VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

HEURISTIKY PRO DEANONYMIZACI V SÍTÍCH KRYPTOMĚN

DEANONYMIZATION HEURISTICS FOR CRYPTOCURRENCIES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. MATYÁŠ ANTON**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. VLADIMÍR VESELÝ, Ph.D.**
SUPERVISOR

BRNO 2019

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav informačních systémů (UIFS) Akademický rok 2018/2019

Zadání diplomové práce

Student: **Anton Matyáš, Bc.**
Program: Informační technologie Obor: Počítačové sítě a komunikace
Název: **Heuristiky pro deanonymizaci v sítích kryptoměn**
Deanonymization Heuristics for Cryptocurrencies
Kategorie: Počítačové sítě

Zadání:

1. Nastudujte si teorii za nejdůležitějšími kryptoměnami (Bitcoin, Ethereum, Ripple, EOS, Stellar, Cardano) a seznamte se s jejich provozní praxí.
2. Seznamte se s problematikou clusterizace adres kryptoměn, obfuskaci objemů přenesených prostředků a mixováním transakcí.
3. Dle doporučení vedoucího navrhněte vlastní řešení, které by se nad vybranými měnami/službami pokoušelo o deanonymizaci transakcí/adres.
4. Implementujte řešení v rámci již existujících nástrojů pro práci s kryptoměnami na projektu TARZAN.
5. Proveďte validační testování, diskutujte možná rozšíření.

Literatura:

- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.
- Ermilov, D., Panov, M., & Yanovich, Y. (2017, December). Automatic bitcoin address clustering. In *Machine Learning and Applications (ICMLA), 2017 16th IEEE International Conference on* (pp. 461-466). IEEE.

Při obhajobě semestrální části projektu je požadováno:

- Body 1 až 3.

Podrobné závazné pokyny pro vypracování práce viz http://www.fit.vutbr.cz/info/szz/

Vedoucí práce: **Veselý Vladimír, Ing., Ph.D.**
Vedoucí ústavu: Kolář Dušan, doc. Dr. Ing.
Datum zadání: 1. listopadu 2018
Datum odevzdání: 22. května 2019
Datum schválení: 9. května 2019

Abstrakt

Kryptoměny se dnes těší nebývalé oblibě, ať už díky své nezávislosti na institucích, nebo zdánlivé anonymitě, kterou poskytují. Ruku v ruce s tím však jde také jejich rostoucí zneužívání ke kriminálním aktivitám. Tato práce se zabývá zkoumáním principů a provozní praxe současných kryptoměn a technikami, které se v nich využívají pro zvýšení anonymity. Na základě zjištění následně navrhuje řešení pokoušející se o deanonymizaci aktivit v sítích vybraných kryptoměn.

Abstract

Nowadays, cryptocurrencies are growing more and more popular, both due to their independency on institutions and the feeling of anonymity they provide. This is, however, also accompanied by an increasing number of their abuse for criminal activities. This thesis explores the principles of current cryptocurrencies as well as techniques used for increasing anonymity of their usage. Based on the findings, it proposes a solution attemping to deanonymise activity in select cryptocurrencies.

Klíčová slova

Kryptoměna, blockchain, Bitcoin, Litecoin, Ethereum, CoinJoin, clusterizace, deanonymizace, Laravel, BestMixer

Keywords

Cryptocurrency, blockchain, Bitcoin, Litecoin, Ethereum, CoinJoin, clusterization, deanonymisation, Laravel, BestMixer

Citace

ANTON, Matyáš. *Heuristiky pro deanonymizaci v sítích kryptoměn.* Brno, 2019. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Vladimír Veselý, Ph.D.

Heuristiky pro deanonymizaci v sítích kryptoměn

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Ing. Vladimíra Veselého Ph.D. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Matyáš Anton
22. května 2019

Poděkování

Chtěl bych poděkovat vedoucímu práce, Ing. Vladimírovi Veselému, Ph.D., za trpělivost a za cenné rady, bez nichž by práce v této podobě nevznikla.

Obsah

Kapitola 1

Úvod

Kryptoměny získaly v posledních letech nebývalou popularitu. Důvodem je mimo jiné fakt, že poskytují rychlou, často levnou a na první pohled anonymní alternativu k běžným měnám. Právě ona anonymita však vede také k nezanedbatelnému počtu uživatelů využívajících kryptoměny pro své nekalé a mnohdy nelegální aktivity. Cílem této práce je navrhnout řešení, s jehož pomocí by bylo možné vybrané transakce deanonymizovat, a poté jej implementovat a otestovat úspěšnost tohoto návrhu. Projekt je vypracováván v rámci projektu Tarzan, který se zabývá bojem proti kyberkriminalitě.

Kapitola 2 se věnuje základním principům kryptoměn. Rozebírá jejich vlastnosti a předkládá výhody a nevýhody jejich používání oproti tradičním měnám a bankovním systémům. Následuje vysvětlení základů fungování decentralizovaného řízení, na němž měny staví, a principů clusterizace spolu se základními metodami, které se proti ní snaží bojovat. Závěrečná část kapitoly je věnována popisu vybraných v současnosti populárních kryptoměn, jejich vlastností, provozní praxe a specifických kroků, které podnikají pro zvýšení anonymity. Analýza a návrh, jimiž se zabývá kapitola 3, zahrnují rozbor 6 mixovacích služeb, a to jak z hlediska vnějšího, tedy jaké služby nabízí, tak vnitřního, neboli jak fungují. Na základě prvotních zjištění navrhuje práce pro jednu z nich, jež se z výsledků jevila jako deanonymizovatelná, heuristiky umožňující párovat jejich vstupní a výstupní transakce. Následně nad ní provádí další testování a přichází s vylepšenou variantou heuristik, která lépe odpovídá funkci služby. Kapitola 4 popisuje návrh aplikačního řešení za použití frameworku Laravel. Rozebírá architekturu vytvořené webové aplikace a dále posloupnost její činnosti navenek i po programové stránce. Úspěšnost řešení je dále ověřena v kapitole 5 s využitím sady příkladů činnosti mixovacích služeb získaných v průběhu zkoumání, jak vnitřně fungují. Výsledky jsou v závěru kapitoly okomentovány spolu se zamyšlením nad úskalími projektu a možnostmi jeho vylepšení. Shrnutí práce a její dopad poté předkládá závěrečná kapitola 6.

Kapitola 2

Principy kryptoměn

Pro hlubší studium kryptoměn je třeba nejprve objasnit jejich základní principy. Tato kapitola se zaobírá vlastnostmi kryptoměn a jejich výhodami a nevýhodami oproti běžným měnám. Následně (2.2) představuje modely, na jejichž základech fungují různé kryptoměnové sítě. Podkapitola 2.4 je věnována rozboru konkrétních kryptoměn reprezentujících odlišné přístupy k provozu i bezpečnosti.

2.1 Vlastnosti kryptoměn oproti běžným měnám

Obchodování za pomoci peněz či jiných platidel je již od pradávna nedílnou součástí lidských životů. S rozvojem civilizace a technologií se manipulace s těmito statky stávala stále jednodušší a dnes je možné během několika sekund poslat peníze třeba i na druhý konec světa. Všechny klasické měny si však s sebou nesou také jednu potenciální nevýhodu. Bývají spravovány jednou centrální autoritou, například centrální bankou nebo vládou, která se stará o jejich emisi a má nad nimi plnou kontrolu. Přísun peněz na trh může regulovat zcela dle vlastního uvážení a tím zásadně ovlivnit jejich hodnotu, zvláště pak směrem dolů.[21]

Právě tomuto neduhu se snaží předejít kryptoměny. Obecně se jedná o množinu digitálních platidel zabezpečených za pomoci asymetrické kryptografie. Na rozdíl od klasických měn, využívajících institut centrální autority, jsou kryptoměny vystavěny na principu decentralizované sítě počítačů využívajících peer-to-peer komunikaci (tedy takovou, kde mají všechny zúčastněné strany ekvivalentní pozici). K rozhodnutím, která by běžně vykonávala autorita (např. legitimnost transakcí), tak mohou v rámci sítě přispívat někdy i statisíce uživatelů a jejich schvalování proto probíhá na základě konsenzu – shody většinové části uzlů. Nemělo by tak být možné, aby někdo se stavem měny manipuloval ve svůj prospěch či snad dokonce falšoval pohyby kryptopeněz, jelikož na to by musel ovládat přes padesát procent výpočetní síly v celé síti. S tím souvisí také absence omezení, se kterými se je možné setkat při spolupráci s bankami a dalšími prostředníky — ať už se jedná o limit přenášených peněžních objemů, cílových a zdrojových účtů, nebo dokonce úplné odstavení přístupu k finančním prostředkům. Současně se však vytrácí i jimi poskytované bezpečnostní mechanismy chránící uživatele před krádežemi či omyly při zadávání pokynů k platbám, které je možné v systému s autoritou oznámit a nechat odpovídající transakci odvolat. Jakmile je transakce jednou potvrzena v kryptoměnové síti, je platná a nelze ji již nijak vzít zpět. Stejně tak není bez spravující třetí strany možné obnovit přístup k elektronické peněžence. Pokud vlastník zapomene nebo ztratí své přístupové údaje, stanou se prostředky v ní uložené navždy nedostupnými.

