that the historical development reveals, that for over 20 years Developers were trying to create an anonymous payment system functional without trusted third party, which on one side is a technological step ahead, however since those developers have voiced their disagreement with the financial system, we also derive that they were trying to develop a trustless anonymous payment system removed from the existing financial regulatory approach as without an operator, there would not be a directly responsible person. Thus, we conclude that the history of Digital Assets does provide valuable insights in the material reasons for its conception as well as motivation and functioning. We believe that any repressive actions, but also regulatory actions should take in account that the decentralization was also conceived as a shield against legal responsibility.

In the next chapter we focus readers on the technological aspects of Digital Assets. The reason why we dedicated a part of the Thesis to this topic is that the function of Digital Assets may be hard to comprehend, and thorough explanation is in our opinion needed. Therefore, it allows us to address the second research question – what are the technological

aspects of Digital Assets. Subsequently, it allows us to write more freely without unnecessary technological explanations in the second more practical part of the Thesis.

In the technical part we therefore start with the introductions of Distributed Ledger Technology, explaining that it is essentially a distributed database, and that any information contained in such distributed database is located at multiple mutually interconnected in participating data storages. We add explain that the widely used backbone of Digital Assets, the Blockchain is its subtype. We explain that Blockchain is a tool used for organization of incoming of data sets (blocks) that are then located on a common ledger that is kept in distributed fashion. We further add that Blockchain uses algorithmic and cryptographic methods to keep the data inside immutable and temper resistant. We further divide Blockchain based on who is allowed to participate, which means who is allowed to add new data to the Blockchain. Thus, introducing the concept of Permissionless Blockchain, which is completely open for participating and is used in example in Bitcoin and Permissioned Blockchain, which has regulated access and requires certain conditions to be satisfied prior to its use. Permissioned Blockchains have better use in business environment, whole the Permissioned Blockchains are usually governed by an authority, it still operates on trustless basis. We then continue to describe various elements that Blockchain uses. We draw readers attention to Blocks, Hash Functions, the Cryptography used in Blockchain, the functioning of transactions and what further explain what the consensus models.

Towards the end of the technological part, we address the Blockchain technology impacts and the proposed impacts. Therefore, explaining its influence on society. There currently recognized the three stages of Blockchain impact. Those stages are referred to as the Blockchain 1.0, Blockchain 2.0, and Blockchain 3.0.

We then briefly introduced those stages. Blockchain 1.0 refers to the first generation and application of Blockchain technology, meaning to the occurrence of Digital Assets such as Bitcoin, Ethereum, Litecoin and others. It primarily focuses on the trustless nature

of Blockchain as it allows to transfer the value among its participants. Blockchain 2.0 is then where we as a society should be now, it described the penetration of the Blockchain and Distributed Ledger Technology into areas, which have a long-established existence, but could be improved by the Blockchain. We argue that such areas could be also the area of finance, such as the securities trading, payment clearing, remittance and other. Further, other authors see its use in international transport or in example health. For the sake of completeness, the Blockchain 2.0 also encompasses the smart contracts, smart property, decentralized applications, decentralized organizations, and so on. While we mention the decentralized organization in the next chapter, we otherwise do not work with the Blockchain 2.0 in this Thesis. Last, we briefly describe the proposed Blockchain 3.0, which is a futuristic conception of Blockchain based society. As we argue in the very last part, we focus the rest of the Thesis primarily on the Blockchain 1.0 conception, which means the Digital Assets that provide monetary and investment functions.

The Thesis then continues with more practical part. We follow the posed research questions and in the first part we research, what the actual use of the Digital Assets is. We begin with evaluation of the promise that Digital Assets bring. It is said, among others, that Bitcoin and other have the potential to help the world with international monetary transactions, financial inclusion and user and internet anonymity. The reality proves to be different at best. The internet media is full of articles promoting various Digital Assets projects, which number is continuously growing. Groups of people are explaining to each other the benefits of decentralized and trustless nature of Digital Assets often arguing its technological superiority.

However, according to us such promotion exists only because people are motivated by the financial gain, they can derive from allocating fiat money in Digital Assets. We quote various studies that show that majority of Digital Assets transaction is connected only with risky investments. Only about 7% of the Bitcoin transaction are connected with actual monetary transfers, where about 20% of those are then of international character. Further even smaller part of transaction leads to Digital Assets being spent with merchants, in fact it is less

than 2%. In this sense we highlight the unprecedent influx of money that is being spent on Digital Assets. We describe that the whole Digital Asset market is completely unstable, and the value of Digital Assets is changing rapidly. We highlight that this unreasonable craziness is now also supported by wholesale professional investors. We therefore partially answer the research question regarding the actual use of Digital Assets, where we argue that nobody really uses them for payments, rather only for risky investments.

Because it is not a secret that Digital Assets and the providers of associated services are often victims of thefts, hacks, and other crimes, we also dedicate question the use of Digital Assets in this sense. We therefore continue the previous research question and also ask whether the Digital Assets and associated service providers used or abused for criminal activity. Given our previous finds from the historical chapter, where the developers wanted to create the trustless payment systems exempt from the financial system, we are also looking at examples of special services existing solely for criminal use.

Before we approach the evaluation of different services, we are explaining to the readers, what is making the Digital Assets such a good target for criminal abuse, by compiling the core characteristics and aspects of Digital Assets in this sense. We are finding that the characteristics are: the technical complexity, the lack of trusted third party, the partial anonymity, the borderless nature of Digital Assets and associated services, the finality and irreversibility of transactions, and of course the lack of sufficient regulation.

We summarize that the technical complexity is two sided. On one side, we believe that the majority of Digital Assets use does not completely understand the functionality of Digital Assets and therefore any flaws of Digital Assets and associated services can be abused. Additionally, we support this by stating that the user interface on such services or Digital Assets itself is done intuitively and thus people are able to use Digital Assets without understanding them and that further makes them vulnerable even more.

Next, we describe the problem of the lack of trusted third party, where we highlight that especially with permissionless Digital Assets, there is no one in charge and therefore cannot be brought to responsibility for any acts. We also highlight that in example anti money laundering regulation depends on cooperation with the intermediaries, who operate such services.

With partial anonymity aspect we summarize that a person is able to operate in Digital Assets without revealing her identity, and that creation of accounts and wallets does not require any cooperation from entities. Even if the partial anonymity of certain Digital Assets has been debunked, as with certain methods as is IP analysis, the anonymity could be theoretically revealed. We point out that using additional methods, which masks the users IP address such as the onion router the Digital Assets environment participants may achieve a complete anonymity.

We continue to describe the borderless nature of Digital Assets and associated services. Where we summarize that such services can be used from anywhere, where there is the Internet connection. Which means that the criminal activity can be happening internationally, but also cause the venue shopping, where the services can choose to incorporate in jurisdictions that have lax or lacking the corresponding regulation.

Regarding the finality and irreversibility of transactions, we explain that the Digital Assets have a similarity with cash payments, that once the transaction has been carried out, the exchange is final and since there is no intermediary a trusted third party, no one will likely help with such transaction. Finally, we address the fact that still there is no effective and comprehensive regulation.

Explaining the core aspects, we continue to provide some practical examples of services using Digital Assets, which only purpose is criminal. We introduce the case of Silk Road Online Marketplace. Silk Road was a service operating on the Deep Web, in its sub part that is often regarded as Dark Web. Dark Web, while part of the general Internet, is different from the Internet

most of the readers would know, instead of using the Internet search engines such as Google, the users have to use specialized services (such as the above-mentioned onion router) and know the address of the online point they are looking for exactly. Silk Road was then marketplace in the actual meaning of the word marketplace.

Silk Road allowed for obtaining controlled substances, illegal services, and other illicit goods. The only possible payment method was Bitcoin because it had no supervision and allowed for anonymous transactions. We are arguing that those modern Dark Markets can exist thanks to the invention of Bitcoin, as it is a crucial service without which, such marketplaces would be easily discoverable via the money trail. Silk Road itself was not selling any illicit products but was working only as a middleman. Once the buyers transferred bitcoins to Silk Road the market would keep them in escrow and wait for the seller to send the goods using post office. It is of course obvious that in case of the Silk Road Online Marketplace the Digital Assets and the service are used and built respectively, only for committing crimes. The only purpose is therefore criminal.

In connection with the Silk Road Online Marketplace, we evaluate other Digital Asset service, which shows to have basically only criminal purpose. This service is called Digital Asset Tumbler and offers to hide the above-mentioned paper trail. We have already explained that even if Digital Assets offer certain level of anonymity, there are services, which can completely hide the origin of Digital Assets. This is one of them. We explain the functioning of Digital Asset Tumblers and its impact on anti-money laundering enforcement. For the purposes of this summary, we can again compare the Digital Asset Tumbler to a bowl of rice. Those mixers therefore work in a similar fashion as if someone takes three seeds of rice and puts them in a bowl full of rice. Proceeds to mix thoroughly the bowl and gives and take some three seeds of rice (minus commission) out of the bowl. Therefore, obtaining Digital Assets of completely different origin. That means that those Digital Assets will also have completely different paper trail. Despite showing one example of legitimate use of those mixers, we also have to conclude that there is only criminal use, and it was developed with such intentions. Throughout this section

of the Thesis, we also follow the legal proceeding held against Ross Ulbricht the developer of Silk Road. We provide summary of the case, and review the Court argument, which finds that Bitcoin can be used for money laundering.

Ensue a short chapter, where we evaluate if even the very basic process of obtaining new Digital Assets, probably better known under mining, could serve as a tool for money laundering. We assert, that since the remuneration for adding a new block is quite high. Which of course differs in case of different Digital Assets and also in Time. Plus, the equipment for mining can be bought of the internet without any know your customer requirements. We think it could be possible to use stolen Digital Assets, purchase the equipment for mining and use to launder the stolen Digital Assets. While we conclude that such approach is possible, we summarize that there are likely better ways and focus readers attention to Digital Asset exchanges and its role in abuse of Digital Assets. We must conclude that while mining for Digital Assets is legitimate part of the Digital Asset economy it could still be abused as a strategy for money laundering.

As mentioned above, in the following part we focus on the activity of Digital Asset Exchanges. First, we provide definition of Digital Asset Exchange. Stating that it is a platform that provides its users with the possibility to trade Digital Assets for other Digital Assets or fiat money. Further we describe its division between centralized Digital Assets Exchanges and decentralized Digital Asset Exchanges, stating that the main difference between them is whether such exchange is governed by a company or an individual. As decentralized Digital Asset Exchanges are still a quite new phenomenon we focus on the centralized exchanges.

We continue by evaluating whether the role in of Digital Asset Exchanges is criminal activity is incidental or whether the exchanges knowingly participate in criminal activity. We begin by explaining how easy it is to use Digital Asset Exchange for different part of money laundering, given that the perpetrator is using stolen Digital Assets. We make analysis of the placement of such Digital Assets on the Digital Asset Exchange, further we are evaluating and suggesting using Digital Asset Exchange for the process of layering and integration. Since this part

of the Thesis was based on one of our articles, we also compare how the situation have developed since we have published the article. We reach a partial synthesis that such process is still possible, for which we cite recent developments. Nevertheless, we cannot answer the question, whether Digital Asset Exchanges are participating on the ongoing criminal activity intentionally.

Therefore, we provide subsequent analysis, where we compare some of the Digital Asset Exchanges that purposefully subordinate itself to the current regulation to those that chose to incorporate outside of the United States jurisdiction. We decided that we could use the volume, meaning the overall value of trades ongoing on such exchanges and compare, which Digital Asset Exchanges have the volume higher. Thus, we have used data from the past 6 months looking at the average volume on four Digital Asset Exchanges. We find that exchanges incorporated outside of the United States have extensively larger volume then those incorporated and licensed in the United States, thus partially derive that it is beneficial for the operators of Digital Asset Exchanges to utilize the borderless nature of Digital Assets take advantage of regulatory less strict environments. Given we still felt like we could not decisively answer the question, whether Digital Asset Exchanges are just abused by criminals or itself operate for the criminal purpose, we continued with the research. We were looking into allegations of the abuse of Digital Asset Exchanges, and we found reports that those exchanges participating in market manipulation, Wash Trading and even money laundering. We therefore decided to further focus on the issue of Wash Trading.

We first explain the legal term of Wash Trading. Providing a few definitions, for this summary we find relevant to provide the following part. Wash Trading involve the use of techniques designed to give the appearance of submitting trades to the open market, while negating the risk or price competition incident to the market; wash trading produces a virtual financial nullity because the resulting net financial position is near or equal to zero, and such transactions are considered harmful because they create illusory price movements in the market.

Since we have a practical experience with Wash Trading as we have been monitoring a smaller Digital Asset Exchange for about two years. We then provide a practical example related to Digital Assets Exchange called COSS. Explaining how we found out that the Wash Trading is going on and what were the implications. We then argue that our approach was only possible due to the limited volume happening on COSS Digital Asset Exchange and continue using other's authors more professional methods. We introduce reports, where the used methodology was to compare the stated volume with incoming web traffic. Such approach allows to determine, whether there is enough participants (traders) that could actually cause such volume. From those reports we then highlight some of its most incredible findings such as the now discontinued exchange called Coinbene, which reported volume over $220 000 000 on a trading pair, and the report have shown that the reality was just $3 000 000, which is difference of about 98%. We further describe a case where the Digital Asset Exchange even build its matching engine, which is a technical part of any exchange, which shall prohibit the buying of your own orders, to allow such trades.

