

Tato práce se zabývá analýzou blockchainu používaného pro Bitcoin. Blockchain je distribuovaná databáze všech uskutečněných transakcí s touto kryptoměnou. Její veřejná dostupnost představuje možnost zkoumání přesunů prostředků mezi veškerými uživateli. Ti však v transakcích vystupují pod anonymními adresami, jejichž počet je prakticky neomezený. Hlavním cílem naší práce je nalézt klastrování adres odpovídající jejich příslušnosti k reálným uživatelům. V práci navrhujeme nové heuristiky, které lze při klastrování využít. Hlavním přínosem je metoda, která využívá vlastnosti velmi rychle po sobě vytvořených transakcí. Dále analyzujeme problém vzniku superklastru obsahujícího neúměrně velkou část adres a navrhujeme způsob, jakým lze klastr vhodně rozdělit.