Jednou z výhod, které kryptoměny oproti běžným měnám nabízejí, je globálnost a nezávislost na státních hranicích. Standardní převody mimo státní území jsou obvykle zdlouhavé a obnáší vysoké poplatky třetí straně, která je zprostředkovává. Kryptoměnové transakce jsou si všechny rovny bez ohledu na množství peněz i to, jestli je protistrana soused odvedle, nebo osoba vzdálená desetitisíce kilometrů. Totéž platí i pro poplatky za jejich vykonání. Ty bývají obvykle nízké, někdy i zcela nulové. Odvíjí se však především od aktuální zatíženosti uzlu, kterému jsou odměnou. S vyšším poplatkem získává transakce větší prioritu a v případě velkého zahlcení tak může cena citelně vzrůst.

Spíše staronovou vlastností kryptoměn je anonymita, resp. pseudonymita. Peněžní hotovost klasických měn je zaměnitelná, a její pohyby a původ, s výjimkou situací, kdy se jedná o čerstvě vytištěnou řadu, která právě vyšla z banky, není možné spolehlivě dohledat. v digitálním světě je však jedinou alespoň vzdáleně se anonymitě blížící možností založení konta v bance na území některé ze zemí, které nespolupracují s místními orgány a nepředávají tudíž údaje o vlastnících. a i zde bude použitelnost spíše k jednorázové anonymizaci než k pravidelnému užívání, vzhledem k poplatkům, které s mezinárodními převody souvisí. v sítích kryptoměn naproti tomu všichni vystupují pod pseudonymy, představovanými náhodně generovanými adresami, a není tak možné spojovat účty s konkrétními osobami, pokud se k jejich vlastnictví samy nepřihlásí. Stejně tak není vlivem distribuovaného charakteru sítě možné jednoznačně určit ani zdroje pokynů k transakcím, jelikož uzel v příchozím směru může být pouze přeposílajícím.

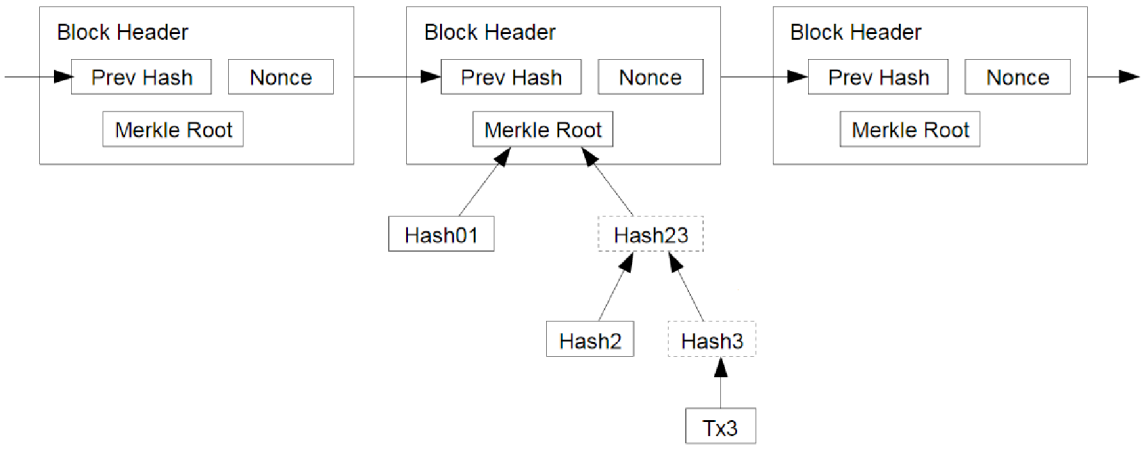
Ani pseudonymita však nepředstavuje nepřekonatelnou ochranu identity majitelů účtů. Hlavním důvodem je další z vlastností většiny kryptoměn, a to transparentnost. Historie veškerých transakcí je přístupná každému za všech okolností. Je tedy možné sledovat platby mezi adresami i vzorce nakládání s prostředky. Na jejich základě lze poté mnohé adresy spárovat jakožto patřící pod jednoho majitele. Dalším z tohoto pohledu kritickým bodem jsou operace vyžadující interakce s reálnou identitou, jakými mohou být například využívání některých směnáren, vklady a výběry z peněženky, nebo i jen prosté platby známým subjektům (ať už jde o konkrétní osoby, nebo obchody). Pomoci s párováním navíc mohou i další tzv. *offchain* informace, tedy údaje z jiných zdrojů, než je historie transakcí, například z internetové komunikace.

I přes svou povahu měn, které nelze ovlivňovat změnami v jejich emisi (jejíž princip bude dále vysvětlen v podkapitole 2.2), nejsou však kryptoměny stálé, jak by se na první pohled mohlo zdát. Právě naopak. v závislosti na náladách ve společnosti, dění na burzách, ale i akcích samotných států, na nichž by měly být teoreticky nezávislé, mohou jejich ceny zásadně kolísat, příkladem budiž čínský zákaz užívání bitcoinu v bankovním sektoru a následné zásahy do možností jeho těžby, které v posledním roce nezanedbatelně tlačí cenu dolů i přes do té doby výrazný růst[8].

2.2 Transakce a emise v oblasti kryptoměn

2.2.1 Blockchain

Při používání libovolné formy nehmotných platidel je třeba vypořádat se s problémem placení prostředky, které některá ze stran nevlastní, případně opakovaného placení týmiž. v případě hmotných statků byl problém vyřešen již z jejich podstaty – fyzickým předáním se vlastnictví jednoznačně přenese. Situace se však zkomplikovala s příchodem bezhotovostních styků, ať už šlo o šeky, nebo pohyby peněz mezi účty. Pokud by neexistovala žádná forma kontroly, záleželo by vše jen na dobrém slovu protistrany a snadno by tak docházelo



Obrázek 2.1: Zjednodušené schéma blockchainu kryptoměny Bitcoin[20]

k podvodům. Roli dohlížejícího arbitra proto zaujímá centrální autorita, obvykle banka. v decentralizovaném systému, jakým jsou kryptoměny, je však nutný jiný způsob ověřování. Tím je právě blockchain[20], jemuž se věnuje tato sekce.

Jedná se o datovou strukturu, která po vzoru účetní knihy obsahuje historii veškerých proběhlých transakcí. Její obsah je veřejně přístupný a kopie se nachází na všech plnohodnotných uzlech v síti. Na nejvyšší úrovni blockchain, jak jeho název napovídá, sestává z řetězu bloků, tvořeného zpětně zřetězeným lineárním seznamem. Provázání bloků je realizováno skrze hashe – každý blok v sobě nese informaci o hashi svého předchůdce. Díky tomu není možné, aby někdo změnil historii tím, že bloky v řetězu zpětně nahradil jinými nebo dokonce včlenil nové.

Samotné bloky pak obsahují jednotlivé podmnožiny transakcí, uspořádané do tzv. *Merkleova stromu*. Data transakcí jsou v tomto binárním stromě uložena v listech, zatímco uzly obsahují konkatenaci hashů svých potomků. Kořenový hash je uložen v hlavičce bloku. Výsledkem této techniky je efektivnější ověřování integrity dat v bloku, jelikož pro kontrolu hashe není potřeba ověřovat veškeré přítomné transakce.

Transakce po svém zadání nejsou vykonány okamžitě. Místo toho se zařadí do množiny k ostatním, které čekají na vyřízení, a odtud jsou postupně vybírány a zařazovány do bloků. Proces vytváření nových bloků řetězu probíhá decentralizovaně, na mnoha uzlech sítě současně. Pro správné fungování je však třeba, aby byla podoba blockchainu pro všechny účastníky stejná. Způsoby, jak se v této situaci dosahuje konsensu, se budeme zabývat v následujících podkapitolách.

2.2.2 Proof of Work

Vytváření bloků za pomoci systému Proof of Work[3] se nazývá *těžba* (anglicky *mining*). Uzly provádějící těžbu, označované jako *mineři*, postupně ověřují platnost transakcí a vkládají je do bloku. Jako klíč pro určení pořadí zpracování slouží výše poplatku stanoveného zadavatelem transakce, tedy částka, která bude jako odměna za vyřízení odevzdána zpracovávajícímu uzlu. Po naplnění bloku začne uzel počítat jeho hash, jehož hodnota musí spadat do stanoveného rozmezí (nazývaného obtížnost). Jestliže výsledný hash tuto podmínku nesplňuje, je třeba blok upravit a pokus opakovat. Pro tyto účely je v hlavičkách bloků vyhrazeno pole *nonce*, jehož obsah je možné libovolně měnit.

První z uzlů, jemuž se podaří najít *nonce*, které vyústí v blok s platným hashem, se stává vítězem a může jej umístit do blockchainu. Jelikož jsou ovšem systémy kryptoměn decentralizované, informace o nalezení nového bloku se v nich šíří postupně. Může tak dojít k situaci, že některý z dalších uzlů sítě vytvoří nový blok také, dříve než se k němu informace o vítězi zpropaguje, a blockchain se rozvětví.