To conclude this subpart and decide whether the Digital Asset Exchanges are being abused or whether they do such activity intentionally we evaluate what would be the benefit for Digital Asset Exchanges. We find that Digital Asset Exchanges do benefit from the artificially inflated volume. We argue that the volume of such exchanges serves as one of the main decisive factors for customers in the Digital Asset environment, therefore the higher the volume the more likely the customers would use the exchange as there is much higher chance of successful trade. Therefore, we assert that the Digital Asset Exchanges could use the inflated volume to attract additional business. Further, we argue that the exchanges charge listing fees (as high as $ 1 000 000) for adding a new Digital Asset to its platform and therefore could misrepresent the volume to attract new projects being listed on their platform. Given the example of COSS we also add that the exchanges could do so to raise value of Digital Assets they issue. Given the above said, we conclude that we have Digital Assets Exchanges have sufficient reasons to misrepresents the data and thus we have a good reason to believe some Digital Asset Exchange also use Digital Assets in criminal way. We further provide short legal analysis of the conduct, stating that most

likely such Digital Asset Exchange are committing various frauds, judged by the New York and Florida law, we further state that the posed issue would likely amount to different security frauds, but given the state of regulation and the broad variety of Digital Asset products we cannot do the proper analysis, but we address the reasons and similar issues in the following chapter.

Successively we are addressing the regulatory response regarding Digital Assets in the United States of America. Therefore, the question to what extend are Digital Assets Integrated in the Current Regulatory Framework? We begin by describing the Security Exchange Commission. SEC is an independent federal agency, which serves a three-part mission; (1) to protect the investors, (2) maintain fair, orderly, and efficient markets, and (3) facilitate capital formation. We further introduce that we will be most concerned with its powers over offering and sales of new securities and introduce some of SEC's powers under the Securities Act of 1933 and Security Exchange Act of 1934. We continue to summarize SEC's approach to Digital Asset, reviewing whether SEC considers Digital Assets securities.

We base the further analysis on practical example, which is derived from the DAO incident. We explain that the DAO incident was a combination of unregistered raise of capital in the form of initial coin offering and security breach in the form of a hack. In this sense we briefly explain what initial coin offering, better known as the ICO is. We explain that it is a raise of capital in exchange for Digital Assets, which while offering some benefits, such as lower costs, increased transparency, and additional liquidity, was rather dangerous for its uncertainty and associated scams. Further, we explain what the DAO was. We summarize that it is a virtual organization embodied in computer code and executed on blockchain. The Purpose of the very first DAO, which was back then simply named DAO, was to create a unique entity encoded into blockchain that would control funds denominated in the Digital Asset Ethereum and act like an independent investor or an authority in the Digital Asset environment. Its investors would then share profits should there be any. To obtain funds for the activities DAO held a public sale of DAO tokens. During the sale DAO sold over 1 billion of so-called DAO tokens for approximately $150 000 000.

There were two main problems, which caught the attention of the SEC, first it was the massive amount of the capital raised, and second came fourteen days after, when a hacker found vulnerability in the code and siphoned about $70 000 000. Since SEC has jurisdiction over the raise of capital and the Securities Act prohibits unregistered offer and sale of securities in the interstate commerce, SEC began investigation regarding the applicability of U.S. federal laws to the offer and sale of the DAO tokens. Further, SEC was concerned to find, whether the DAO tokens amount to securities.

To prove that the DAO tokens are in fact securities SEC used the catch all part of the security definition, the investment contracts. Since the investment contract is defined by judge made law, we then present its definition to the readers. An investment contract is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. We further explain to the readers that the definition of investment contract gave rise to the Howey Test and that Howey Test is used when one is evaluating whether an asset could amount to security. We continue to describe the single prongs of the test, for which we present additional case law. For the sake of completeness, the prongs are 1. investment of money, 2. common enterprise, 3. reasonable expectation of profits, and 4. the entrepreneurial and managerial effort of others.
As one of the prongs of the Howey Test is the investment of money, SEC further verified, whether the raise of capital, which was done in the Digital Asset Ethereum can satisfy the requirement of money. SEC bypassed the requirement of money quoting Uselton v. Comm. Lovelace Motor Freight, Inc.: "[…] it is well established that cash is not the only form of contribution or investment that will create an investment contract." SEC thus argued that Ethereum is: "[…] the type of contribution of value that can create an investment contract under Howey. SEC subsequently finds that the DAO token is a security, as it satisfies all of the four prongs of the Howey Test. However, we add that the vast majority of Digital Assets does not pass the Howey Test. Therefore, in example Bitcoin or Ethereum is not security as they do not satisfy the last two prongs.

Successively, we continue with the evaluation of the Commodity Futures Trading Commission approach to Digital Assets. We begin by introduction of the Commodity Futures Trading Commission also known under CFTC, stating it is also an independent federal agency of the US government. U.S. Congress formed the CFTC in 1974 by enacting the Commodity Futures Trading Act of 1974. We further state that CFTC regulates commodity futures trading (derivates relating to commodities) in the United States. The Commodity Futures Trading Commission is also one of the most vocal and active authority in the US regarding Digital Assets. The core of CFTC power is embodied in the Commodity Exchange Act of 1936 and has exclusive jurisdiction regarding transactions involving commodity interests. The Commission is thus the CFTC is able to assert jurisdiction over Digital Assets interests if Digital Assets amount to commodities as it would be essentially commodity interests.

We therefore continue with analysis, whether Digital Assets could be classified as commodities. Luckily, the concept of a commodity in the United States is understood broadly under the Commodity Exchange Act. First the act lists a wide variety of agriculture products, with the exception of onions and then adds more " […] goods and articles […] and all services, rights, and interests […] in which contracts for future delivery are present or in future dealt in." Under this definition commodity can be all sort of things (except the above-mentioned onions and also movie tickets). Given the broad spectrum of the definition, without any further explanation the CFTC rules that Bitcoin can amount (and in this sense any Digital Asset) can be considered commodity. We follow the case of the platform Derivabit, operated by corporation Coinflip Inc. It facilitated connection between the buyers and sellers of standardized Bitcoin options contract as eligible for trading. In that sense CFTC then verifies whether the above-mentioned Bitcoin Futures can be considered an option contract pursuant to the Commodity Exchange Act. CFTC finds that yes and asserts jurisdiction over Digital Asset derivates. Subsequently stating that the Derivabit platform should have been registered with the CFTC. We then provide additional information on the CFTC approach.

In the next subchapter we shortly summarize the approach of Internal Revenue Services, known also as the IRS. Since IRS is concerned with tax income only, it does not really provide any reasoning and pronounce Digital Assets to be a property.

We the offer a synthesis of the posed question arguing that the United States approach is not a priori restrictive, but that it seems that the US is aware of the ongoing issues. We further argue that the current situating is problematic as this fragmental approach causes a number of issues. We are giving examples in connection with the areas we have addressed so far. In example we are arguing that while SEC could normally regulate the ongoing Wash Sales, but since it derives its power, in this case, from the IRS provided definition it has to look on Digital Assets as property, and property is not subject to the ban on Wash Trading. Similarly, the CFTC can regulate the derivate Digital Asset markets, but cannot do the same in connection with spot markets.

We thus suggest some improvements. We believe that the proper response should be a federal regulation of Digital Assets. However, this seems to be generally problematic in the United States. Two bills have already been proposed. First being the "Virtual Currency Consumer Protection Act of 2018" addressing price manipulation and protection of the investors and also suggesting CTFC's supervision over the market and the second being the "Virtual Currency Market and Regulatory Competitiveness Act of 2018" talking about the general regulation of Digital Assets, clarification of their legal status and most importantly giving CFTC more rights to improve the growth of the adoption of Digital Assets. In 2022 none of those Bills have been passed.

In conclusion we believe that any federal law that would regulate the Digital Asset in the United States should focus on the problems outlined above, but also create a new authority with exclusive jurisdiction over the Digital Assets, as the division between SEC, CFTC, and IRS apparently causes problems. Define Digital Assets in federal law using technical analysis, because once again the current regime is too complicated and there are likely examples when Digital Asset satisfies each of the prongs of the above-mentioned agencies meaning being

Security, Commodity, and Property. The above-mentioned new authority should also have exclusive jurisdiction over the secondary trading of Digital Assets.

Given the conclusions to the previous question, we do not find Digital Assets as a particularly useful phenomenon, we further describe the only subset, which we believe makes any sense. Further, during out research a new proposal for a comprehensive regulation was proposed in European Union, we therefore also provide its short review. Next, we thus address the phenomenon of Stablecoins. We shortly introduce Stablecoins from the historical point of view, where we mainly argue its growing relevance and describe the reasons for its development. We then proceed to explain what Stablecoins are. Stablecoins are Digital Assets that are designed in a way that allows them to maintain a stable value against a target price, while highlighting some of its benefits Besides offering and bringing stability to the Digital Asset economy it seems that stablecoins might have quite a few of innovative characteristics, some of which it partially shares with other distributed ledger technology based Digital Assets and some that it brings on its own. A fully functioning and legal concept of Stablecoin could introduce so called smart money (programable money), higher efficiency in payments through its 24/7 availability, borderless character, ability to employ smart contracts, micropayments, and fractioning. As well as financial inclusion for less developed regions in the world. We believe that the main difference from the above-described Digital Assets such as Bitcoin, which makes Stablecoins interesting is that Stablecoins are not conceived with limited supply. Therefore, do not motivate its user to hold them and wait for value increase, but rather actually use them.

We then provide a technical division of Stablecoins. General dividing line between Stablecoins could be draw based on the fact, whether such stablecoins are backed by assets and if so, by what kind of asset. For the purposes of this Thesis, we decided to divide stablecoins depending on its stabilization mechanism. We provide the division of Asset-Backed Stablecoins, which can be further divided based on whether the collateralized asset is a traditional asset or rather a Digital Asset such as Bitcoin, or whether such collateral is mixed. We also mention

that some Stablecoins projects promise a working solution based on an algorithm. However, we show that algorithmic Stablecoins are not the best choice as of now.

We then argue that under the current (European) regulatory framework some stablecoins might be regulated under the Second Electronic Money Directive. Whether a stablecoin could fall under the EMD2 definition of electronic money depends on the technical background (back end) of such stablecoin. The decisive factor seems to be whether such stablecoin represents a contractual relationship between the issuer and a customer amounting to IOU. We follow the example of a fiat backed Stablecoin Tether and explain that due to its character Tether could be considered electronic money under EMD2, its and the operator of Tether might be under certain obligations. However, since Tether can also be used as a form of investment transferred over blockchain, where the contractual relationship between issuer and customer could be diminished, it could be also considered e-money token under the below mentioned regulation.

Subsequently, we introduce the new proposal of the regulation of the European Parliament and the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, which should be a general response to the quickly developing Digital Asset technology and more importantly a prime regulation on stablecoins. MiCA introduces new definition of stablecoins and additional obligations for stablecoins issuers depending on its type and significance. The MICA proposal has been enacted with four general and related objectives: 1. Legal certainty, 2. Support innovation, 3. Instill appropriate levels of consumer and investor protection, and 4. Ensure financial stability. We further bring overview of MiCA's subject matter, scope and its approach to Digital Assets. We explain its main definitions such as what is Crypto-Asset, Asset-Referenced Token, Electronic Money Token or E-money Token, Utility Token, and Crypto-Asset service providers. We explain some of the differences between the conception of different tokens. Regarding the scope of MiCA, we explain that we find problematic the exclusion of MiCA in connection with some financial instruments, securitization, structured deposits, and electronic money, as MiCA does not provide any guidance on such exclusion.

We continue with description of certain new rules that would apply to Stablecoins, where we highlight that MiCA brings a completely new set of rules primarily for Asset-referenced tokens in some other cases it links to existing regulation. In example regarding e-money tokens it often references to EMD2. We proceed to explain the need of issuer to prepare and publish a White Paper. While the contents of White Papers are quite specific under MiCA, we can summarize it as providing sufficient information about the project, information on the issuer, technologies, and standards, but also information relating to the functioning of the projects and rights of the asset or token holders and so on. We believe this will be important addition to the transparency of the Digital Asset environment as potential users will have necessary information to evaluate the quality of the product and the issuers should be liable for the contents of the White Papers. We also explain that the issuers of Stablecoins will have to be authorized to offer such Digital Assets to public and provider the specifics for different types. To this extent we also mention the need to retain reserve assets.

We also address a few rules pertaining to crypto-assets service providers. Crypto-asset services are defined quite broadly MiCA: means any of the services and activities listed below relating to any crypto-asset: (a) the custody and administration of crypto-assets on behalf of third parties; (b) the operation of a trading platform for crypto-assets; (c) the exchange of crypto-assets for fiat currency that is legal tender; (d) the exchange of crypto-assets for other crypto-assets; (e) the execution of orders for crypto-assets on behalf of third parties; (f) placing of crypto-assets; (g) the reception and transmission of orders for crypto-assets on behalf of third parties; (h) providing advice on crypto-assets. We judge the broad scope of MiCA in regard to Crypto Asset services providers positively, because as we have shown in the previous chapters the unregulated services providers are causing incentives for criminals unless such providers are committing the crimes themselves.

The crypto-asset services shall be provided only by legal persons. Further, such person has registered office in a Member State of the Union and must have been properly authorized. The authorization will be provided by the competent authority of the Member State where they

have their registered office. Further, the competent authorities shall inform the European Securities and Market Authority of awarded authorizations. “Competent authorities shall inform ESMA of all authorizations granted under this Article. ESMA shall add all the information submitted in successful applications to the register of authorized crypto-asset service providers.” Thus, strengthening the supervision. Under certain conditions, the competent authorities can, of course, withdraw the granted authorization to operate as crypto-asset services provider.

While we find the MiCA regulation generally good, it would require more time to evaluate, and we leave that to further research, as MiCA regulation was revealed after we have done most of our research and we have added it for the sake of completeness. Further, we can generally state that the comprehensive regulation offered by MiCA would resolve majority of the above-mentioned problems associated with Digital Assets. Especially, the mentioned market manipulation and misrepresentation of Digital Assets. Additionally, we believe that the MiCA presents strong case of protection to customers and also new supervision to Digital Assets both on national and Union lever. We are pleased with the broad and strict approach as otherwise we do not feel the Digital Assets generally would be worthy of keeping legal. In short, we have basically only two issues with the regulation, even if there might be more under specific research.

We believe that the regulation should have been completely dedicated to the Digital Assets (crypto assets) as any reference and connection with the existing regulatory regime may be problematic, due to the novelty of the issue at hand, which have proven in the chapter with American approach. Second, the regulation does not address or provide regulatory response to the ongoing decentralized finance, which we see as a future issue, as we believe that the criminal element could migrate towards decentralized platforms.

7.2. Conclusion

In the submitted Thesis we stated six research questions to address basic contemporary aspects of Digital Assets. Herein we provide the final synthesis resulting in relevant answers.

7.2.1. Can the history of Digital Assets help us with its understanding and with regulatory approach?

Yes, the history helps us with both elements. We found that even the forerunners to the current Digital Assets were developed with the intent to liberate themselves from supervision of the financial system regulation. Once such systems were functional, they were immediately criminally abused. As such, the regulatory approach should be strict.

7.2.2. What are the technological aspects of Digital Assets?

The distributed ledger technology is complex and hard to understand without special education in computer science. In our opinion, this complexity, combined with the absence of a central authority to oversee the operation of the Digital Asset, encourages numbers of well-educated offenders to commit crimes. The scale of this activity is increasing. In most cases, there is also no trusted third party to protect and help the victims.

7.2.3. What is the actual use of Digital Assets?

We find that Digital Assets are used for payment on minimal scale. The retail use of the most relevant Digital Asset Bitcoin is less than 2% of all its transactions. Digital Assets are primarily used as a risk asset investment. In our opinion, the motivation for investment of money into Digital Assets is their limited supply, technological promise, and wide misunderstanding of the market, which is fueled by endless and baseless internet promotion.

7.2.4. Are Digital Assets and associated services providers abused or used for criminal activity?

Both. Nearly every aspect of Digital Assets is abusable and abused, especially its anonymity and trustless nature. We show that in the current digital asset environment, it is better to either capitalize on the abuse or to use digital assets or their associated services directly for criminal activity. It is just more profitable. Digital Assets serve as a critical component of, thus allow for development of, services that are purely and intentionally criminal. Such as Dark Web Online Markets or Digital Asset Tumblers.

7.2.5. To what extend are Digital Assets Integrated in the current regulatory framework?

The situation is changing. When we started with the research, the regulatory response was essentially non-existent. Subsequently, becoming fractional but depending on limited jurisdictions of deciding authorities. At this time, we are on the verge of change. The era of fractional regulation, which is complicated, confusing and, frankly, fundamentally inadequate, seems to be coming to an end, and the era of regulation in the form of comprehensive codes is beginning to take shape. However, it is too soon to evaluate its impact as the first relevant proposal – MiCA is still not in effect. Further, we must add that the regulatory response is very slow.

7.2.6. Do Digital Asset make any sense as global payment systems?

With somewhat personal surprise, we have to say that currently no. Controversially, the immense criminal dimension is in our opinion not the main issue. We feel that it is just a child disease that is native to all new technology and could be solved with regulation. The main argument is that nobody seems to be using Digital Assets as a payment system. In this sense we argue that the colossal success of Bitcoin caused its failure. Bitcoin grew too quickly too valuable and sparked thousands of useless copies. Absolute majority of those altcoins have no use and exists only as a monument to hope of becoming rich. Those Digital Assets that were conceived with different than payment function in mind, are exploring the other possibilities of Blockchain rather than payment services and thus are not logically used as a payment system.

We believe that this approach holds the key to the future of Digital Assets. We honestly believe, that the Blockchain will still cause a revolution.

Finally, Stablecoins could be removed from the previous statement in future. Their conception is very close to electronic money, which is a conception that at least the European regulators know, have experience with, and if people will start using Stablecoins for payments, we believe it may grow to be a successful fintech.

References

Monographs

BAINS, Parma. Blockchain Consensus Mechanism: A primer for Supervisors [online]. International Monetary Fund, 2022, (Note 2022/003), 1-26 [cit. 2022-04-20]. Available at: https://www.elibrary.imf.org/downloadpdf/journals/063/2022/003/063.2022.issue-003-en.xml (Archived version available via: https://archive.ph/OKy0E)

BAKEŠ, M., Karfíková, M., Kotáb, P., Marková, H. et al. Financial Law. 6th revised edition. Prague: C. H. Beck, 2012, 549 p. at 335.

BLACK, HENRY, JOSEPH NOLAN a JACQUELINE NOLAN-HALEY at all. Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern. 2nd Reprint. United States of America: WEST PUBLISHING CO., 1990, 1-150. ISBN 0-314-77165-4. Available at: https://thelawdictionary.org/asset-2/ (Archived version available via: https://archive.ph/1iOrm)

BLACK, HENRY. BLACK'S LAW DICTIONARY: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern [online]. 4th Ed. Rev. WEST PUBLISHING CO., 1968 [cit. 2022-04-18]. Available at: https://heimatundrecht.de/sites/default/files/dokumente/Black%27sLaw4th.pdf (Archived version available via: https://archive.ph/GGcjS)

HAYEK, Friedrich. The Road to Serfdom. Fiftieth Anniversary Edition, 274 p. 205. Chicago USA: University Of Chicago Press, 15th 1994n. l. ISBN 9780226320618.

JOHN, Markoff. What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry. Penguin Books; Annotated edition, (28 Feb. 2006), 352 s. ISBN 978-0143036760.

LEE KUO CHEUM, David. Handbook of Digital Currency. Elsevier Books, 2015, 612 p, at 168 p., ISBN 0128021179.

MENEZES, A., van OORSCHOT, P. and VANSTONE S., Handbook of Applied Cryptography. Handbook of applied cryptography [online]. Boca Raton: CRC, 1997, s. 1-780 [cit. 2022-01-04]. CRC Press series on discrete mathematics and its applications. ISBN 0-8493-8523-7. Available at: https://cacr.uwaterloo.ca/hac/about/chap1.pdf (archived version available via: https://archive.fo/AR1Rm)

MONEY-LAUNDERING, Black's Law Dictionary (10th ed. 2014), ISBN 978-0314621306

RAJPUT, Dharmendra, Ramjeevan THAKUR, Syed BASHA. Transforming Businesses with Bitcoin Mining and Blockchain Applications. India, 2019, 282 p at 209. ISBN 9781799801863.

SWAN, Melanie. Blockchain: Blueprint for a New Economy. USA: O'Reilly Media, 2015 pp 152(9). ISBN 978-1491920497.

Articles

ABRAR, Waleed. Untraceable Electronic Cash with Digicash [online]. University of Konstanz, 2014, 1-3 [cit. 2022-01-02]. Available at: https://www.researchgate.net/profile/Waleed-Abrar/publication/277598468_Network_and_communication_Privacy_Digi_cash/links/556e5fc008aeab777226a488/Network-and-communication-Privacy-Digi-cash.pdf (archived version available via: https://archive.ph/IfZLj)

ALBERT, Miriam. The Howey Test Turns 64: Are Courts Grading This Test on a Curve: Are Courts Grading This Test on a Curve. 2 Wm. & Mary Bus L. Rev. 1 (2011) [online]. [cit. 2022-06-12]. Available at: https://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=1184&=&context=faculty_scholarship&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Den%2526as_sdt%253D0%25252C5%2526q%253Dhowey%252Btest%252Bprongs%2526btnG%253D#search=%22howey%20test%20prongs%22 (Archived version available via: https://archive.ph/Oj4KQ

ALBERT, Miriam. The Howey Test Turns 64: Are Courts Grading This Test on a Curve: Are Courts Grading This Test on a Curve. 2 Wm. & Mary Bus L. Rev. 1 (2011) [online]. [cit. 2022-06-12]. Available at: https://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=1184&=&context=faculty_scholarship&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Den%2526as_sdt%253D0%25252C5%2526q%253Dhowey%252Btest%252Bprongs%2526btnG%253D#search=%22howey%20test%20prongs%22 (Archived version available via: https://archive.ph/Oj4KQ

Allison Caffarone & Meg Holzer, "*Ev'ry American Experiment Sets A Precedent": Why One Florida State Court's Bitcoin Opinion Is Everyone's Business,* 16 J. Intl. Bus. & L. 6, 9 (2016) Available at: https://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=2124&context=faculty_scholarship (Archived version available via: https://archive.ph/2Ew5c)

AMMOUS, Saifedean. Can cryptocurrencies fulfil the functions of money? [online]. In: Working Paper no. 92. Columbia University: Center on Capitalism and Society, 2016, 2016, s. 1-31 [cit. 2022-03-22]. Available at: https://capitalism.columbia.edu/files/ccs/workingpage/2017/ammous_cryptocurrencies_and_the_functions_of_money.pdf (archived version available via: https://archive.ph/wp2vT)

ARNER, Douglas, Raphael AUER a Jon FROST. BIS Working Papers No 905: Stablecoins: risks, potential and regulation [online]. 2020, page 7, 1-31 [cit. 2021-11-21]. Available at: https://www.bis.org/publ/work905.pdf (Archived version available via: https://archive.ph/GQMqB)

BAINS, Parma. Blockchain Consensus Mechanism: A primer for Supervisors [online]. International Monetary Fund, 2022, (Note 2022/003), 1-26 [cit. 2022-04-20]. Available at: https://www.elibrary.imf.org/downloadpdf/journals/063/2022/003/063.2022.issue-003-en.xml (Archived version available via: https://archive.ph/OKy0E)

BANK OF INTERNATIONAL SETTLEMENTS. Central bank digital currencies: foundational principles and core features [online]. 2020, 1-21 [cit. 2022-06-14]. Available at: https://www.bis.org/publ/othp33.pdf (Archived version available via: https://archive.ph/Ztscf)

BAUR, Dirk, KiHoon HONG a Adrian LEE. Bitcoin: Medium of exchange or speculative assets? Journal of International Financial Markets, Institutions and Money [online]. May, 2018, 54, 177-189 [cit. 2022-03-25]. Available at: https://www.sciencedirect.com/science/article/pii/S1042443117300720?ref=cra_js_challenge&fr=rjs doi: https://doi.org/10.1016/j.intfin.2017.12.004, (archived version available via: https://archive.ph/0rk3E)

BELLAVITIS, Cristiano, Christian FISCH a Johan WIKLUND. A Comprehensive Review of the Global Development of Initial Coin Offerings (ICOs) and Their Regulation. Journal of Business Venturing Insights [online]. 2020 [cit. 2022-06-11]. Available at https://www.researchgate.net/profile/Christian-Fisch/publication/346413693_A_Comprehensive_Review_of_the_Global_Development_of_Initial_Coin_Offerings_ICOs_and_Their_Regulation/links/5fc0b33c92851c933f65077e/A-Comprehensive-Review-of-the-Global-Development-of-Initial-Coin-Offerings-ICOs-and-Their-Regulation.pdf (Archived version available via: https://archive.ph/z0JCu)

BESHIRI, Arbër S. a Arsim SUSURI. Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. Journal of Computer and Communications [online]. Scientific Research Publishing, 07(03) [cit. 2022-05-22]. Available at: https://www.scirp.org/html/4-1730998_91242.htm (archived version available via: https://archive.ph/oifvg)

BIS Annual Economic Report 2018: V. Cryptocurrencies: looking beyond the hype. 2018. 91-114 [cit. 2021-12-19] Available at: https://www.bis.org/publ/arpdf/ar2018e5.pdf (archived version available via: https://archive.ph/LdFXi)

BJERG, Ole. How is Bitcoin Money. Theory, Culture & Society. Copenhagen Business School: Sage, 2016, 33(1), 53-72. DOI: 10.1177/0263276415619015, Available at: https://d1wqtxts1xzle7.cloudfront.net/52627298/Theory_Culture_Society-2015-Bjerg-with-cover-page-v2.pdf?Expires=1648047733&Signature=BbLNI~gZ15z1FUzSDXcv3QqM8P7VRccd-NnPoB-21TGLo1~QmmTS9U6kkRqdhIPEKax2GFMCqBXNCHRTGDh3plBfQ0vWKRJznSt0c05u~pscZnpsUHOdsTALR-9d8m9kSpLihSZu6IMt0UPCJHgB4XrfsGJC4iQY-oF1ASAPJrg0-erqSN4Gi27VLvRHx-90ZFcJTGSIwipwQb8GSUF84jFA4UqPoWBqgwsj1IB0tmBKdS9orin5xsLbblKFENL~YTr4AnN~1ijlaBqM2q-bGcz5klaj-I3KSl1yh0LKcU7huUCdwje6iXxXbiuEP7miPKUp8KoZ~Zf6N5NLpLKaww__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (archived version available via: https://archive.ph/DAMZn)

BLACK, Adam. Hashcash - A Denial of Service Counter-Measure [online]. September 2002, 1-10 [cit. 2022-04-11]. Available at: https://www.researchgate.net/publication/2482110_Hashcash_-_A_Denial_of_Service_Counter-Measure (Archived version available via: https://archive.ph/h09S9)

BODZIONY, Norbert, Paweł JEMIOŁO, Krzysztof KLUZA a Marek OGIELA. Blockchain-Based Address Alias System. Journal of Theoretical and Applied Electronic Commerce Research [online]. 2021, (16), 1280-1296, at 1283 [cit. 2022-04-19]. Available at: https://www.mdpi.com/0718-1876/16/5/72/htm (Archived version available via: https://archive.ph/ 5r1on)

BROWNING, Steve. Cryptocurrencies: Bitcoin and other exchange tokens. Briefing Paper [online]. United Kingdom, 2020(8780) [cit. 2022-06-07]. Available at: https://researchbriefings.files.parliament.uk/documents/CBP-8780/CBP-8780.pdf (Archived version available via: https://archive.ph/alioe)

BUELL, Samuel. WHAT IS SECURITIES FRAUD? Duke Law Journal [online]. 2011, 512 - 581 [cit. 2018-12-20]. Available at: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1518&context=dlj

BULLMANN, Dirk, Jonas KLEMM a Andrea PINNA. Occasional Paper Series: In search for stability in crypto-assets: are stablecoins the solution? [online]. August 2019, 1-53 [cit. 2021-11-21]. ISSN 1725-6534. Available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf (Archived version available via: https://archive.ph/Q3XSt)