Vzniklá nejednoznačnost se řeší pravidlem *longest chain*[9], tedy tak, že nové bloky jsou vždy připojovány na konec nejdelší větve řetězu a ta je považována za platnou. Transakce z ostatních větví se nicméně neztrácí. Pokud se v nejdelší větvi dosud nenachází, jsou zařazeny zpět do množiny čekající na zpracování.

Důsledkem tohoto systému je, že zabezpečení bloků proti modifikacím a podvrhování se s přibývajícími následníky v řetězu (a tedy s postupem času) zvyšuje. Potenciální útočník by totiž pro zásah musel krom hashe bloku samotného přepočítat také veškeré jeho nástupce a současně předehnat ostatní uzly v síti, aby vytvořil nejdelší řetěz. Klíčovou vlastností pro fungování celého systému je asymetričnost použité hashovací funkce. Výpočet hashe (a tedy nalezení správného *nonce*) musí být výpočetně náročný, ale ověření jeho správnosti musí být snadné. Konkrétní použitá funkce se nicméně odvíjí od příslušné kryptoměny.

2.2.3 Proof of Stake

Alternativním způsobem pro dosažení konsensu ohledně generovaných bloků je přístup Proof of Stake[29]. Na rozdíl od metod založených na řešení náročných matematických úloh zde záleží především na množství vlastněné měny. o tom, čí blok bude zařazen, je rozhodováno na základě semináhodné volby. Uzly mohou vsázet svoje mince a pravděpodobnost vybrání konkrétního uzlu se odvíjí od toho, jaký podíl celkové částky jeho sázka představuje.

Koncept vychází z předpokladu, že získat 51 % existující měny potřebných pro ovládnutí blockchainu by bylo příliš nákladné a pokud by k této situaci přesto došlo, neměl by jejich vlastník důvod k nekalé činnosti, jelikož by zásady do blockchainu devalvoval vlastní majetek. Přesto však tato potenciální centralizace řízení jde proti myšlence kryptoměn, a proto jsou v řadě realizaci Proof of Stake do volby bloku zahrnuty také další faktory, jako například stáří vsazených mincí.

Možná je také delegovaná varianta Proof of Stake, při níž je rozhodování přenecháno omezené množině uzlů a stanoví se náhradníci pro případ jejich nezpůsobilosti, viz 2.4.9.

2.3 Clustering a opatření proti jeho realizaci

Jednou z hlavních myšlenek kryptoměn je pseudonymita. v transakcích je účet identifikovaný pouze adresou, která by v ideálním případě neměla poskytovat žádné spojení se skutečnou identitou vlastníka nebo jeho dalšími účty. Jelikož je však blockchain v síti Bitcoinu a řady dalších kryptoměn veřejně přístupný, nabízí informace o transakcích v něm uložených prostor k hlubší analýze.

2.3.1 Clustering

Vzhledem k doporučované jednorázovosti adres a potřebě uchovávat klíče, které s nimi umožňují manipulovat, s používáním sítě značně narůstá množství informací, které uživatel musí ukládat. Tento problém řeší klientské aplikace nazývané peněženky, které jednotlivé účty a jejich klíče spravují a umožňují s nimi nakládat jako s jediným účtem. Problém

nastává ve chvíli, kdy je podobná množina účtů použita k platbě. Jelikož vstupy transakcí jsou v sítích na bázi Bitcoinu nutně navázány na nedělitelné výstupy již proběhlých transakcí a požadovanou částku je tak složit z dostupných hodnot, vzniká v blockchainu doklad o potenciální souvislosti adres. Proces vyhledávání těchto souvislostí a určování adres spadajících pod stejnou peněženku – a tedy i vlastníka – se nazývá *clusterizace*[10], zatímco množiny takto sdružených adres *clustery*. S využitím dalších informací získatelných z off-chain zdrojů, jakými mohou být například fóra nebo sociální sítě, je navíc možné některé adresy spárovat s konkrétními osobami nebo institucemi a prolomit tak anonymitu úplně. Na následujících řádcích jsou popsány příklady některých heuristik používaných pro clusterizaci v rámci blockchainu.

Jedním z jevů ukazujících na společného vlastníka adres se zabývá heuristika společné útraty[10]. Pokud má transakce na vstupu více adres a pouze jedinou výstupní, dá se předpokládat, že všechny vstupy patří jediné osobě. v případě, že by bylo na výstupu více adres, heuristika stále může být platná, použil-li odesilatel některou z běžných klientských peněženek. Jistota se však ztrácí vzhledem k příchodu techniky CoinJoin popsané níže.

Další možností párování je využití častých vlastností adresy pro drobné [22]. Ta vychází z předpokladu, že peněženka pro příjem přebytku z platby generuje pokaždé novou adresu. Pokud má tedy transakce 2 výstupy a právě jeden z nich je dosud nepoužitá adresa, je šance, že je rovněž vlastněna odesilatelem. Postup je možná dále kombinovat například se znalostí, že klienti při budování transakce eliminují nepotřebné vstupy, které by vedly ke zvětšení a v důsledku prodražení transakce. Pokud je tedy navíc některý z výstupů dané transakce menší než libovolný ze vstupů, jedná se pravděpodobně o adresu pro drobné.

2.3.2 Mixování transakcí

Clustering značně snižuje míru soukromí v rámci sítě, což mnozí mohou považovat za nežádoucí. z toho důvodu vznikají obfuskační techniky, jejichž cílem je heuristiky clusteringu znefunkčnit. Jednou z variant je mixování transakcí[19], které se pokouší propojit transakce různých entit tak, aby účastníky nebylo možné na výstupu rozlišit.

Příkladem takové techniky je *CoinJoin*[12], neboli sloučení vstupů a výstupů z více transakcí do jedné. v případě zásadně rozdílných částek však je možné vazby mezi některými vstupy a výstupy určit na základě určení možných kombinací vstupů a výstupů. Příkladem budiž následující bitcoinová transakce[1]:

Vstupy:	**Výstupy:**
A1: 0,01053 BTC	B1: 0.18230926 BTC
A2: 0,19280926 BTC	B2: 0.01 BTC
A3: 0,01 BTC	B3: 0.01 BTC
	B4: 0,01 BTC

V uvedené tabulce je vidět, že vstup A2 a výstup B1 mají znatelně vyšší hodnoty než ostatní. Současně by kombinací zbylých vstupů nebylo možné hodnoty B1 dosáhnout. z toho vyplývá, že mezi vstupem A2 a výstupem B1 existuje spojení. Základní varianta CoinJoinu navíc trpí problémem, jak domluvit společnou transakci, aniž by byla prozrazena identita účastníků. Je třeba vzájemné důvěry mezi zúčastněnými, nebo vložit důvěru ve službu třetí strany, která transakci zorganizuje. Se zmíněnými nedostatky CoinJoinu se pokouší vypořádat technika PrivateSend, používaná v síti kryptoměny Dash (viz 2.4.3).

[1] CoinJoin transakce https://www.blockchain.com/btc/tx/92a78def188053081187b847b267f0bfabf28368e9a7a642780ce46a78f551ba

Alternativou ke CoinJoinu je využití centralizovaných mixovacích služeb, které opět staví na nutnosti důvěry v třetí stranu. Uživatel službě zašle peníze, ta provede jejich vyprání a odpovídající částku zašle na zvolenou adresu, často s volitelným zpožděním pro ztížení dohledatelnosti. Samotné praní může probíhat sloučením vkladů na jednu adresu a jejich opětovné rozdistribuování mezi zákazníky, nebo mixováním na principech CoinJoinu. Rozdíly se mohou vyskytovat také v původu peněz určených k vyplacení klientů, resp. v tom jestli je možné získat na výstupu tytéž mince, jež uživatel vložil. k tomu může dojít v případě výplat za použití množiny aktuálně vložených peněz. Druhou možností je vyplácet klienty z interní zásoby peněz budované skrz vklady předchozích klientů, případě z vlastního kapitálu, čímž se vazba mezi vstupy a výstupy zcela rozpadne.

Existuje i mnoho dalších možností obfuskace transakcí. Většinou jsou však specifické pro konkrétní měny, jež je implementují, a proto byly jejich popisy umístěny do odpovídajících částí následující podkapitoly.

2.4 Srovnání konkrétních kryptoměn

2.4.1 Bitcoin

Bitcoin, označovaný také zkratkou *BTC*, je nejstarší a v současnosti nejdominantnější z kryptoměn. Vznikla v roce 2009 a za jejím návrhem stála neznámá osoba nebo skupina osob vystupující pod jménem Satoši Nakamoto. Nejmenší částka, jakou je možné v rámci měny rozlišit, tedy $10^{-}8$, je na počest tohoto tvůrce označována jako *1 satoši*.

Generování nových bloků blockchainu využívá princip Proof of Work blíže popsaný v kapitole 2.2.2. Kromě zabezpečení před manipulací s historií a prevence neoprávněného využívání prostředků má však tento přístup ještě druhou funkci, slouží k emisi nových mincí. Mimo standardních transakcí vkládá miner na začátek bloku také tzv. *coinbase transakci*. Jedná se o zvláštní transakci s jediným vstupem, *coinbase*, který generuje nové mince. Výstupy jsou poté standardní adresy, na něž mají být peníze rozeslány (obvykle patřící těm, kdo se podíleli na vytěžení bloku).

Po vzoru reálného světa, kde surovinám, jako je zlato, dodává na ceně jejich vzácnost, je i množství uměle Bitcoinů omezené. Počet nově emitovaných mincí se postupně snižuje, a to tak, že po každých 210 000 připojených blocích klesne stávající hodnota na polovinu. z původních 50 BTC za blok tak v současnosti odměna klesla na 12,5 BTC a další snížení je odhadováno na 25. května 2020[2].

Nuly dosáhne v roce 2140, kdy se přísun měny definitivně uzavře na celkovém objemu 21 milionů BTC a poté již budou těžícím uzlům odměnou pouze poplatky za zpracování transakcí. Pro výpočet hashů bloků se v síti Bitcoin používají dva průchody algoritmu SHA-256. Jak se ovšem postupem času ukázalo, není pro účely systému Proof of Work příliš vhodný, jelikož umožňuje snadnou implementaci a paralelizaci v hardwaru. Z běžných CPU a GPU osobních počítačů se tak těžba postupně přesouvala také na specializované ASIC obvody, vyřazující ze hry běžné uživatele. v zemích s levnou elektřinou, jako je Čína, navíc vznikají velké výpočetní farmy ovládané malým počtem osob, a dochází tak opět k jisté formě centralizace[14].

S nárůstem výpočetních zdrojů přirozeně klesá také čas potřebný pro vytěžení jednoho bloku. Stejně tak může v síti dojít k úbytku těžících uzlů, což těžbu bloků naopak zpomalí. z toho důvodu je obtížnost hledání *nonce* každých 2016 bloků přepočítávána tak, aby interval mezi bloky (a v důsledku tempo vydávání nových mincí) zůstával přibližně 10 minut.

[2]Bitcoin Block Reward Halving Countdown http://www.bitcoinblockhalf.com/

Nová obtížnost se určuje na základě vzorce:

$$obtiznost_{n+1} = obtiznost_n \times \frac{(ocekavany\ \ cas)}{(realny\ \ cas)}$$

Ocekavany cas je 2016 bloků po 10 minutách, tedy 20 160 minut. *Realny cas* přestavuje dobu, za kterou bylo posledních 2016 bloků vytěženo ve skutečnosti.

Koncept účtů známý z klasického bankovnictví je v případě Bitcoinu reprezentován dvojicí soukromého a veřejného klíče generovanou za pomoci asymetrické kryptografie. Veřejný klíč, neboli adresa, slouží jako identifikátor účtu v rámci transakcí. Soukromý klíč plní funkci autorizace a umožňuje majiteli nakládat s finančními prostředky, které jsou s účtem spjaté. Na rozdíl od běžných účtů však adresa sama o sobě nenese žádnou informaci o svém finančním zůstatku. Ten se určuje na základě informací z transakcí uložených v blockchainu.

Data transakce jsou tvořena dvěma množinami – vstupy a výstupy – kde jednotlivé vstupy vždy musí odpovídat výstupům jiné, již proběhlé transakce. Částku v rámci jednoho vstupu navíc nelze rozdělit a musí být při transakci spotřebována celá. Pokud tedy hodnota vstupu převyšuje částku určenou pro příjemce, nezbývá než přidat mezi výstupy transakce tzv. adresu pro drobné (*change address*), kam bude přebytek zaslán. Tou může být jak nově vygenerovaná adresa, tak některá ze stávajících (včetně zdrojové). Znovupoužití adres se však nedoporučuje, jelikož může vést ke sledování nákupů a dalších aktivit vlastníka a narušit tak jeho anonymitu. v případě, že přebytky ze vstupů transakce nemají určenu výstupní adresu, jsou automaticky považovány za poplatek pro *minera*. Z tohoto principu vyplývá, že zmiňovaný aktuální zůstatek na účtu je možné stanovit jakožto součet výstupů transakcí ve prospěch účtu, které dosud nebyly dále využity.

Slabinou sítě Bitcoinu je její špatná škálovatelnost, daná kombinací dvou faktorů. Prvním je již zmíněný pevný desetiminutový interval mezi jednotlivými nově přidávanými bloky. Ten sám o sobě není nutnou komplikací, jelikož by způsoboval prodlevu nanejvýš právě těchto deset minut. Situace se však mění vlivem druhé vlastnosti, kterou je omezená velikost bloku. Pro záznamy o transakcích je tak k dispozici pouze 1 MB paměti. Výsledkem je, že propustnost sítě je stále stejná (cca 7 transakcí za sekundu) bez ohledu na počet aktivních uzlů a v případě velkého počtu požadavků může dojít k prodlevám, hromadění transakcí a v důsledku také prudkému růstu poplatků za přednostní zpracování. Snaha o řešení tohoto nedostatku vyústila v několik návrhů vylepšení protokolu.

Technika SegWit, neboli Segregated Witness („segregovaný svědek“)[16], přistupuje k řešení formou snahy o navýšení počtu transakcí, které je možné uložit v rámci jednoho bloku. Toho dosahuje skrze rozdělení transakcí na dvě části – podpisy používané pro validaci transakce jsou odděleny od vstupů a výstupů a umístěny do samostatné struktury na konec transakce. Současně je zaveden nový způsob výpočtu limitu velikosti bloku na základě tzv. váhových jednotek (WU) s limitem 4 000 000. Pro data o vstupech a výstupech odpovídá 1 byte 4 WU, tedy původnímu limitu 1 MB. Sekce s podpisy však využívá vztah 1 byte = 1 WU, a má tak čtyřnásobnou kapacitu, což vede k nezanedbatelné úspoře. Současně tento systém umožňuje uvedení do provozu bez narušení zpětné kompatibility s dosud neaktualizovanými uzly. Část s podpisy je jimi jednoduše ignorována a samotné vstupy a výstupy, vnímané starým uzlem tak, že mohou být utraceny kýmkoli, nemohou překročit původní limit 1 MB.

Pro snadné rozlišení mezi klasickým typem adres a novými, které využívají SegWit, byl zaveden jednotný formát. Původní adresy mají na začátku 1, zatímco adresy využívající SegWit začínají 3 nebo bc1.

Lightning Network[27] je vylepšení, jehož cílem je vyřešit potíže se škálováním sítě přenosem vybraných transakcí mimo blockchain do samostatné platební vrstvy. Zasláním zvláštní transakce (nebo transakcí) s počátečním vkladem mezi sebou mohou dvě strany vytvořit tzv. platební kanál. v rámci něj následně mohou mezi sebou vložené finance libovolně redistribuovat, a to opakovaně a takřka bez čekání. Prostředky je navíc možné oboustranně převádět po malých částech, aniž by se tím kumulovaly poplatky transakce, jelikož kanál zůstává otevřený, dokud jej některá ze stran neukončí. v tu chvíli se aktuální stav rozložení prostředků zapíše zpět do klasického blockchainu, čímž se definitivně potvrdí. Veškeré transakce v rámci kanálu musí být pro nabytí platnosti podepsány – a tedy schváleny – oběma zúčastněnými stranami.

Platby je možné provádět také zprostředkovaně. Mají-li obě strany otevřený platební kanál s třetí stranou, může být využita jakožto prostředník, aby nebylo nutné vytvářet nový platební kanál a platit tak jeho ustavení a rušení. Jelikož kromě počátečního vkladu a ukončovací transakce probíhá veškerá manipulace s prostředky mimo blockchain, technika výrazně zkracuje dobu vyřízení požadavků a snižuje zahlcení kryptoměnové sítě. Současně s sebou toto řešení přináší taky posílení soukromí, neboť většina aktivity není zapsána v blockchainu a vědí o ní pouze zúčastněné strany, případně prostředníci.

2.4.2 Litecoin

Litecoin[11], označovaný zkratkou *LTC*, vznikl v roce 2011 jako jeden z klonů Bitcoinu s cílem vytvořit odlehčenou, rychlejší a levnější alternativuṄaváže-li na analogii z podkaptioly 2.4.1 přirovnávající Bitcoin ke zlatu, Litecoin mezi pomyslnými vzácnými kovy představuje stříbro. Pro hashování bloků používá algoritmus *scrypt*, který byl navržen tak, aby byl odolný proti hardwarovým útokům. Dosahuje toho vysokou paměťovou náročností, která vede k vysoké ceně případných specializovaných obvodů a značně tak omezuje možnosti paralelizace výpočtu[25].