BURDETTH, Kenneth, Alberto TREJOS a Randall WRIGHT. [online]. January 22, 2000, 117-142 [cit. 2022-03-25]. Available at: https://reader.elsevier.com/reader/sd/pii/S0022053100927315?token=9BCC20937B3F6F8728630527175144BC7D491EA93AEA67F71BD89CA5500BFA3F69BD4E8463D50F1B864066A35D2DC12E&originRegion=eu-west-1&originCreation=20220325134415 (Archived version available via: https://archive.ph/X9hsU)

BUTLER, Simon. Criminal use of cryptocurrencies – a great new threat or is cash still king?. Information Security Group [online]. 2019, 1-23, p.7 [cit. 2022-06-07]. Available at: https://pure.royalholloway.ac.uk/portal/files/42792707/Accepted_Manuscript.pdf (Archived version available via: https://archive.ph/B8b0N)

CAMPBELL-VERDUYN, Malcolm. Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change [online]. Springer, 69(1), 1-30 [cit. 2022-06-02]. Available at:

https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance (Archived version unavailable)
Carmine DiPiero, *Deciphering Cryptocurrency: Shining A Light on the Deep Dark Web*, 2017 U. Ill. L. Rev. 1267, 1273 (2017)

CHAUM, David. Blind Signatures for Untraceable Payments [online]. Santa Barbara, CA, 1983 [cit. 2022-01-02]. Available at: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF. University of California. (Archived version available via: https://archive.ph/QPK9u)

CHENG, Hsing Kenneth, Daning HU a J. Leon ZHAO. The landscape of Blockchain research: impacts and opportunities. Information Systems and e-business Management [online]. 2021, 749-755 [cit. 2022-05-09]. Available at: https://link.springer.com/article/10.1007/s10257-021-00544-1 (Archived version available at: https://archive.ph/Qfd3W)

CHERTOFF, Michael. A public policy perspective of the Dark Web. Journal of Cyber Policy [online]. 2017, 2(1) [cit. 2022-05-22]. Available at: https://www.tandfonline.com/doi/pdf/10.1080/23738871.2017.1298643?needAccess=true& (Archived version available via: https://archive.ph/5qj3X)

CHOHAN, Usman. The Double Spending Problem and Cryptocurrencies. Discussion Paper Series: Notes on the 21st Century [online]. Critical Blockchain Research Initiative, 2017, 6th January, 2021, 1-10 [cit. 2022-03-12]. Available at: https://deliverypdf.ssrn.com/delivery.php?ID=107064121121024002092084007007102002098014089077064041076068086098122007091113120094058057003006039016043112010113119092097096106078031069085002081098107071122124113073040045013124085090098076004023107068089103106094022006021096116030101103098116111074&EXT=pdf&INDEX=TRUE (archived version available via: https://archive.ph/QkmxM)

CHRISTIN, Nicolas. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace [online]. November 30, 2012 [cit. 2022-05-24]. Available at: https://arxiv.org/pdf/1207.7139.pdf (Archived version available via: https://archive.ph/uuAJM)
CipherTrace, *Cryptocurrency Anti-Money Laundering Report (*2018), 2, https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf (last visited Jun 5, 2019) (Archived version available via: https://archive.ph/JSCSI)

COSS. Coss: Crypto-one-stop-solution made easy [online]. 2017, 1-50 [cit. 2022-06-18]. Available at: https://cryptorating.eu/whitepapers/COSS/coss-whitepaper-v3.pdf (Archived version available via: https://archive.ph/6S78y)

Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 Ind. L.J. 441, 446 (2014) Available at: https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj (Archived version available via: https://archive.ph/ShrUs)
December 2018 - Exchange Volume Report. Blockchain transparency [online]. 2018 [cit. 2018-12-18]. Available at: https://www.blockchaintransparency.org (data also available via: https://blogs.airdropalert.com/best-airdrops-newsletter-week-15/)

DEMIRÜÇ-KUNT, Asli, Leora KLAPPER, Dorothe SINGER a Jake HESS. The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution [online]. 2018 [cit. 2022-05-10]. ISSN 978-1-4648-1268-2. Available at: https://globalfindex.worldbank.org/sites/globalfindex/files/chapters/2017%20Findex%20full%20report_chapter2.pdf (Archived version available via: https://archive.ph/K2Mw7)

DEPARTMENT OF THE TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK. Guidance FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies [online].

March 13, 2013, 1 Cited at Nov 5, 2018). Available at: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

DILHARA, Shashie. A Review on Application of Hash Functions and Digital signatures in the Blockchain Industry. Department of Network & Security [online]. Sri Lanka: NSBM Green University, September 2021, 1-5 p., at 2 [cit. 2022-04-18]. Available at: https://www.researchgate.net/publication/354700341_A_Review_on_Application_of_Hash_Functions_and_Digital_signatures_in_the_Blockchain_Industry/link/61489c713c6cb310697fbd67/download (Archived version available via: https://archive.ph/f847M)

DOGUET, Joshua. The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System. Louisiana Law Review [online]. Luisiana, USA: LSU Law Digital Commons, 2013, 73(4), 1120-1153 [cit. 2022-03-22]. Available at: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=6425&context=lalrev (archived version available via: https://archive.ph/Qsksl)

DOUCEUR, John R. The Sybil Attack. In: DRUSCHEL, Peter, Frans KAASHOEK and Anthony ROWSTRON. Peer-to-Peer Systems. Cambridge, MA, USA, March, 2002. pp. 251-261 Available also at: https://link.springer.com/content/pdf/10.1007/3-540-45748-8.pdf (Archived version available via: https://archive.ph/xUeFe)

DROZD, Oleksii, Yaroslav LAZUR and Ruslan SERBIN. THEORETICAL AND LEGAL PERSPECTIVE ON CERTAIN TYPES OF LEGAL LIABILITY IN CRYPTOCURRENCY RELATIONS. Baltic Journal of Economic Studies [online]. 2017, 3(5), 221-227 [cit. 2022-03-22]. Available at: http://www.baltijapublishing.lv/index.php/issue/article/view/289/pdf (archived version available via: https://archive.ph/7g4C2)

Duncan E. Alford, *Anti-Money Laundering Regulations: A Burden on Financial Institutions*, 19 N.C. J. Intl. L. & Com. Reg. 437, 439 (1994) Available at: https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1535&context=ncilj (Archived version available via: https://archive.ph/rEZqB)

DUPONT, Quinn. Experiments in Algorithmic Governance: A history and ethnography of "The DAO," a failed Decentralized Autonomous Organization. (ed. Malcolm Campbell-Verduyn) Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance (forthcoming). [online]. 1-18 [cit. 2022-06-11]. Available at: https://moodle.epfl.ch/pluginfile.php/2861870/mod_resource/content/1/DUPONT-2017-Preprint-Algorithmic-Governance.pdf (Archived version available via: https://archive.ph/ohUOQ)

Dwork C., Naor M. (1993) Pricing via Processing or Combatting Junk Mail. In: Brickell E.F. (eds) Advances in Cryptology — CRYPTO' 92. CRYPTO 1992. Lecture Notes in Computer Science, vol 740. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48071-4_10 available at: https://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf (archived version available via: https://archive.fo/kkvkb)

EFANOV, Dmitry a Pavel ROSCHIN1. The All-Pervasiveness of the Blockchain Technology. 8th Annual International Conference on Biologically Inspired Cognitive Architecture, BICA [online]. 2018, 2018(123), 116-121 [cit. 2022-05-08]. Available at: https://reader.elsevier.com/reader/sd/pii/S1877050918300206?token=67C1D0ED992D918DEFCD6A4610C20160D3BE62479397C5805FDDBF51AC775EC013E60A1FAA63B4F9B6B40C77162C38D2&originRegion=eu-west-1&originCreation=20220508202227 (Archived version available at: https://archive.ph/PTE86)

EMERY, Jules a Matthieu LATAPY. Full Bitcoin Blockchain Data Made Easy. 2021 IEEE/ACM International Conference on Advances in Social Network Analysis and Mining (ASONAM 2021) [online]. Netherlands, 2021, 1-16 [cit. 2022-04-19]. Available at: https://hal.archives-ouvertes.fr/hal-03443053/document (Archived version available via: https://archive.ph/P5KUW)

EUROPEAN CENTRAL BANK. Virtual Currency Schemes [online]. October 2012. EU, 2012 [cit. 2022-03-21]. ISBN 978-92-899-0862-7. Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (archived version available via: https://archive.ph/jYQ4f)

EUROPOL. Cryptocurrencies: Tracing the Evolution of Criminal Finances [online]. Luxembourg: Publications Office of the European Union, 2021, 1-20 [cit. 2022-05-30]. ISSN ISBN 978-92-95220-37-9. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf (Archived version available at: https://archive.ph/s8vgT)

FANUSIE, Yaya a Tom ROBINSON. Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services [online]. 2018, s. 1-16 [cit. 2022-03-22]. Available at: https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf (archived version available via: https://archive.ph/rfvPg)

FATF. Virtual Currencies Key Definitions and Potential AML/CFT Risks. FATF REPORT [online]. june 2014 [cit. 2022-06-07]. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Archived version available via: https://archive.ph/ad7Lj)

FEYEN, Erik, Yusaku KAWASHIMA a Raunak MITTAL. Crypto-Assets Activity around the World: Evolution and Macro-Financial Drivers. Policy Research Working Paper: Finance, Competitiveness and Innovation Global Practice & Information and Technology Solution Vice Presidency [online]. 2022, (9962) [cit. 2022-05-08]. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/37115/Crypto-Assets-Activity-around-the-World-Evolution-and-Macro-Financial-Drivers.pdf?sequence=1 (Archived version available via: https://archive.ph/1Xj13)

Financial Action Task Force, *Virtual Currencies Key Definitions and Potential AML/ CFT Risks* (June 27, 2015), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Archived version available via: https://archive.ph/ad7Lj)

Financial Stability Board: Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document [online]. April 14, 2020, page 1, 1-62 [cit. 2021-11-21]. Available at: https://www.fsb.org/wp-content/uploads/P140420-1.pdf (Archived version available via: https://archive.ph/A138l)

FINKLEA, Kristin. Dark Web. Congressional Research Services informing the legislative debate since 1914 [online]. March 10, 2017, 1-16 [cit. 2022-05-22]. Available at: https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf (Archived version unavailable)

FRIIS BO, Jens. Digicash implementation [online]. University of Aarhus, 1-21 [cit. 2022-01-02]. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.197.7531&rep=rep1&type=pdf (archived version available via: https://archive.ph/2cHeg)

Genci Bilali, *Know Your Customer-or Not*, 43 U. Toledo L. Rev. 319 (2012) Available at: https://heinonline.org/HOL/Page?handle=hein.journals/utol43&div=15&g_sent=1&casa_token=&collection=journals (Archived version available via: https://archive.ph/VOSlq)

GLASER, Florian, Kai ZIMMERMANN, Martin HAFERKORN, Moritz Christian WEBER a Michael SIERING. BITCOIN - ASSET OR CURRENCY? REVEALING USERS' HIDDEN INTENTIONS. Twenty Second European Conference on Information Systems [online]. Tel Aviv, 2014(1), 1-14 [cit. 2022-03-25]. Available at: https://deliverypdf.ssrn.com/delivery.php?ID=659113087090031100005100106064073095007085007037003090100005002104097066091124070102026056048010010036110094097024089084113002104006091005020071011089029112066078004004007050007012107029066112103028115002088072021012070127009103007118080019082002026081&EXT=pdf&INDEX=TRUE (Archived version available at: https://archive.ph/yI0qW)

GRAF VON LUCKNER, Clemens, Carmen M. REINHART a Kenneth S. ROGOFF. DECRYPTING NEW AGE INTERNATIONAL CAPITAL FLOWS. NBER WORKING PAPER SERIES [online]. 1-54 [cit. 2022-05-08]. Available at: https://www.nber.org/system/files/working_papers/w29337/w29337.pdf (Archived version available via: https://archive.ph/a9got)

GRAYDON, Matthew a Lisa PARKS. 'Connecting the unconnected': a critical assessment of US satellite Internet services. Media, Culture & Society [online]. SAGE, 2019, 1-17 [cit. 2022-05-29]. [online]. Available at: shorturl.at/fgmFJ [cit. 2022-05-29].