Tvorba bloků (a tedy zpracování transakcí) je oproti Bitcoinu skutečně rychlejší. Optimální čas pro nalezení konsensu skrze Proof of Work je v síti Litecoin stanoven na 2,5 minuty, tedy čtvrtinovou dobu než u Bitcoinu. Odměna pro minera se nicméně půlí až každých 840 000 bloků, a proto i zde dojde k ukončení přísunu mincí odhadem kolem roku 2140 (resp. 2142, jelikož je Litecoin o dva roky mladší). Celkový počet však bude čtyřnásobný (84 milionů LTC). Motivací k tomuto kroku bylo umožnit uživatelům měny platit v celých částkách. I přesto však, stejně jako původní Bitcoin, Litecoin poskytuje v transakcích možnost definovat obnosy s přesností na 8 desetinných míst. Z Bitcoinu byla převzata také podpora některých nástrojů podporujících anonymitu, např. SegWit a Lightning Network.

2.4.3 Dash

Dash[18] je dalším představitelem měn založených na Bitcoinu. Vznikl s cílem umožnit okamžité vykonávání plateb a vyšší míru soukromí. Vedle běžných těžících uzlů v síti tentokrát existují i takzvané *master* uzly, které krom běžných funkcí poskytují také pokročilé služby sítě. Systém Proof of Work v případě Dashe využívá hashovacího algoritmu X11. Jak jeho název naznačuje, používá posloupnost jedenácti algoritmů, které jsou postupně aplikovány na výstup. Výsledná složitost má alespoň dočasně zabránit nástupu specializovaných ASIC obvodů pro těžbu bloků.

Aby mohl uzel sloužit jako master, musí se prokázat vlastnictvím alespoň 1000 DASHů a být konstantně dostupný, což je průběžně ověřováno ostatními master uzly. Motivací jejich pro provozovatele je finanční kompenzace v podobě 45 % z odměny za vytěžení bloku,

která se mezi ně rozdělí. Významnou dvojici služeb, kterou uzly poskytují, jsou *PrivateSend* a *InstantSend*.

InstantSend je službou umožňující okamžitý převod mincí bez nutnosti čekání na to, až bude transakce zanesena do bloku. Master uzly mezi sebou rozešlou informaci i transakci a následně uzamknou její vstupy, aby nebylo možné přijmout žádnou jinou transakci nebo blok, který se je pokusí spotřebovat.

PrivateSend je služba poskytující zvýšení soukromí při manipulaci s penězi. Jedná se v principu o CoinJoin (viz 2.3.2), avšak doplněný o kroky zabraňující standardnímu párování vstupů a výstupů. Mixování vyžaduje tři účastníky, kteří na vstupu i výstupu využijí shodné částky. Pro usnadnění jsou standardizovány hodnoty 0,1, 1, 10, 100 a 1000 DASH. Jelikož i v tomto případě lze s pravděpodobnosti 1:3 určit spojení mezi vstupem a výstupem, mixování se obvykle provádí zřetězeně napříč více master uzly, čímž se možnosti párování exponenciálně snižují. Pravděpodobnost, že by se do sítě dostal dostatečný počet master uzlů s nekalými úmysly, aby bylo možné tok mincí při mixování sledovat, je vzhledem k omezené zásobě mincí v oběhu, požadovanému vstupnímu kapitálu a náhodné povaze volby použitého master uzlu, mizivá.

2.4.4 Zcash

Kryptoměna Zcash[13] vznikla stejně jako předchozí zmíněné odštěpením od původního Bitcoinu. Nejzásadnější změnou, kterou přinesl, jsou tzv. důkazy s nulovou znalostí (anglicky *zero-knowledge proofs*. Jedná se o kryptografickou metodu umožňující ověřit znalost určité hodnoty, aniž by musela být sdělena sama hodnota. v případě Zcash je použita varianta zK-SNARKs. S její pomocí je možné utajit v rámci transakcí informace o adrese příjemce, adresáta, i přenesené částce. Tato metoda se nazývá *shielding*.

V rámci sítě jsou poskytovány dva typy adres [26]. *Transparentní adresy* začínají písmenem t a svou strukturou a chováním de facto odpovídají těm bitcoinovým. Informace o těchto transakcích jsou v blockchainu veřejně dostupné. *Shielded adresy* naproti tomu začínají písmenem z a všechny informace o nich jsou skryté, z blockchainu tedy lze zjistit jen, že transakce proběhla, ale už ne mezi kým a čeho. Situace se komplikuje, interagují-li adresy rozdílných typů. v takovém případě nelze zajistit plné utajení, ale jen omezení informací na nutné minimum. Shielded adresy zůstávají v záznamu transakce skryté, zatímco transparentní jsou čitelné a je vidět i obnos, který přijaly nebo odeslaly.

2.4.5 Monero

Monero[17] je kryptoměna založená na protokolu CryptoNote, který se snaží vylepšit myšlenky Bitcoinu současně posílit soukromí v síti. Umožňuje anonymizovat transakce do takové míry, že není možné určit, jestli měly 2 platby stejného odesilatele, případně příjemce. Dosahuje toho skrze několik opatření.

Pro příjem jsou v síti používány tzv. *stealth adresy*. Ty umožňují skrze sadu několika veřejných klíčů generovat nové adresy, o jejichž existenci vědí pouze účastníci jednotlivých transakcí a jež může vybrat pouze cílová osoba s příslušnými soukromými klíči.

Na straně odesilatele jsou transakce podepisovány kruhovým podpisem (anglicky *ring signature*)[23]. Jedná se o podpis použitelný libovolným příslušníkem skupiny, které náleží, a není možné určit, čí klíč v rámci skupiny byl k podepsání použit. Skupiny se vytváří dynamicky kombinací soukromého klíče uživatele a veřejných klíčů z blockchainu. Vylepšená varianta *RingCT* navíc skrývá i přenesené objemy měny, čímž zabraňuje deanonymizaci skrze analýzu blockchainu.

2.4.6 Ethereum

Ethereum[28] na rozdíl od svých konkurentů není čistě kryptoměnovou sítí. Jedná se o distribuovaný turingovský úplný systém nad blockchainem, který je možné použít i pro další aplikace. Jednotkou kryptoměnové stránky sítě je 1 Ether (zkratka *ETH*), který je možné dělit s přesností až na 18 desetinných míst. Stejně jako v případě měn na bázi Bitcoinu stojí i zde blockchain na systému Proof of Work, ovšem s vlastním hashovacím algoritmem Ethash, navrženým tak, aby byl skrze svou paměťovou náročnost těžce implementovatelný specializovanými ASIC obvody. z důvodu energetické náročnosti těžby nicméně vývojáři do budoucna plánují přechod na protokol *Casper* založený na bázi Proof of Stake.

Bloky v síti vznikají výrazně rychleji než u Bitcoinu, cílí se na čas 12 sekund. Výsledkem je rychlejší zpracování transakcí na úkor vyššího počtu větvení a osiřelých bloků. Odměna za vytěžení bloku (momentálně 3 ETH) se v čase samovolně nemění. Je však v rámci boje s inflací dle potřeb modifikována vývojáři a již v současnosti je ohlášeno, že se do budoucna sníží na 2 ETH[7].

Roli standardních poplatků za realizaci transakce v případě Etherea zastupuje parametr *gas*, tedy jistá forma reprezentace energie potřebné pro vykonání kódu transakce, která se následně dle předpisu zpoplatní. Jedná se o způsob, jak řádně ohodnotit složitost transakce bez přímé vazby na měnu, a zároveň prevenci nekonečných smyček – jak již bylo zmíněno, skripty Etherea jsou turingovsky úplné a transakce tak mohou vykonávat komplexní kód v závislosti na aktuální situaci. S tím souvisí také existence dvou typů účtů. Externě vlastněné účty odpovídají účtům z běžných kryptoměn, řízeným uživateli skrze vlastnictví soukromého klíče. Zůstatky však jsou na rozdíl od měn založených na Bitcoinu uchovávány napřímo, nikoliv skrze výčet neutracených výstupů transakcí. Druhým typem jsou tzv. *smluvní účty*. Ty jsou uloženy uvnitř blockchainu a jakmile jsou přidány, neovládá je uživatel, ale jejich řídící kód. Stále však mají svůj vlastní zůstatek, mohou v reakci na dění v síti komunikovat s dalšími účty a dokonce i vytvářet transakce.

2.4.7 Ripple

Ripple[30] se mezi ostatními kryptoměnovými sítěmi poněkud vymyká. Vznikl totiž primárně pro účely levných a rychlých převodů mezi bankami a dalšími institucemi. Veškeré transakce jsou uloženy v neveřejné distribuované účetní knize, kterou v řádech sekund aktualizují vybrané validační servery, z většiny vlastněné právě bankami a dalšími institucemi.

V rámci sítě je možné obchodovat s libovolnými statky, ať už kryptoměnami, běžnými měnami, nebo třeba body věrnostních programů. Přesto však Ripple má i vlastní kryptoměnu, označovanou zkratkou XRP. Na rozdíl od standardních kryptoměn bylo všech 100 miliard XRP předgenerováno již na začátku a tvůrce sítě, Ripple Labs, Inc., je postupně vypouští do oběhu.

Z výše zmíněných důvodů je status Ripple jakožto typického zástupce kryptoměny poněkud diskutabilní, jelikož je v důsledku centralizovaný a v případě toku statků také nelze příliš mluvit o anonymitě. Přesto však jde v současnosti o kryptoměnovou síť s druhou nejvyšší hodnotou hned po Bitcoinu[3].