GROENEWEG, Nikolaj. Evaluating Cryptocurrency Exchanges in the Absence of Governmental Frameworks: - A multiple criteria scoring model - [online]. Switzerland, 1-28 [cit. 2022-05-10]. Available at: https://deliverypdf.ssrn.com/delivery.php?ID=739098086122105021068114015106124011123049028029039027085068064111098103126097115094055034030123018059015112077097064110093120038013054059039029117103065082004122092022035014117081026107102025012094025085103110077125121083029121030122015108095005022085&EXT=pdf&INDEX=TRUE (Archived version available via: https://archive.ph/fTvdp)

HAMDY, Abdulrahman. Explaining the Bitcoin Block Reward. Argoblockchain.com [online]. 2022 [cit. 2022-04-20]. Available at: https://argoblockchain.com/articles/explaining-the-bitcoin-block-reward (Archived version available via: https://archive.ph/iiZML)

HAUBEN, Michael. History of ARPANET: Behind the Net - The untold history of the ARPANET [online]. 1-20 [cit. 2022-06-08]. Available at: https://www.jbcoco.com/Arpa-Arpanet-Internet.pdf (Archived version available via: https://archive.ph/mEotQ)

HENRIQUES, Michelle a Nagaraj VERNEKAR. Using symmetric and asymmetric cryptography to secure communication between devices in IoT. 2017 International Conference on IoT and Application (ICIOT) [online]. 19 October 2017n. l., 1-4 [cit. 2022-04-19]. Available at: https://ieeexplore.ieee.org/abstract/document/8073643 (archived version available via: https://archive.ph/574QF

HOUBEN, Robby a Alexander SNYERS. Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion [online]. European Parliament, 2018, 1-100 [cit. 2021-12-19]. ISBN 978-92-846-3200-8. Available at: https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (archived version available via: https://archive.fo/u1cEi)

INTERNAL REVENUE SERVICE. Notice 2014-21 [online]. 1-6 (Cited at Nov 1, 2018). Available at: https://www.irs.gov/pub/irs-drop/n-14-21.pdf (Archived version available via: https://archive.ph/xy1jc)
IRS. Investment Income and Expenses [online]. 2021, 1-77 p. 56 [cit. 2022-06-22]. Available at: https://www.irs.gov/pub/irs-pdf/p550.pdf (Archived version available via: https://archive.ph/yz06c)

JAKOBSSON, Markus a Ari JUELS. PROOFS OF WORK AND BREAD PUDDING PROTOCOLS (EXTENDED ABSTRACT). Secure Information Networks [online]. Springer Science+Business Media Dordrecht, 1999, 258-272 [cit. 2022-04-05]. Available at: https://link.springer.com/content/pdf/10.1007/978-0-387-35568-9_18.pdf (Archived version available via: https://archive.ph/YLvkx)

JIRWAN, Nitin, Ajay SINGH a Sandip VIJAY. Review and Analysis of Cryptography Techniques. International Journal of Scientific & Engineering Research [online]. 2013, 4(3), 1-6 [cit. 2022-04-19]. Available at: https://d1wqtxts1xzle7.cloudfront.net/44421110/Review_and_Analysis_of_Cryptography_Tech20160404-17928-1wutbod-with-cover-page-v2.pdf?Expires=1650387017&Signature=fl7AWaGnt00tsn-Bq-s-aGffQCY~66q1lOCUbLwi7diksMmgrV3tXAvimZvKNqMsAVSd0uSOx5NcFeKxubZoIiE4w1iTQ2YQfwUJzASPxYLMWLn2chfV-em-GT9hBvgEyJxSgBeFj6v7hbfmk-7IScbq1ZBUFuQGTe1dtcOVxSQLd9GkPKdgEO8keKYYkFja~nGdeELNbd00MAavjJvH~fH9Y7ifOCjBnuQIORe5o86bVIH38SxECN1p0jnSEIdPR-ylW6k5eMq9cln84uJM9vrxeAFUdahIvAg7fmvlcmP-zs08R8G-

iZD3tpjbs8fe6aYSUAYpDIqUluEI7TBN7A__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (Archived version available via: https://archive.ph/wip/2WySo)

KAPLANOV, Nikolei. Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation. Loyola Consumer Law Review [online]. USA: LAW eCommons, 2012, 2013, 25(1), 111-174 [cit. 2022-03-22]. Available at: https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1920&context=lclr (archived version available via: https://archive.ph/Qsksl)

Kerem Kaskaloglu, *Near Zero Bitcoin Transaction Fees Cannot Last Forever*, INT'L CONF. ON DIGITAL SECURITY & FORENSICS 91, 91-93 (June 2014) Available at: https://www.researchgate.net/profile/Natalie-Walker-15/publication/263617788_Proceedings_of_the_International_Conference_on_Digital_Security_and_Forensics_DigitalSec2014/links/0f31753b5cd085c06a000000/Proceedings-of-the-International-Conference-on-Digital-Security-and-Forensics-DigitalSec2014.pdf#page=93 (Archived version available at: https://archive.ph/oTgo4)

KERMITSIS, Emmanouil, Demitrios KAVALLIEROS, Demitrios MYTTAS, Euthimios LISSARIS a Gerogios GIATAGANAS. Dark Web Markets. AKHGAR, Babak, Marco GERCKE, Stefanos VROCHIDIS a Helen GIBSON. Dark Web Investigation [online]. 85 - 118 [cit. 2022-06-08]. ISBN 978-3-030-55343-2. Available at: https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Tor/Dark%20Web%20Investigation.pdf#page=99 (Archived version available via: https://archive.ph/DgXtM)

KETHINENI, Sesha, Cassandra DODGE a Ying CAO. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. American Journal of Criminal Justice [online]. Texas USA, May 2017, May 2017, 43(2) [cit. 2022-06-02]. Available at: https://www.researchgate.net/profile/Ying-Cao-25/publication/316655308_Use_of_Bitcoin_in_Darknet_Markets_Examining_Facilitative_Factors_on_Bitcoin-Related_Crimes/links/5c4503ec299bf12be3d79300/Use-of-Bitcoin-in-Darknet-Markets-Examining-Facilitative-Factors-on-Bitcoin-Related-Crimes.pdf (Archived version available via: https://archive.ph/iliFo)

Kevin Scura, *Money Laundering*, 50 Am. Crim. L. Rev. 1271, 1271 (2013)

KIFFER, Lucianna, Dave LEVIN a Alan MISLOVE. Stick a fork in it: Analyzing the Ethereum network partition. HotNets-XVI: Proceedings of the 16th ACM Workshop on Hot Topics in Networks [online]. 2017, 94-100 [cit. 2022-06-07]. Available at: https://dl.acm.org/doi/pdf/10.1145/3152434.3152449 (Archived version available via: https://archive.ph/wip/UFhmN)

KIM, Suah, Beomjoong KIM a Hyoung KIM. Intrusion Detection and Mitigation System Using Blockchain Analysis for Bitcoin Exchange [online]. Singapore: Association for Computing Machinery, October 29–31, 2018, 1-5 [cit. 2022-04-14]. Available at: https://www.researchgate.net/profile/Suah-Kim-3/publication/330205979_Intrusion_Detection_and_Mitigation_System_Using_Blockchain_Analysis_for_Bitcoin_Exchange/links/5e686005299bf1744f72cd20/Intrusion-Detection-and-Mitigation-System-Using-Blockchain-Analysis-for-Bitcoin-Exchange.pdf (Archived version available via: https://archive.ph/Yxir1)

KING, Sunny a Scott NADAL. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake [online]. 2012 [cit. 2022-04-20]. Available at: https://whitepaper.io/document/139/peercoin-whitepaper (Archived version available via: https://archive.ph/l2Mvp)

KLUCHENEK, Matthew. BITCOIN AND VIRTUAL CURRENCIES: WELCOME TO YOUR REGULATOR. Harvard Business Law Review Online [online]. 2016(7) [cit. 2022-06-13]. Available at: https://www.hblr.org/wp-content/uploads/sites/18/2016/12/M.-Kluchenek_Bitcoin-and-Virtual-Currency-Regulation-1.pdf

KOHAJDA, Michael - MORAVEC, Jiří. Contemporary Development of Criminal Activity in Cryptocurrency Environment. *Daně a finance*. 2019, **27** (1-2), 55-60. ISSN 1801-6006.

KOHAJDA, Michael - MORAVEC, Jiří. Elemental Analysis of the U.S. Regulation of Cryptocurrencies. Daně a finance. 2018, 26 (4), 23-28. ISSN 1801-6006.

KOHAJDA, Michael - MORAVEC, Jiří. The Illicit Use of Bitcoin. *Daně a finance*. 2020, **28** (1-4), 43-50. ISSN 1801-6006.

LICHTFOUS, Marco, Vivek YADAV a Valentina FRATINO. Can blockchain accelerate financial inclusion globally? Inside Magazine [online]. 19(02) [cit. 2022-05-29]. Available at: https://theblockchaintest.com/uploads/resources/Deloitte%20-%20Can%20Blockchain%20Accelerate%20financial%20inclusion%20globally%20-%202019.pdf (Archived version available via: https://archive.ph/4ZUWQ)

Liu ZIYAO, Luong NGUYEN CONG, Wang WENBO, Niyato DUSIT, Liang YING-CHANG a Kim DONG. A Survey on Applications of Game Theory in Blockchain [online]. IEEE, 15 March 2019 [cit. 2022-04-14]. Available at: https://arxiv.org/pdf/1902.10865.pdf (Archived version available via: https://archive.ph/xEBcr)

LIU, Hannah. Why do People Invest in Initial Coin Offerings (ICOs)?. Joseph Wharton Scholars [online]. 2019, (5) [cit. 2022-06-11]. Available at: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1073&context=joseph_wharton_scholars (Archived version available via: https://archive.ph/YEVXl)

LIU, Manlu, Kean WU a Jennifer JIE XU. How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain. CURRENT ISSUES IN AUDITING American Accounting Association [online]. 2019, 13,(2) [cit. 2022-04-18]. Available at: https://www.researchgate.net/profile/Kean-Wu/publication/335472340_How_Will_Blockchain_Technology_Impact_Auditing_and_Accounting_Permissionless_Vs_Permissioned_Blockchain/links/5e270a3e299bf15216707ef4/How-Will-Blockchain-Technology-Impact-Auditing-and-Accounting-Permissionless-Vs-Permissioned-Blockchain.pdf (Archived version available via: https://archive.ph/VpXpR)

M. Tran, L. Luu, M. Suk Kang, I. Bentov, and P. Saxena, "Obscuro: A Bitcoin Mixer using Trusted Execution Environments," in ACSAC '18 (Annual Computer Security Applications Conference), ser. ACSAC '18, vol. 18. New York, NY, USA: ACM, 2018, pp. 692–701. [Online]. Available at: https://dl.acm.org/citation.cfm?id=3274750{\%}0A (Archived version available via: https://archive.ph/a20Qg)

M.S. STEEL, Chad. Stolen Identity Valuation and Market Evolution on the Dark Web [online]. USA, 2019, 13(1) [cit. 2022-06-03]. Available at: https://www.cybercrimejournal.com/Steelvol13issue1IJCC2019.pdf (Archived version unavailable)

MA, Guangkai, Chunpeng GE a Lu ZHOU. Achieving reliable timestamp in the bitcoin platform. Special Issue on Security and Privacy in Machine Learning Assisted P2P Networks [online]. 13 May 2020, (13), 2251–2259 [cit. 2022-04-14]. Available at: https://link.springer.com/content/pdf/10.1007/s12083-020-00905-6.pdf (Archived version available via: https://archive.ph/XA0d0)

MACEY, Jonathan a Geoffrey MILLER. Origin of the Blue Sky Laws. Texas Law Review [online]. USA, 1991, 70(2) [cit. 2022-06-11]. Available at: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/884/Origin_of_the_Blue_Sky_Laws.pdf?sequence=2&isAllowed=y (Archived version available via: https://archive.ph/6CaPq)
MANSA, Julius. Consensus Mechanism (Cryptocurrency). Investopedia.com [online]. 2021 [cit. 2022-04-14]. Available at: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp (Archived version available via: https://archive.ph/6a8TR)

MARTIN, James. Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. Criminology & Criminal Justice [online]. Sage, 2014, 14(3), 351-367 [cit. 2022-05-24]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.838.8982&rep=rep1&type=pdf (Archived version not available)

MEIER, Julia a Benedikt SCHUPPLI. The DAO Hack and the Living Law of Blockchain. DAL MOLIN-KRÄNZLIN, Alexandra, Anne Mirjam SCHNEUWLY a Jasna STOJAVIC. Digitalisierung - Gesellschaft - Recht: Analysen und Perspektiven von

Assistierenden des Rechtswissenschaftlichen Instituts der Universität Zürich. s. 27-44. ISBN 978-3038910817. Chapter available at: https://www.researchgate.net/profile/Benedikt-Schuppli/publication/348419598_The_DAO_Hack_and_the_Living_Law_of_Blockchain/links/5ffe286f92851c13fe09c754/The-DAO-Hack-and-the-Living-Law-of-Blockchain.pdf (Archived version available via: https://archive.ph/mSFBI)

MORAVEC, Jiří - KOHAJDA, Michael. Legal Issues of Stablecoins. *Daně a finance*. 2021, **28** (1-4), 93-98. ISSN 1801-6006.

MORAVEC, Jiří. The Perfect Digital Money That Nobody Wants. Daně a finance. 2019, 27 (3-4), 30-35. ISSN 1801-6006.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. October 31, 2008, s. 1-9 [cit. 2022-03-29]. Available at: https://bitcoin.org/bitcoin.pdf (Archived version available via: https://archive.ph/b7ICx)

NOFER, Michael, Peter GOMBER, Oliver HINZ a Dirk SCHIERECK. Blockchain [online]. Springer Fachmedien Wiesbaden 2017, 2017, 20 March 2017, 183 - 187 [cit. 2022-04-14]. Available at: https://link.springer.com/content/pdf/10.1007/s12599-017-0467-3.pdf (Archived version available via: https://archive.ph/ZNJFD)

O'MAHONY, Donal a Hitesh TEWARI. Electronic Payment Systems. EDPACS the EDP audit, control and security newsletter [online]. January 1997, 1-36 [cit. 2022-03-30]. doi:DOI: 10.1201/1079/43233.25.11.19980501/30170.7 Available at: https://www.researchgate.net/profile/Hitesh-Tewari/publication/220693934_Electronic_Payment_Systems/links/56470d7508ae451880abcae8/Electronic-Payment-Systems.pdf (Archived version available via: https://archive.ph/NNVJj)

PARK, Sehyun, Seongwon IM, Youhwan SEOL a Jeongyeup PAEK. Nodes in the Bitcoin Network: Comparative Measurement Study and Survey [online]. 30 April 2019, 57009 - 57022 [cit. 2022-04-14]. ISSN 2169-3536. Available at: https://ieeexplore.ieee.org/abstract/document/8703385 (Archived version available via: https://archive.ph/DG8Bx)
Peter Reuter & Edwin M. Truman, Chasing dirty money: the fight against money laundering, 25 (Institute for International Economics) (2004), https://piie.com/publications/chapters_preview/381/3iie3705.pdf (Archived version available via: https://archive.ph/I5vx2)

PHELPS, Amy a Allan WATT. I shop online – recreationally! Internet anonymity and Silk Road enabling drug use in Australia. Digital Investigation [online]. December 2014, 11(04), 261-272 [cit. 2022-05-24]. Available at: https://www.sciencedirect.com/science/article/pii/S1742287614000930 (Archived version available via: https://archive.ph/2havz)

PRENEEL, Bart. CRYPTOGRAPHIC HASH FUNCTIONS. Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 161–171, 1993. [online]. 1-29 [cit. 2022-04-07]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.800.5133&rep=rep1&type=pdf (Archived version available at: https://archive.ph/V2Btv)