2.4.8 Stellar

Stellar[4] je platební síť vzniklá odštěpením od projektu Ripple a otevřením svých zdrojových kódů. Stejně jako původní síť umožňuje okamžité platby a směny v libovolných kryp-

[3] Top 100 Cryptocurrencies by Market Capitalization https://coinmarketcap.com/

toměnách i běžných měnách za nízké poplatky a cílí tak opět spíše na banky a další velké instituce. Zásadní rozdíl představuje přístup k budování účetní knihy. v případě Stellaru je síť decentralizovaná a využívá k dosahování konsensu vlastní algoritmus nazvaný *SCP*. Nabízí samozřejmě i vlastní měnu nazvanou *Lumen* (zkratka XLM). Vzhledem k účelům, za jakými síť vznikla, a jejímu původu však ani zde žádné zásadní vylepšení po stránce ochrany soukromí nenalezneme.

2.4.9 EOS

EOS[1] je platforma operující jako decentralizovaný operační systém. Snaží se tak navázat na koncept Etherea a jeho turingovské úplnosti umožňující provoz decentralizovaných aplikací, avšak s lepší škálovatelností a rychlostí odbavování transakcí. Platby za vykonání požadavků sítí jsou zcela volitelné a odvíjejí se od konkrétních aplikací, s nimiž uživatel interaguje. Zároveň je zaveden systém „obnovitelných zdrojů“, například CPU a paměti, které je možné od uzlů pro konkrétní činnost pronajmout zastavením částí svých mincí, a po uvolnění daných prostředků a uplynutí určené doby se opět obnoví.

Pro budování blockchainu slouží delegovaná varianta systému Proof of Stake, popsaného v 2.2.3. Uživatelé sítě si zvolí 21 delegátů, kteří budou mít na starost tvorbu bloků, a zjednoduší tak proces rozhodování. z volby vzejdou současně také náhradníci, kteří delegáty nahradí v případě, že by byl některý z nich mimo provoz nebo odvolán. Volby delegátů probíhají nejzákladnější formou Proof of Stake – kolik mincí hlasující vlastní, takovou má jeho hlas váhu.

Omezená množina rozhodujících uzlů si dává za cíl urychlit vytváření bloků, ale také zjednodušit eventuální zásahy do pravidel fungování sítě bez nutnosti její náhrady. Centralizace moci s sebou však přináší i řadu kontroverze[15]. Jak se ukázalo, arbitři sítě mohou v případě, že shledají, že byly něčí peníze zcizeny či jinak zneužity, zmrazit související účty a dokonce i provést návrat blockchainu do stavu před nežádoucí událostí, čímž se síť přibližuje klasickým bankovním systémům.

2.4.10 Cardano

Cardano[24] je další ze sítí, které se pokouší rozvíjet myšlenu decentralizované aplikační platformy. Zaštiťuje se přitom tím, že je první odborně posouzenou kryptoměnovou sítí. Po strukturní stránce je rozdělena do dvou nezávislých vrstev.

CSL (Cardano Settlement Layer) zajišťuje provoz platební sítě pro vlastní měnu *ADA*, jejíž fungování vychází z podobného systému transakcí, jako má Bitcoin. Konsensus v rámci blockchainu zajišťuje algoritmus *Ouroboros*[2]. Generování bloků probíhá v rámci dvacetisekundových časových slotů, které se sdružují do delších časových intervalů označovaných jako *epochy*. Každý slot má svého leadera, zvoleného v rámci předchozí epochy, a opravňuje ho k vytvoření právě jednoho bloku. Pokud leader svůj čas propásne (například je zrovna offline), slot propadá, žádný blok v rámci něj nevznikne a leader o svou pozici přichází, dokud není znovu zvolen. Po stránce soukromí síť nepřináší žádné zásadní změny oproti Bitcoinu.

Druhou vrstvou je *CCL* (Cardano Computation Layer), nad kterou běží smluvní účty aplikací. Existence vlastní vrstvy umožňuje připojovat pro potřeby aplikací nové řetězy bloků (tzv. *sidechainy*), což, jak autoři doufají, do budoucna umožní v rámci sítě provádět směnu s jinými kryptoměnami.

Kapitola 3

Analýza a návrh

Tato kapitola se zabývá analýzou vybraných služeb poskytujících mixování a praní špinavých peněz. Ze zjištěných závěrů následně navrhuje heuristiku, na jejímž základě by bylo možné v případě vybraných služeb zpětně určit přerušené vazby mezi penězi na vstupu a výstupu.

3.1 Vnější rozbor vybraných mixovacích služeb

Pro účely práce bylo ke zkoumání zvoleno šest ověřených, v současnosti používaných zástupců mixovacích serverů[1]. Na následujících řádcích budou popsány služby, které nabízejí, a poznatky získané při jejich použití.

3.1.1 Bitcoin Blender

Bitcoin Blender[2] je mixovací služba pro Bitcoin dostupná pouze přes síť Tor. Na běžném webu je pod totožným názvem možné najít reprezentativní stránku s instrukcemi, jak se ke službě připojit, a dále popisující obecné principy mixování, motivaci k používání těchto služeb a dokonce i doporučení alternativ (v současné době vesměs již nefunkčních). Současně však stránky zdůrazňují, že jsou pouze informativního charakteru a nejsou nijak napojeny na provozovatele reálné služby.

Stránka v síti Tor nabízí dvě varianty mixování, buď rychlou, nebo s registrací. Funkce je podobná, nicméně registrovaná varianta umožňuje mince nejprve do služby uložit a až poté, skrze účet, ovládat, kdy budou vybrány. Pro posílení anonymity je navíc možné peníze vložit v jednu chvíli až skrze 5 různých adres. Při uložení je naúčtován náhodný poplatek z rozmezí 1 až 3 % vkládané částky pro snížení dohledatelnosti. Výstupy je ze stejného důvodu možné rozeslat až mezi 10 různých adres. Pro rozesílání je možné nastavit interval, v rámci něhož se má pohybovat zpoždění výběru. Služba nabízí také věrnostní program a možnost doporučení služby známým. v případě, že uživatel spolu s ostatními, kterým službu doporučil, dohromady za posledních 7 dní vložil více než 5 BTC, získá odměnou 0,5 % z každé další uložené částky.

Pro rychlé míchání jsou možnosti poplatků, zpoždění a výstupních adres shodné, vstup je však možný pouze skrz jednu adresu a služba požaduje vklad minimálně 0,001 BTC po odečtení všech poplatků. Uživatel navíc dostane jednorázové ID, pomocí kterého může stav

[1] 9 Best Bitcoin Tumbler (Mixer) Services - Review 2018
https://cryptalker.com/best-bitcoin-tumbler/

[2] Bitcoin Blender (unofficial) https://bitblender.io/

mixování sledovat. Veškeré záznamy o aktivitách služba uchovává po dobu 10 dní a následně je maže.

3.1.2 Bitcoin Laundry

Bitcoin Laundry[3] taktéž poskytuje mixovací služby nad měnou Bitcoin, nabídka služeb je však jednodušší než u předchozího zástupce. Dostupná je jak přes web, tak přes síť Tor, a poskytuje pouze přímé míchání bez dlouhodobého uložení. Za použití je účtován fixní poplatek 1 % z uložené částky (v lednu 2019 v rámci propagační akce dočasně snížen na 0,1 %) plus 0,00008 BTC za každou výstupní adresu, kterých může být až 5. Pro každou je možné zvolit individuální zpoždění, s jakým budou peníze odeslány, ve fixních variantách 0, 1, 3, 7, 12 a 24 hodin, případně náhodně. Minimální mixovaná částka je stanovena na 0,0005 BTC, maximum se v čase mění podle aktuálních dispozic služby (v listopadu 2018 bylo 38 BTC, v lednu 2019 78 BTC). Pro každý požadavek je vygenerováno *session ID* umožňující sledovat průběh mixování. Veškeré záznamy jsou automaticky mazány po 7 dnech, případně okamžitě na vyžádání.

3.1.3 BestMixer.io

BestMixer.io[4] nabízí mixovací služby pro Bitcoin, Litecoin, Bitcoin Cash a do budoucna slibuje i podporu Etherea a BitcoinSV. Dostupný je přes web nebo síť Tor, poskytuje navíc také vlastní API. Poplatky jsou pro Bitcoin volitelné mezi 1 až 5 % plus až 0,00003390 BTC (voleno náhodně) za každou výstupní adresu, pro zbylé měny jsou hranice intervalu trojnásobné (3 až 15 %) a 0,00028703 LTC, resp. 0,00000290 BCH za každou výstupní adresu. Výstupních adres může být až deset a minimální mixovaná částka musí být 0,001 BTC, LTC nebo BCH. Maximální podporované zpoždění navracené částky je 72 hodin. Za každé mixování uživatel obdrží kód, který slouží jako věrnostní karta a podle prané částky na základě něj může v dalších mixech obdržet slevu z poplatku.

Služba navíc poskytuje tři varianty mixování používající odlišené zásoby peněz – Alpha, Beta a Gamma. Zatímco Alpha funguje na klasickém principu vyplácení peněz z prostředků uložených ostatními uživateli, Beta kromě nich přidává také obnos ze soukromých zdrojů provozovatele a jeho investorů, což údajně poskytuje rezervy pro praní větších částek. Gamma pak uživatelské peníze zcela obchází a slibuje, že veškeré výstupy budou s čistých, legálních zdrojů. Volba zásoby přímo koresponduje se zvolenou výší poplatků, pod 2 % je využita varianta Alpha, nad 4 % Gamma (pro LTC a BCH jsou tyto hranice posunuty na 6 % a 12 %).

3.1.4 PrivCoin

PrivCoin[5] je služba dostupná přes web, nebo Tor, případně vlastní API. v současnosti podporuje měny Bitcoin, Litecoin a Ethereum. Web nepůsobí příliš důvěryhodně, mnoho podstránek má problémy s načítáním grafiky a stylů a sekci pro Ethereum antivirus AVG označuje za podvodnou stránku z důvodu údajného phishingu. v podmínkách užití navíc zapovídají používání občanům Spojených států, zřejmě v reakci na tamní vyhlášku o regulaci mixovacích služeb[5]. Poplatky za službu se odvíjí od zvolené měny a jsou nastavitelné uživatelem. Pro Bitcoin je to 0,5 až 3,5 % plus 0,0005 BTC za každou výstupní adresu.

[3] Bitcoin Laundry https://bitcoin-laundry.com/
[4] BestMixer.io https://bestmixer.io/
[5] PrivCoin https://www.privcoin.io/

Minimální vložená částka je 0,005 BTC. v případě Litecoinu a Etherea jsou poplatky 2 až 5 % a 0,001 LTC/ETH za adresu při minimálním vkladu 0,01. Zpoždění je rovněž podporováno, uživatel je manuálně nastavuje z intervalu 0 až 24 hodin. Logy jsou mazány ihned po vykonání mixu.

3.1.5 Blender.io

Blender.io[6] je další z čistě bitcoinových mixovacích služeb dostupných přes běžný web i Tor. Poplatky jsou volitelné z intervalu 0,5 až 2,5 % s 0,0001 BTC za každou výstupní adresu, kterých může být až 8, přičemž minimální vložená částka je 0,001 BTC. Zpoždění je volitelné mezi 0 a 24 hodinami. Při použití služby uživatel obdrží kód, který při příštím mixování může použít, chce-li mít záruku, že neobdrží mince, které v minulosti sám vložil.

3.1.6 MixTum

MixTum[7] operuje na běžném webu i přes Tor a poskytuje opět mixování pouze pro Bitcoin. Od konkurence se odlišuje tím, že umožňuje „bezplatnou zkoušku“ a v případě zaslání přesně 0,001 BTC všechny poplatky uhradí protistrana. Výstup je však v takovém případě limitován pouze na jednu adresu, zatímco při běžném mixování je možné použít dvě. Zpoždění je voleno náhodně v intervalu od 0 do 6 hodin, poplatek je taktéž náhodně vybrán z rozmezí 4 až 5 % plus fixních 0,00015 BTC. Minimální vložená částka je již zmíněných zkušebních 0,001 BTC, maximum je z důvodu snížení možností analýzy stanoveno na 50 BTC. Logy jsou mazány automaticky po dokončení mixování.

3.1.7 Shrnutí poznatků

I přes rozdílnou prezentaci a dílčí detaily jednotlivých mixovacích služeb je možné pozorovat, že techniky, které využívají pro posílení anonymity, jsou de facto shodné a liší se pouze parametry. Jmenovitě se jedná o zapojení časové prodlevy mezi vstupem a výstupy bránící vyhledávání transakcí v blockchainu na základě shodného času a využití více výstupních adres rozmělňujících výstupní částku. Dále pak zavedení dvou vrstev poplatků -– odvodu určitého procenta svěřené částky službě, což provozovateli generuje zisk, a plateb za jednotlivé výstupní adresy, prohlašovaných obvykle za odměnu pro těžící uzly při potvrzení transakce Tyto postupy samy o sobě nezaručují přetrhání vazeb mezi vstupy a výstupy, vedou nicméně ke zvýšení míry nejednoznačnosti případných snah o jejich spárování.

3.2 Analýza fungování na úrovni blockchainu

Dosud se práce kapitola zabývala pouze zkoumáním mixovacích služeb tak, jak jsou prezentovány navenek. Pro návrh deanonymizačního algoritmu je však stejně důležité i chování interní, tedy z hlediska operací na úrovni blockchainu.

Během ledna 2019 byl proto v rámci průzkumu do všech šesti mixovacích služeb zaslán zkušební obnos za účelem vyhledání možných souvislostí mezi jejich vstupy a výstupy. Jak se ukázalo, ve všech případech se jednalo o variantu vyplácející z interní zásoby peněz (viz 2.3.2), jelikož vložené peníze byly dále odeslány až hodiny či dny po zpětném obdržení obnosu, v jednom případě dokonce nebyly utraceny vůbec. Pro analýzu řetězu transakcí

[6] Blender.io https://blender.io/
[7] MixTum https://mixtum.io/

v rámci blockchainu byl využit online prohlížeč adres a transakcí Blockchain.com[8] v kombinaci s clusteringovým portálem WalletExplorer[9].

Jak už bylo zmíněno, PrivCoin finance z poskytnuté vstupní adresy dosud nevyzvedl, přestože na ni bylo kromě zkušebního vkladu směřováno i 35 dalších transakcí. Nenachází se ani v žádném známém clusteru, čímž bylo možné spojení s výstupní platbou zcela přerušeno. Podobná situace nastala v případě služby MixTum, tentokrát byl však vklad první a jedinou transakcí zahrnující danou adresu. Vklad do Bitcoin Blenderu sice vybrán byl, avšak pouze formou přeposlání na další adresu, kde se opět hromadí nevybrané peníze[10].

Zajímavější situace nastala u Bitcoin Laundry. Nejen že vklad byl přeposlán dál, postupně cesta vedla až k několika adresovým clusterům a směnárně Bittrex.com. Na výstupní straně však žádné pojítko objeveno nebylo. Průlom přinesla až služba BestMixer.io a Blender.io. Ukázalo se, že adresy pro vklad spadaly do clusterů adres, v případě BestMixeru označeného 072d4eec44[11], u Blender.io pak 03b49dda3b[12] (identifikátory z databáze WalletExploreru). Adresy téhož clusteru byly současně objeveny také mezi výstupy transakce, která zaslala výstup mixování na uživatelovu adresu. Zjištěná závislost posloužila jako základ pro návrh heuristiky párující vstupy a výstupy těchto dvou mixovacích služeb.

3.3 Návrh prvotní heuristiky pro párování vstupů a výstupů mixovacích služeb

Heuristika pro BestMixer využívá zmíněného poznatku o vztahu mezi odchozími a příchozími penězi při využití mixovací služby. Předpokládá, že je-li vstupní adresa součástí clusteru, měla by jedna nebo více adres tohoto clusteru figurovat také mezi výstupy transakce odesílající vyprané peníze zákazníkovi. Stačí tedy vyhledat transakci obsahující clusterové výstupy a současně výstup na adresu mimo cluster takový, že částka tohoto výstupu odpovídá částce zaslané na počátku do služby snížené o případné poplatky. Současně výstupní transakce musí být od vstupní časově vzdálená nanejvýš na maximální dobu prodlevy poskytovanou službou.

Bodově by se dal postup popsat následovně:

- Určit cluster C, do něhož spadá adresa pro zaslání peněz.
- Procházet transakce v blocích počínaje časem vstupní transakce t, dokud jejich čas nepřekoná $t + d_{max}$, kde d_{max} představuje maximální dobu zpoždění (72 hodin).
- Pro každou transakci proběhne kontrola, zda splňuje následující podmínky:
  - Obsahuje na výstupu jednu nebo více adres z daného clusteru.
  - Obsahuje na výstupu jednu nebo více adres mimo cluster.
  - Částka směřovaná na některou z neclusterových adres je rovna $n_x - fee$, kde n_x je vstupní částka a fee spadá to intervalu mezi nejvyšším a nejnižším poplatkem služby.