Q3 2018 Cryptocurrency Anti-Money Laundering Report [online]. 2018 [cit. 2022-06-17]. Available at: https://ciphertrace.com/q3-2018-cryptocurrency-anti-money-laundering-report/ (Archived version available via: https://archive.ph/Jhy4z)

RAHALKAR, Chaitanya a Anushka VIRGAONKAR. Summarizing and Analyzing the Privacy-Preserving Techniques in Bitcoin and other Cryptocurrencies [online]. 1-11 [cit. 2022-04-19]. Available at: https://arxiv.org/pdf/2109.07634.pdf (Archived version available via: https://archive.ph/rJAyJ)

REID, Fergal a Martin HARRIGAN. An Analysis of Anonymity in the Bitcoin System [online]. Clique Research Cluster, May 2012, 1-26 [cit. 2022-06-08]. Available at: https://arxiv.org/pdf/1107.4524.pdf?ref=https://githubhelp.com (archived version available via: https://archive.ph/oa4tb)

Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 Hastings Sci. & Tech. L.J. 159, 160 (2012) Available at: https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1063&context=hastings_science_technology_law_journal (Archived version available via: https://archive.ph/ZCb0g)

ROBLEH, Ali, John BARRDEAR, Roger CLEWS a James SOUTHGATE. Innovations in payment technologies and the emergence of digital currencies [online]. Bank of England Quarterly Bulletin 2014 Q3. 2014, 262-275 [cit. 2022-03-23]. Available at: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/innovations-in-payment-technologies-and-the-emergence-of-digital-currencies.pdf?la=en&hash=AB46869B3EF355A0486F7B0BAF086F2EEE31554D (archived version available via: https://archive.ph/lw1wj)

Sasha A. Klein, Andrew R. Comiter, *Bitcoin Are You Ready for This Change for A Dollar?*, 29 Prob. & Prop. 10 (March/April 2015) Available at: https://heinonline.org/HOL/Page?handle=hein.journals/probpro29&div=23&g_sent=1&casa_token=&collection=journals (Archived version available via: https://archive.ph/3Tynz)

SECURITIES AND EXCHANGE COMMISSION. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO [online]. 2017, July 25, 2017, 2017(Release No. 81207), 1 [cit. 2022-06-11]. Available at: https://www.sec.gov/litigation/investreport/34-81207.pdf (archived version available via: https://archive.ph/kv05f)

SMITH, Daniel. More Money, More Problems: The Bitcoin Virtual Currency and the Legal Problems that Face it. Journal of Law, Technology, & the Internet. Texas, USA, 2012, 3(2), 427-442. ISSN 1949-6451. Available also at: https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1035&=&context=jolti&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fq%253Dvirtual%252Bcurrency%252Bbitcoin%2526hl%253Den%2526as_sdt%253D0%25252C5%2526as_ylo%253D2008%2526as_yhi%253D2012#search=%22virtual%20currency%20bitcoin%22 (archived version available via: https://archive.ph/fwjJW)

SOBTI, Rajeev a G. GEETHA. Cryptographic Hash Functions: A Review. International Journal of Computer Science Issues [online]. March, 2012, 9(iss. 2) [cit. 2022-04-07]. ISSN 1694-0814. Available at: https://www.researchgate.net/profile/Geetha-Ganesan/publication/267422045_Cryptographic_Hash_Functions_A_Review/links/549cf6d10cf2b8037138c35c/Cryptographic-Hash-Functions-A-Review.pdf (Archiver version available via: https://archive.ph/EWzTw)

SRIMAN, B., GANESH, Kumar and SHAMILI, P. Advances in Intelligent Systems and Computing: Intelligent Computing and Applications Proceedings of ICICA 2019, in Blockchain Technology, Consensus Protocol Proof of Work and Proof of Stake [online]. Springer Nature Singapore Pte, 2021, 1-781, at 396 [cit. 2022-04-20]. ISBN: Available at: https://www.researchgate.net/profile/Saroj-Kumar-22/publication/345005910_Intelligent_Monitoring_of_Bearings_Using_Node_MCU_Module/links/6128 6be70360302a005f4941/Intelligent-Monitoring-of-Bearings-Using-Node-MCU-Module.pdf#page=395 (Archived version available via: https://archive.ph/CIlcR)

Stablecoins: an overview of the current state of stablecoins [online]. 2020, 1-31 [cit. 2021-11-21]. Available at: https://download.blockdata.tech/blockdata-stablecoin-report-blockchain-technology.pdf (Archived version available via: https://archive.ph/JePwl)

SWANSON, Tim. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems [online]. April 6, 2015, 1-66 [cit. 2022-04-14]. Available at:

https://allquantor.at/blockchainbib/pdf/swanson2015consensus.pdf (Archived version available via: https://archive.ph/rXdGG)
The Rise of Stablecoins: The Rise of Tether [online]. USA, 2020, s. 1-20, page 3, [cit. 2021-11-21]. Available at: https://f.hubspotusercontent00.net/hubfs/5264302/The%20Rise%20of%20Stablecoins.pdf (Archived version available via: https://archive.ph/O1Pfq)

U.S. Congress, Office of Technology Assessment, *Information Technologies for Control of Money Laundering*, 19 OTA-ITC-630 (Washington, DC: U.S. Government Printing Office, September 1995) Available at: https://www.princeton.edu/~ota/disk1/1995/9529/9529.PDF (Archived version available via: https://archive.ph/sjCXE)

VRIES, Alex. Bitcoin's Growing Energy Problem. Joule [online]. Elsevier, 2018, May 16, 801-809 [cit. 2022-04-20]. Available at : https://reader.elsevier.com/reader/sd/pii/S2542435118301776?token=5EF3950165D72642454B31509AAB1C623722D6D5D43DA64494C534E31A92DEFF030114FF34EAA018F8620DCFE2EDD95C&originRegion=eu-west-1&originCreation=20220420210056 (Archived version available via: https://archive.ph/1Hms6)

Wade V. Davies, *Bitcoin Criminals*, 53 Tenn. B.J. 24, 26 (July 2017) Available at: https://www.tba.org/index.cfm?pg=LawBlog&blAction=showEntry&blogEntry=28335 (Archived version available via: https://archive.ph/AfPca)

WANG, Maoning, Meijiao DUAN a Jianming ZHU. Research on the Security Criteria of Hash Functions in the Blockchain [online]. 2018 [cit. 2022-04-18]. ISBN 978-1-4503-5758-6/18/06. Available at: https://dl.acm.org/doi/epdf/10.1145/3205230.3205238 (Archived version available via: https://archive.ph/xaQV2)

WHITE, Lawrence. The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-Gold. Cato Journal [online]. Washington DC, USA, 2014, 2014(34), 281-301 [cit. 2021-12-21]. Available at: https://ciaotest.cc.columbia.edu/journals/cato/v34i2/f_0031473_25521.pdf (archived version available via: https://archive.fo/FWaBK)

WIJAYA, Dimaz, Joseph LIU, Ron STEINFELD a Dongxi LIU. Monero Ring Attack: Recreating Zero Mixin Transaction Effect [online]. Faculty of Information Technology, Monash University, 1-9 [cit. 2022-06-08]. Available at: https://eprint.iacr.org/2018/348.pdf (Archived version available via: https://archive.ph/BtqQt)

World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed- Ledger-Technology-and-Blockchain-Fintech-Notes.pdf (archived version available via: https://archive.fo/SyRup)

WU, Jiajing, Jieli LIU, Yijing ZHAO a Zibin ZHENG. Analysis of Cryptocurrency Transactions from a Network Perspective: An Overview. Journal of Network and Computer Applications [online]. Elsevier, 7 august 2021n. l., 1-24 p. at 4 [cit. 2022-04-18]. Available at: https://arxiv.org/pdf/2011.09318.pdf (Archived version available via: https://archive.ph/ZPtML)
XIA, Pengcheng. Characterizing Cryptocurrency Exchange Scams [online]. China, 2020, 1-15 [cit. 2022-05-10]. Available at: https://arxiv.org/pdf/2003.07314.pdf (Archived version available via: https://archive.ph/xdkJ8)

XU, Min, Xingtong CHEN a Gang KOU. A systematic review of blockchain. Financial Innovation [online]. 2019, 5(27) [cit. 2022-05-08]. Available at: https://jfin-swufe.springeropen.com/articles/10.1186/s40854-019-0147-z (Archived version available via: https://archive.ph/GmSHn)

Y. Xinyi, Z. Yi and Y. He. Technical Characteristics and Model of Blockchain 2018 10th International Conference on Communication Software and Networks (ICCSN), 2018, pp. 562-566, [cit. 2022-04-19]. Available at: https://ieeexplore.ieee.org/abstract/document/8488289 (Archived version available via: https://archive.ph/TS6jB)

YAGA, Dylan, Peter MELL, Nik ROBY a Karen SCARFONE. Blockchain Technology Overview. National Institute of Standards and Technology [online]. October 2018, 1-43, at 5, [cit. 2022-04-14]. Available at: doi:https://doi.org/10.6028/NIST.IR.8202 (Archived version available via: https://archive.ph/PbsmJ)

YANO, Mokoto, Chris DAI, Kenichi MASUDA a Yoshio KISHIMOTO, at all. Blockchain and Crypt Currency: Building a High Quality Marketplace for Crypt Data. Tokyo, Japan: Springer, 2020, 1-135. ISBN 978-981-15-3376-1. Also available at: https://library.oapen.org/bitstream/handle/20.500.12657/37713/2020_Book_BlockchainAndCryptCurrency.pdf?sequence=1#page=71 (archived version available via: https://archive.ph/3WkhM)

ZETZSCHE, Dirk, Douglas ARNER a Linus FÖHR. The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators. Law Working Paper Series Paper number 2017-011 [online]. 1-39 [cit. 2022-06-11]. Available at: https://www.researchgate.net/profile/Ross-Buckley/publication/321381542_The_ICO_Gold_Rush_It%27s_a_Scam_It%27s_a_Bubble_It%27s_a_Super_Challenge_for_Regulators/links/5bb6d1a6a6fdcc9552d3ddd0/The-ICO-Gold-Rush-Its-a-Scam-Its-a-Bubble-Its-a-Super-Challenge-for-Regulators.pdf (Archived version available via: https://archive.ph/DkJoo)

ZHU, Xingxiong. Research on blockchain consensus mechanism and implementation. IOP Conference Series: Materials Science and Engineering [online]. 2019, 1-6 [cit. 2022-04-20]. Available at: https://iopscience.iop.org/article/10.1088/1757-899X/569/4/042058/pdf (Archived version available via: https://archive.ph/vlMKd)

Internet resources

5 CHEAPEST Altcoins to Make You RICH (Under a Penny). Youtube.com [online]. 2021, 2021 [cit. 2022-03-23]. Available at: https://www.youtube.com/watch?v=12LB1SpQMMo (archived version available via: https://archive.ph/nbxHd)

Address - Bitcoin Wiki, https://en.bitcoin.it/wiki/Address (last visited Jun 6, 2019) (Archived version available via: https://archive.ph/WbtTP)

An Interview With A Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A) Forbes, https://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/#42e590c95732 (last visited Jun 4, 2019) (Archived version available via: https://archive.ph/B1Wh5)

ANDRUS MORTAZAVI, SOHALE. Cryptocurrency Is a Giant Ponzi Scheme. Jacobinmag.com [online]. [cit. 2022-05-30]. Available at: https://www.jacobinmag.com/2022/01/cryptocurrency-scam-blockchain-bitcoin-economy-decentralization (Archived version available via: https://archive.ph/5aYgz)

Asset Definition. Investopedia.com [online]. 2022 [cit. 2022-03-27]. Available at: https://www.investopedia.com/terms/a/asset.asp (Archived version available via: https://archive.ph/wjgpA)

BERWICK, Angus a Tom WILSON. How crypto giant Binance became a hub for hackers, fraudsters and drug traffickers. Reuters [online]. June 2022 [cit. 2022-06-18]. Available at: https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirtymoney/ (Archived version available via: https://archive.ph/NoqOS)

Binance Exchange: Overall Exchange volume [online]. [cit. 2022-06-18]. Available at: https://www.cryptocompare.com/exchanges/binance/overview (Archived version available via: https://archive.ph/9YCR0)

Bitcoin (BTC) price, charts, market cap, and other metrics CoinMarketCap, https://coinmarketcap.com/currencies/bitcoin/ (last visited Jun 5, 2019) (Archived version available via: https://archive.ph/bqQ2s)

Bitcoin Price Chart (BTC). Coingecko.com [online]. [cit. 2022-05-16]. Available at: https://www.coingecko.com/en/coins/bitcoin (Archived version available via: https://archive.ph/ZMzFY)

Bitcoin price. Coinbase.com [online]. [cit. 2022-06-10]. Available at: https://www.coinbase.com/price/bitcoin (Archived version available via: https://archive.ph/M49lV)
Bitcoin to USD Chart. Coinmarketcap.com [online]. [cit. 2022-05-08]. Available at: https://coinmarketcap.com/currencies/bitcoin/ (Archived version available via: https://archive.ph/tZKaI)

Blockchain and Cryptocurrency). Natlawreview.com [online]. [cit. 2022-06-18]. Available at: https://www.natlawreview.com/article/cracking-crypto-code-new-reporting-obligations-current-developments-world-blockchain (Archived version available via: https://archive.ph/Cx2wU)

BOOM VAN, Daniel. A Typo Sent $36 Million of Crypto Into the Ether. Cnet.com [online]. May 5, 2022 [cit. 2022-05-30]. Available at: https://www.cnet.com/personal-finance/crypto/a-typo-sent-36-million-of-crypto-into-the-ether/ (Archived version available via: https://archive.ph/Rxqf7)

Cambridge Dictionary: Meaning of cryptography in English in computing [online]. [cit. 2022-03-27]. Available at: https://dictionary.cambridge.org/dictionary/english/cryptography (Archived version available via: https://archive.ph pF4UM)

Cambridge Dictionary: Meaning of virtual in English [online]. [cit. 2022-03-27]. Available at: https://dictionary.cambridge.org/dictionary/english/virtual (Archived version available via: https://archive.ph/ZAtf3)

CBS, Interactive Inc. Inside the FBI takedown of the mastermind behind website offering drugs, guns and murders for hire. Cbsnews.com [online]. Nov. 10, 2022 [cit. 2022-05-22]. Available at: https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/ (archived version available via: https://archive.ph/WCMsR)

CFTC. CFTC Mission Statement [online]. [cit. 2022-05-22]. Available at: https://www.cftc.gov/About/MissionResponsibilities/index.htm (Archived version available via: https://archive.ph/fEr9g)

CHAUM, David. DigiCash. Chaum.com [online]. [cit. 2022-04-14]. Available at: https://www.chaum.com/ecash/ (archived version available via: https://archive.ph/iuZyq)

Coin Market Cap: Fei price today [online]. USA, 2021 [cit. 2021-11-21]. Available at: https://coinmarketcap.com/currencies/fei-usd/ (Archived version available via: https://archive.ph/w6URF0)

Coin Market Cap: Tether price today [online]. USA, 2021 [cit. 2021-11-21]. Available at: https://coinmarketcap.com/currencies/tether/ (Archived version available via: https://archive.ph/Br2fh)

COLDEWEY, Davin. How German and US authorities took down the owners of darknet drug emporium Wall Street Market [online]. 2019 [cit. 2022-06-08]. Available at: https://archive.ph/GJwgM.

Controlled supply Controlled supply - Bitcoin Wiki, https://en.bitcoin.it/wiki/Controlled_supply (last visited Jun 5, 2019) (Archived version available via: https://archive.ph/vfMiY)

CRAWLEY, Jamie. MicroStrategy Buys $191M Worth of Bitcoin [online]. 2022 [cit. 2022-05-29]. Available at: https://www.coindesk.com/business/2022/04/05/microstrategy-buys-1905m-worth-of-bitcoin/ (Archived version available via: https://archive.ph/A3uqU)

Crypto One Stop Solution. Coss.io [online]. 2021 [cit. 2022-05-08]. Available at: https://www.coss.io (Archived version available at: https://archive.ph/G5mYE)

Cryptocurrency prices, Charts and Market Capitalizations. Coinmarketcap.com [online]. March 21, 2022 [cit. 2022-03-21]. Available at: https://coinmarketcap.com (archived version available via: https://archive.ph/58VUG)

CRYSTALBLOCKCHAIN. Map of Security Breaches and Fraud Involving Crypto 2011-2021. Crystalblockchain.com [online]. [cit. 2022-06-11]. Available at: https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/ (Archived version available via: https://archive.ph/ESIlG)

D. Kaminsky. Black Ops of TCP/IP Presentation. Black Hat, Chaos Communication Camp, 2011. Available at: https://dankaminsky.com/2011/08/05/bo2k11/ (Archived version unavailable)

DigiByte Community Infopaper [online]. 2014, 1-17 [cit. 2022-05-08]. Available at: https://digibyte.org/docs/infopaper.pdf (Archived version available via: https://archive.ph/Cp0Rw)

Digicash to Test Live Internet Cash System with Mark Twain. American Banker [online]. USA, October 23, 1995 [cit. 2022-01-02]. Available at: https://www.americanbanker.com/news/digicash-to-test-live-internet-cash-system-with-mark-twain (archived version available via: https://archive.ph/FEv0v).

DILLET, Romain. Facebook scales back its crypto ambitions once again. TechCrunch.com [online]. [cit. 2021-11-21]. Available at: https://techcrunch.com/2021/10/19/facebook-scales-back-its-crypto-ambitions-once-again/ (Archived version available via: https://archive.ph/bhYux)
E-Gold [online]. [cit. 2022-03-29]. Available at: https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/Bitcoins/e-gold.html (Archived version available via: https://archive.ph/b8abu)

EBIEFUNG, Will. 2 Top Cryptocurrencies to Buy and Hold for Decades. The Motley Fool: Fool.com [online]. 2022 [cit. 2022-03-23]. Available at: https://www.fool.com/investing/2022/03/22/2-top-cryptocurrencies-to-buy-and-hold-for-decades/ (Archived version available via: https://archive.ph/99rPt)

FALKON, Samuel. The Story of the DAO — Its History and Consequences. Medium.com [online]. [cit. 2022-06-11]. Available at: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee (Archived version available via: https://archive.ph/YgyVQ)

Fei Protocol White Paper [online]. 2020, 1-18 [cit. 2021-11-21]. Available at: https://fei.money/static/media/whitepaper.7d5e2986.pdf (Archived version available via: https://archive.ph/AYPP5)

For more information please see: The Cryptocurrency for Payments: Based on Blockchain Technology [online]. [cit. 2022-05-08]. Available at: https://litecoin.org (Archived version available via: https://archive.ph/Jy7nw)

From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited Coin Desk, Available at: https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited (last visited Jun 3, 2019) (Archived version available via: https://archive.ph/mkxzp)

Gemini Exchange: Overall Exchange volume [online]. [cit. 2022-06-18]. Available at: https://www.cryptocompare.com/exchanges/gemini/overview (Archived version available via: https://archive.ph/16i7x)

Google.com [online]. [cit. 2022-03-23]. Available at: https://www.google.com/search?client=safari&rls=en&q=what+cryptocurrency+to+buy&ie=UTF-8&oe=UTF-8 (archived version available via: https://archive.ph/13lR5)

Google.com [online]. [cit. 2022-03-23]. Available at: https://www.google.com/search?client=safari&rls=en&q=which+cryptocurrency+is+best+for+transactions&ie=UTF-8&oe=UTF-8 (archived version available via: https://archive.ph/L9S1F)

Grow, B.; Cady J.; Rutledge, S.; and Polek, D. (2006) "Gold Rush." Business Week (8 January). Available at www.businessweek.com/stories/2006-01-08/gold-rush (archived version available via: https://archive.fo/Ffp3K#selection-3219.0-3219.461)

How I Would Invest $1,000 in Cryptocurrency in 2022? | CryptosRUs. Youtube.com [online]. 2022 [cit. 2022-03-23]. Available at: https://www.youtube.com/watch?v=hOxH-YL_exY (archived version available via: https://archive.ph/a6OqS).
https://twitter.com/bti___ (Archived version available via: https://archive.ph/u04MD)

HUGHE, Eric. Manifesto. Activism.net [online]. 9 March 1993n. l. [cit. 2022-03-30]. Available at: https://www.activism.net/cypherpunk/manifesto.html (Archived version available via: https://archive.ph/6of6P)

INSIDER INC. The growing list of applications and use cases of blockchain technology in business and life. Insider.com [online]. 2022 [cit. 2022-03-23]. Available at: https://www.businessinsider.com/blockchain-technology-applications-use-cases (archived version available via: https://archive.ph/E0o6k)

KHARIF, Olga. Bitcoin's Rally Masks Uncomfortable Fact: Almost Nobody Uses It [online]. [cit. 2022-05-29]. Available at: https://www.bloomberg.com/news/articles/2019-05-31/bitcoin-s-rally-masks-uncomfortable-fact-almost-nobody-uses-it?srnd=cryptocurrencies (Archived version available at: https://archive.ph/4CIiR)

KIM, Victoria. Dutch national pleads guilty to running online marketplace for drugs. Latimes.com [online]. September 3, 2014 [cit. 2022-06-08]. Available at: https://www.latimes.com/local/la-me-online-drug-marketplace-20140904-story.html (Archived version available via: https://archive.ph/PHWKF)

KOINLY. Top 7 No-KYC Exchanges [online]. Jan 2022 [cit. 2022-06-17]. Available at: https://koinly.io/blog/top-no-kyc-crypto-exchanges/

Kucoin Exchange: Overall Exchange volume [online]. [cit. 2022-06-18]. Available at: https://www.cryptocompare.com/exchanges/kucoin/overview (Archived version available via: https://archive.ph/ZpwXr)

Lexico - English Dictionary. Lexico.com [online]. [cit. 2022-03-27]. Available at: https://www.lexico.com/en/definition/virtual (Archived version available via: https://archive.ph/CR2Lz)

Lexico - English Dictionary. Lexico.com [online]. [cit. 2022-03-27]. Available at: https://www.lexico.com/en/definition/digital (Archived version available via: https://archive.ph/FYgky)

LIELACHER, Alex. How exchange listings affect cryptocurrency prices [online]. 2018 [cit. 2022-06-18]. Available at: https://bravenewcoin.com/insights/how-exchange-listings-affect-cryptocurrency-prices (Archived version available via: https://archive.ph/WTMnf)

MANATT, PHELPS a PHILLIPS. Crypto Reporting Rules in the Biden Infrastructure Deal [online]. 2022 [cit. 2022-06-18]. Available at: https://www.jdsupra.com/legalnews/crypto-reporting-rules-in-the-biden-1784927/

MONIACE, Paul R. La. Tesla still owns $2 billion in bitcoin, but crypto volatility has taken a toll [online]. [cit. 2022-05-29]. Available at: https://edition.cnn.com/2022/02/07/investing/tesla-bitcoin/index.htmlP (Archived version available via: https://archive.ph/TdWuG

NIMFUEHR, Marcel. The Amazing Story of Cryptocurrencies Before Bitcoin. Medium.com [online]. [cit. 2022-03-30]. Available at: https://medium.com/hackernoon/the-amazing-story-of-cryptocurrencies-before-bitcoin-fe1b0e55155b (Archived version available at: https://archive.ph/Uzmrb)

Online Etymology Dictionary: Digitalize. Etymonline.com [online]. [cit. 2022-03-27]. Available at: https://www.etymonline.com/word/digitalize#etymonline_v_53950 (Archived version available via: https://archive.ph/UZ2gx)

Other examples can find here: LUTKEVITCH, Ben. Timestamp. Techtarget.com [online]. 2021 [cit. 2022-04-11]. Available at: https://www.techtarget.com/whatis/definition/timestamp (archived version available via: https://archive.ph/bE66w)

Peníze a vzrušení ze hry. Mladé od kryptoměn neodrazují ani nekončící série krachů. Aktualne.cz [online]. [cit. 2022-05-22]. Available at: https://zpravy.aktualne.cz/finance/penize-hra-a-vzruseni-mlade-obchodniky-od-kryptomen-neodrazu/r~ce6a57c2d74b11eca873ac1f6b220ee8/?utm_source=www.seznam.cz&utm_medium=sekce-z-internetu (Archived version available via: https://archive.ph/foDbH)

PITTA, Julie. Requiem for a Bright Idea. Forbes.com [online]. Nov 1, 1999 [cit. 2022-01-02]. Available at: https://www.forbes.com/forbes/1999/1101/6411390a.html (archived version available via: https://archive.fo/FZD4Y)

Poloniex Exchange: Overall Exchange volume [online]. [cit. 2022-06-18]. Available at: https://www.cryptocompare.com/exchanges/poloniex/overview (Archived version available via: https://archive.ph/dq6rx)

PORNIN, Thomas. Is it safe to ignore the possibility of SHA collisions in practice?. Stackoverflow.com [online]. 2010 [cit. 2022-04-18]. Available at: https://stackoverflow.com/questions/4014090/is-it-safe-to-ignore-the-possibility-of-sha-collisions-in-practice (Archived version available via: https://archive.ph/6JH6i)

POWER, Mike. Online highs are old as the net: the first e-commerce was a drugs deal [online]. 2013 [cit. 2022-06-07]. Available at: https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal (Archived version available at: https://archive.ph/iToGH)

QURESHI, Haseeb. The Cypherpunks. Nakamoto.com [online]. Dec., 29, 2019 [cit. 2022-04-05]. Available at: https://nakamoto.com/the-cypherpunks/ (Archived version available via: https://archive.ph/Jr1dW)

RAMALHO, David a Nuno MATOS. What we do in the (digital) shadows: anti-money laundering regulation and a bitcoin-mixing criminal problem. ERA Forum [online]. Springer, 2021, 2021(22), 487-506 [cit. 2022-06-08]. Available at: https://link.springer.com/content/pdf/10.1007/s12027-021-00676-4.pdf (Archived version available via: https://archive.ph/dw3q0)

Statista.com [online]. 2022, February 8, 2022 [cit. 2022-03-21]. Available at: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/ (archived version available via: https://archive.ph/IkZGD)

SZABO, Nick. Bit Gold. Blogspot.com [online]. December 27, 2008 [cit. 2022-04-05]. Available at: https://unenumerated.blogspot.com/2005/12/bit-gold.html (Archived version available via: https://archive.ph/4RWXv)

SZABO, Nick. Secure Property Titles with Owner Authority. Nakamotoinstitute.com [online]. 1998 [cit. 2022-04-11]. Available at: https://nakamotoinstitute.org/secure-property-titles/ (Archived version available via: https://archive.ph/uTHzS)

SZABO, Nick. Trusted Third Parties Are Security Holes. Www.fon.hum.uva.nl [online]. 2001 [cit. 2022-04-07]. Available at: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/ttps.html (Archived version available via: https://archive.ph/YQpMa)

Tether.to: Assurance Opinion Confirms Tether's Reserves Fully Backed; Company Shares as Part of Ongoing Transparency Commitment [online]. USA, 2021 [cit. 2021-11-21]. Available at: https://tether.to/assurance-opinion-mar-21/ (Archived version available via: https://archive.ph/ZxJLE)

The cost to list tokens on cryptocurrency exchanges: Crypto exchanges are charging up to $1,000,000 for ICO to list tokens: It is a Pure Capitalism. Businessinsider.com [online]. 2018, March 12, 2018. cit. [2018-12-18] Available at: https://medium.com/@bitfinexed/wash-trading-bitcoin-how-bitfinex-benefits-from-fraudulent-trading-8bd66be73215 (Now also available here: https://uk.news.yahoo.com/crypto-exchanges-charging-1-million-064500807.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAA-KMd_Hc-jpFEus723Bt3Cjzf9ZDY-I-waoI9Cb5EDScy4rwzjcNUVCdTkznQarG-v5lJjR2PWxf1iw9r2Am9GWBsVUnm-8QeCzuS9BpajniZMFYHYh4ax_cKX2HtC3QR-bNPy6GR0jO0tFpvunqCDvtCkYV-BSfXOELpwSPTls) Archived version available via: https://archive.ph/yjswr)

The investors lost $ 40 billion. NEWBERY, Emma. Binance CEO Says LUNA Collapse Left Him 'Poor Again [online]. [cit. 2022-06-21]. Available at: https://www.fool.com/the-ascent/cryptocurrency/articles/binance-ceo-says-luna-collapse-left-him-poor-again/ (Archived version available via: https://archive.ph/16i7x)

The Role of the SEC [online]. [cit. 2022-05-22]. Available at: https://www.investor.gov/introduction-investing/investing-basics/role-sec (Archived version available via: https://archive.ph/2KP49)

TRETINA, Kat a John SCHMIDT. Top 10 Cryptocurrencies In March 2022. Forbes.com [online]. 2022, March, 2022 [cit. 2022-03-23]. Available at: https://www.forbes.com/advisor/investing/top-10-cryptocurrencies/ (Archived version available via: https://archive.ph/s6EQx).

U.S. Immigration and Customs Enforcement, Ross Ulbricht, aka Dread Pirate Roberts, sentenced to life in federal prison for creating, operating 'Silk Road' website. Ice.gov [online]. [cit. 2022-06-09]. Available at: https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating (Archived version available via: https://archive.ph/KV0Z7)

UNITED STATES OF AMERICA, COMMODITY FUTURES TRADING COMMISSION. ORDER INSTITUTING PROCEEDINGS PURSUANT TO SECTIONS 6(c) AND 6(d) OF THE COMMODITY EXCHANGE ACT, MAKING FINDINGS AND IMPOSING REMEDIAL SANCTIONS: In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, [online]. 2015, Sept 17, 2015, 2015(15-29), 2 [cit. 2018-11-21]. Available at: https://www.cftc.gov/sites/default/files/2018-06/enfsocietegeneralesaorder060418.pdf (Archived version available via: https://archive.ph/VbE1K)

United States Secret Service: In U.S. Secret Service-Led Investigation, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges. Secretservice.gov [online]. USA: U.S. Secret Service Media Relations, 2008 [cit. 2021-12-22]. Available at: https://www.secretservice.gov/press/releases/2008/07/us-secret-service-led-investigation-digital-currency-business-e-gold-pleads (archived version available via: https://archive.fo/Ga6pw)

Unknown. Wash Trading Bitcoin: How Bitfinex benefits from fraudulent trading [online]. 2018, October 21, 2017. Available at: https://medium.com/@bitfinexed/wash-trading-bitcoin-how-bitfinex-benefits-from-fraudulent-trading-8bd66be73215 [cit. 2018-12-18]

VACA, Inigo. While Bitcoin price starts 2022 with a slump, mining difficulty is on the rise. Cointelegraph.com [online]. [cit. 2022-05-29]. Available at: https://cointelegraph.com/news/while-bitcoin-price-starts-2022-with-a-slump-mining-difficulty-is-on-the-rise (Archived version available via: https://archive.ph/8Uit4)

WALKER, Jones. Cracking the Crypto Code: New Reporting Obligations (Current Developments in the World of Blockchain and Cryptocurrency). Natlawreview.com [online]. [cit. 2022-06-18]. Available at: https://www.natlawreview.com/article/cracking-crypto-code-new-reporting-obligations-current-developments-world-blockchain (Archived version available via: https://archive.ph/Cx2wU)

Wash Trading Bitcoin: How Bitfinex benefits from fraudulent trading Medium, https://medium.com/@bitfinexed/wash-trading-bitcoin-how-bitfinex-benefits-from-fraudulent-trading-8bd66be73215 (last visited Jun 4, 2019) (Archived version available via: https://archive.ph/Rj6kS)

Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails [online]. 2014 [cit. 2022-03-31]. Available at: https://www.gwern.net/docs/bitcoin/2008-nakamoto (Archived version available via: https://archive.ph/02G8p)

Weidai.com: B-money. Weidai.com [online]. [cit. 2022-03-30]. Available at: http://www.weidai.com/bmoney.txt (archived version available via: https://archive.ph/9YprR)

Weidai.com: Cyberpunks. Weidai.com [online]. [cit. 2022-03-30]. Available at: http://www.weidai.com (archived version available via: https://archive.ph/O0luA)

What is a Timestamp? Computerhope.com [online]. 2022 [cit. 2022-04-11]. Available at: https://www.computerhope.com/jargon/t/timestam.htm (archived version available via: https://archive.ph/K0S9z)

What was DigiCash? A super speedy walkthrough the grandfather of cryptocurrencies. Decrypt.com [online]. Feb 4, 2019 [cit. 2022-03-30]. Available at: https://decrypt.co/resources/digicash-what-is-cryptocurrency-explainer (Archived version available via: https://archive.ph/vC8gf)

Legislative:

Commodity Exchange Act of 1936

Commodity Futures Trading Act of 1974

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

Money Laundering Control Act of 1986

Regulation of the European Parliament and the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937

Securities Act of 1933

Securities Exchange Act of 1934

The 16th Amendment, March 15, 1913; Ratified Amendments, 1795-1992; General Records of the United States Government; Record Group 11; National Archives Available at: https://www.archives.gov/milestone-documents/16th-amendment (Archived version available via: https://archive.ph/rLmSj)

Case Law

Kish v. A.W. Chesterton Co., 930 So. 2d 704, 707 (Fla. 3d Dist. App. 2006)

Knauer v. United States, 328 U.S. 654, 657, 66 S.Ct. 1304, 90 L.Ed. 1500 (1946)

McMorrow v. Dime Sav. Bank of Williamsburgh, 852 N.Y.S.2d 345, 347 (N.Y. App. Div. 2d Dept. 2008)

Reddy v. CFTC, 191 F.3d 109 (2d Cir. 1999)

Reves v. Ernst & Young, 494 U.S. 56, 61 (1990) Available at: https://scholar.google.com/scholar_case?case=18068523124125938239&q=494+U.S.+56&hl=en&as_sdt=2006 (Archived version available via: https://archive.ph/Sdkq2)
SEC v. Edwards, 540 U.S. 389, 393 (2004)

SEC v. Sg Ltd., 265 F. 3d 42, 50 - Court of Appeals, 1st Circuit 2001 Available at: https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1335&=&context=umblr&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Den%2526as_sdt%253D0%25252C5%2526q%253Dhowey%252Btest%2526btnG%253D#search=%22howey%20test%22 (Archived version available via: https://archive.ph/8paNX)

SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946)

U.S. v. Ulbricht, 31 F. Supp. 3d 540, 546 – 547 (S.D.N.Y. 2014) Available at: https://casetext.com/case/united-states-v-ulbricht-11 (Archived version available via: https://archive.ph/MQIbV)

United Hous. Found., Inc. v. Forman, 421 U.S. 852 (1975) Available at: https://scholar.google.com/scholar_case?case=11168754825085710379&q=421+us+837+1975&hl=en&as_sdt=2006 (Archived version available via: https://archive.ph/uqc8n)

United States v. E-Gold, Ltd., 521 F.3d 411, 412 (D.C.Cir. 2008), available at: https://scholar.google.com/scholar_case?case=8874345388360794335&q=UNITED+STATES+of+America,+Appellee+v.+E-GOLD,+LTD.,+et+al.,+Appellants&hl=en&as_sdt=2006

United States v. Grainger, 701 F.2d 308, 311 (4th Cir. 1983), cert. denied, 461 U.S. 947 (1983).
US v. E-Gold, Ltd., 550 F. Supp. 2d 82 - Dist. Court, Dist. of Columbia 2008, available at: https://scholar.google.com/scholar_case?case=11718339043645598961&q=US+v+E+gold&hl=en&as_sdt=2006

Wilson v. Commodity Futures Trading Commn., 322 F.3d 555 (8th Cir. 2003) Available at: https://scholar.google.com/scholar_case?case=17618803477312186888&q=Wilson+v.+Commodity+Futures+Trading+Commn.,+322+F.3d+555+(8th+Cir.+2003)&hl=en&as_sdt=2006

Other sources

Explanatory memorandum of MiCA, available at: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF (Archived version available via: https://archive.ph/dxxME)

MORAVEC, Jiří. Bitcoin - Legal Aspects and Regulation. 2016. Master thesis. Charles University, Faculty of Law, Department of Financial Law and Financial Science. Thesis supervisor Kohajda, Michael. Available at: https://dspace.cuni.cz/bitstream/handle/20.500.11956/82909/DPTX_2015_2_11220_0_327151_0_177426.pdf?sequence=1&isAllowed=y (archived version available via: https://archive.ph/KSLok)

Senate Hearing 113-640 [online]. [cit. 2022-06-13]. Available at: https://www.govinfo.gov/content/pkg/CHRG-113shrg94366/html/CHRG-113shrg94366.htm (Archived version available via: https://archive.ph/jJ6O4)

CFTC. Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry [online]. 2014 [cit. 2022-06-13]. Available at: https://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6 (Archived version available via: https://archive.ph/wip/71IMK)

I AM HODLING. Bitcointalk.com [online]. [cit. 2022-03-23]. Available at: https://bitcointalk.org/index.php?topic=375643.0 (archived version available via: https://archive.ph/M3adv)

US DISTRICT COURT. United States District Court for the Central District of California September 2011 Grand Jury Indictment [online]. [cit. 2022-06-08]. Available at: https://www.wired.com/images_blogs/threatlevel/2012/04/WILLEMSIndictment-FILED.045.pdf

PAKKI, Jaswant. Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask). University Thesis - Arizona State University [online]. April 2020 [cit. 2022-06-08]. Available at: https://keep.lib.asu.edu/_flysystem/fedora/c7/224575/Pakki_asu_0010N_19863.pdf (Archived version available via: https://archive.ph/E9ImK)

Steven Mnuchin, Sec'y, U.S. Dep't of Treasury, Panel Discussion at the World Economic Forum: The Remaking of Global Finance (Jan. 25, 2018)

Financial Aspects of Global Payment Systems

Abstract

This dissertation summarizes findings on Digital Asset's development, which would fit under the era of Blockchain 1.0. We analyzed and synthetized available resources focusing on the following areas: (i) historic aspects of Digital Assets, (ii) technical solutions of Digital Assets, (iii) actual use of Digital Assets, (iv) abuse of Digital Assets, (v) Digital Assets' legal integration, (vi) Digital Assets as a global payment system.

Analyzing history of Digital Assets, we summarize that Digital Assets were developed with the intent to liberate payment systems from existing financial supervision. Once such system became functional it was immediately abused. In connection with technical solutions, we find that as technical complexity of Digital Assets (especially the lack of the trusted third party) diminishes protection of Digital Assets users, it incentivizes criminal activity. Consequently, Digital Assets are vastly abused for different criminal purposes, including development of services dedicated to criminal activity, such as Dark Web Marketplaces or Digital Assets Mixer. Further, Digital Assets are used for payments on minimal scale, and the retail use if practically nonexistent. Currently, Digital Assets' legal integration is slow and fractional; however, we predict its positive developments in respect of the upcoming European regulation on Markets in Crypto Asset.

We conclude that Digital Assets such as Bitcoin do not represent a truly functional global payment system. We show that no one uses them as a medium of exchange, and that Digital Assets are used rather as investments. Despite its presence we find the crime wave associated with Digital Assets transitory. Finally, we expect that in future, once proper regulation is in place, Stablecoins will be a functional global payment system.

Key Words

Digital Asset, Distributed Ledger Technology, MiCA

Finančněprávní aspekty globálních platebních systémů

Abstrakt

Disertační práce shrnuje poznatky o vývoji digitálních aktiv, které spadají do éry Blockchainu 1.0. Při studiu a zpracování dostupných dat jsme se zaměřili na následující oblasti: (i) historické aspekty digitálních aktiv, (ii) technická řešení digitálních aktiv, (iii) skutečné využití digitálních aktiv, (iv) zneužití digitálních aktiv, (v) právní začlenění digitálních aktiv, (vi) digitální aktiva a jejich schopnost fungovat jako globální platební systém.

Z analýzy historických dat vyplývá, že digitální aktiva byly vyvinuty tak, aby na ně nedosáhla ruka stávajícího finančního dohledu. V důsledku toho byl takový systém od začátku zneužíván. Ukazuje se, že s tím, jak technická složitost digitálních aktiv (zejména absence centrální autority) snižuje ochranu nezkušených uživatelů digitálních aktiv, motivuje ostatní k trestné činnosti. V důsledku toho jsou digitální aktiva ve velké míře zneužívány k různým kriminálním aktivitám, včetně vývoje služeb určených čistě k trestné činnosti, jako jsou Dark Web Marketplaces nebo Digtal Asset Mixers. Další důležitou skutečností je, že se digitální aktiva používají k platbám v minimálním rozsahu a jejich maloobchodní využití, prakticky neexistuje. V současné době je právní integrace digitálních aktiv pomalá a dílčího charakteru, nicméně s ohledem na nařízení EU o trzích s kryptoaktivy předpovídáme její pozitivní vývoj.

Došli jsme k závěru, že digitální aktiva, jako je Bitcoin, nepředstavují skutečně funkční globální platební systém. Ukazujeme, že je nikdo nepoužívá jako prostředek směny a že pokud už se digitální aktiva používají, potom spíše jako investice. Navzdory aktuálně vysoké vlně kriminality s digitálními aktivy spojené, považujeme tento negativní jev za přechodný. Po zvážení všech skutečností nicméně očekáváme, že v budoucnu, až bude zavedena stálá regulace, budou Stablecoiny, funkčním globálním platebním systémem.

Klíčová slova

Digitální aktiva, Distributed Ledger Technology, MiCA