[8] Prohlížeč blockchainu https://www.blockchain.com/

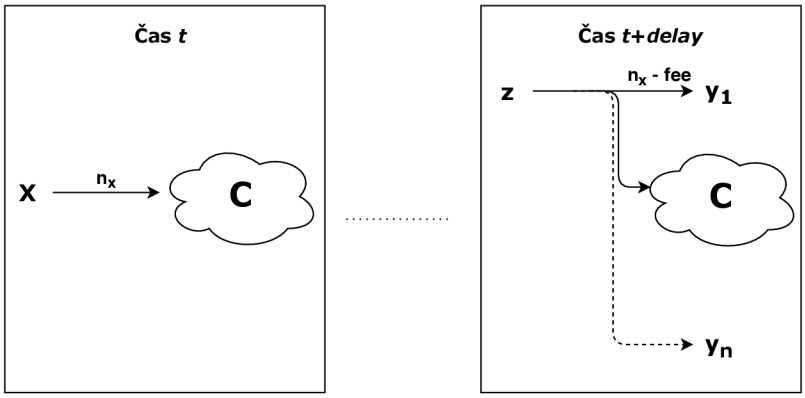
[9] Wallet Explorer https://www.walletexplorer.com/

[10] https://www.blockchain.com/btc/tx/3b039d67b5703abf4ce49cf102550fdb431d34d4ef1a904fa1c3bc9088ed50d5

[11] https://www.walletexplorer.com/wallet/072d4eec44012d68?from_address=3KuhVxYpcCEoZezNPndTPxqnoDdsPiiM3Z

[12] https://www.walletexplorer.com/wallet/03b49dda3b289973?from_address=3BwAei7PGo8MxsfbDtVVu2kFWtpZuaZr3n

- Jestliže jsou podmínky splněny, adresa odpovídajícího výstupu je přidána do množiny možných řešení.



Obrázek 3.1: Grafické znázornění inkriminovaných transakcí

S drobnými úpravami je možné provést hledání související adresy také opačným způsobem, kdy známe výstup a chceme najít vstupní adresu:

- Určit cluster C, do něhož spadají ostatní výstupní adresy koncové transakce
- Procházet transakce v blocích nazpět počínaje časem výstupní transakce t, dokud jejich čas neklesne pod $t - d_{max}$, kde d_{max} představuje maximální dobu zpoždění (72 hodin).
- Pro každou transakci proběhne kontrola, zda splňuje následující podmínky:
  - Obsahuje na výstupu právě jednu adresu z daného clusteru a případně druhou, která do clusteru nespadá.
  - Žádná z adres na vstupu nespadá do daného clusteru.
  - Součet částek ze vstupů je po částky pro výstupní neclusterovou adresu roven $n_y + fee$, kde n_y je částka po mixování a fee spadá to intervalu mezi nejvyšším a nejnižším poplatkem služby.
- Jestliže jsou podmínky splněny, množina adres odpovídajícího vstupu je přidána do možných řešení.

3.4 Podrobnější zkoumání vlastností vybraných služeb a zpřesnění heuristiky

Po prvotních zjištěních z ledna 2019 byly v průběhu následujících čtyř měsíců (tedy od února do května 2019) do služby BestMixer.io, která se jevila jako potenciálně demixovatelná, zasílány další obnosy s rozličnými parametry ve snaze odhalit zákonitosti, které by mohly vést ke zpřesnění prvního návrhu heuristiky.

Ukázalo se, že je v některých záznamech možné vysledovat pevnou strukturu, která usnadní zužování množiny potenciálních výsledků. Cluster adres figurující v transakcích vždy obsahuje větší množství vstupních transakcí (tedy takových, kdy jsou peníze ukládány na adresy clusteru). Naproti tomu výstupní transakce (odchod peněz z clusteru) je

přítomna vždy jen jedna a představuje úplně poslední manipulaci s clusterem, v rámci níž jsou veškeré finanční prostředky odvedeny pryč. Clustery tak mají omezenou životnost, konkrétně v řádu dní, a není proto možné na základě získaných údajů transakce interagující s mixovací službou identifikovat dlouhodobě.

Prostředky se do clusteru dostávají dvěma způsoby. Prvním jsou vklady uživatelů. Tyto transakce mohou vypadat takřka jakkoli. Není omezen počet vstupů ani výstupů, a jediným pravidlem tak je, že se mezi výstupy objevuje adresa z clusteru, na niž vklad směřuje. Druhým typem vstupních transakcí jsou paradoxně zpětná vyplácení částek uživatelům. Zde je struktura fixní. Vstup je právě jeden, pocházející z adresy mimo cluster (jak již bylo zmíněno v podkapitole 3.1.7, peníze se vyplácí z interní zásoby). Výstupy jsou přítomny dva – prvním je adresa patřící vyplácenému uživateli (nespadá tedy do clustery a směřuje na ni výsledná přepraná částka), druhý pak slouží jako návratová adresa pro drobné a vede do zkoumaného clusteru. Dalším prvkem, jež je třeba zohlednit, jsou možnosti rozdělení výstupu mezi více adres (10 pro BestMixer.io), navíc s časovými rozestupy. Tento typ transakcí je z hlediska clusteru realizován pro dílčí adresy realizován stejně jako v případě jednoduchého výstupu. Každá cílová adresa má vlastní transakci držící se formátu 1 vstup a 2 výstupy (výplata uživateli a odvod zbytku do clusteru).

Zvláštní případ vstupů představuje mixování za pomoci kódu pro prevenci obdržení vlastních peněz při více paralelních použitích mixéru. v takové situaci uživatel jako cílovou adresu pro zaslání prostředků nedostává adresu z clusteru, nýbrž jednorázovou adresu, z níž jsou finance rozeslány dále.

Nutno je zmínit také vlastnost specifickou pro BestMixer.io, a to dělení mixování do tří kategorií zmíněných v 3.1.3. Alpha (tedy míchání čistě s penězi od uživatelů) i Beta (směs uživatelských financí s čistými prostředky pocházejícími z jiných zdrojů zajištěných službou) se chovají způsobem popsaným v dosavadním textu. Je možné, že v případě Bety budou mezi vstupy clusteru přítomny i transakce nepocházející od uživatelů, avšak tuto domněnku není jak jednoznačně prokázat. Varianta Gama slibuje výplatu kompletně ze zdrojů služby, a tedy z peněz neposkvrněných uživateli. Slib, zdá se, plní a vstupní cluster je odlišný od toho, který se objevuje ve výstupních transakcích. Z tohoto důvodu nebyla mezi vstupy a výstupy objevena žádná vazba a kategorie bude v řešení vynechána.

Další pokusy naznačují, že veškeré poznatky ohledně BestMixer.io získané při použití Bitcoinu by měly být platné i v případě míchání měny Litecoin.

Po zapracování nových zjištění by heuristika vypadala následovně:

- Určit cluster C, do něhož spadá adresa pro zaslání peněz.
- Procházet transakce clusteru C, jejichž čas t_2 je vyšší než čas vstupní transakcet_1, dokud jejich čas nepřekoná $t + d_{max}$, kde d_{max} představuje maximální dobu zpoždění (72 hodin).
- Pro každou transakci proběhne kontrola, zda splňuje následující podmínky:
  - Obsahuje právě 1 vstupní a 2 výstupní adresy.
  - Druhá výstupní adresa spadá do clusteru C.
- Jestliže jsou podmínky splněny, přidá se do seznamu potenciálních
- Pro N od 1 do $addr_{max}$, kde $addr_{max}$ je nejvyšší počet možných výstupních adres:
  - Zkoušet kombinace pro N prvků ze seznamu potenciálních.

  - Pokud součet jejich prvních výstupních adres je v rozmezí $n_x - fee$, kde n_x je vstupní částka a fee spadá to intervalu mezi nejvyšším a nejnižším poplatkem služby, přidá se kombinace do seznamu možných řešení.

Naopak pro určení vstupní adresy na základě výstupní by se použil následující postup:

- Určit cluster C, do něhož spadá adresa pro drobné ve výstupní transakci.
- Procházet transakce clusteru C, jejichž čas t_2 je menší než čas vstupní transakcet_1, počínaje časem $t - d_{max}$, kde d_{max} představuje maximální dobu zpoždění (72 hodin).
- Pro každou transakci určit adresu vedoucí do clusteru.
- Jestliže je hodnota výstupní adresy transakce vedoucí do clusteru v rozmezí $n_x + fee$, kde n_x je částka ve výstupní transakci a fee spadá to intervalu mezi nejvyšším a nejnižším poplatkem služby, přidá se transakce do seznamu možných řešení.

Kapitola 4

Programová realizace navrženého řešení

Aby bylo možné ověřit funkčnost heuristik navržených v předchozí kapitole a současně je také využívat v praxi v rámci projektu Tarzan, byla vytvořena webová aplikace s pracovním názvem Coin Demixer, která navržené řešení implementuje. Případy užití aplikace je možné rozdělit na tři základní situace vztahující se k párování transakcí. Uživatel musí mít možnost na základě znalosti vstupní transakce vyhledat transakci výstupní a s ní také konkrétní z výstupních adres, jež reprezentují vyplácení mixovaných obnosů. Analogicky by mělo být možné i stanovit na základě zadané výstupní transakce stanovit, jaký byl vstup a jaké mohly být další potenciální výstupy. v obou případech je nutné zajistit, aby aplikace dokázala v rámci transakce správně rozpoznat adresu clusteru, podle které bude párování probíhat. Třetí variantou je, že uživatel zná i některé doplňující parametry mixování, např. další zúčastněné transakce, počet výstupních adres, poplatky nebo časový rozptyl, a chce je využít pro zpřesnění výsledku.

Pro implementaci byl zvolen otevřený PHP framework Laravel[1], jehož cílem je zjednodušovat vývoj webových aplikací. Kromě interní správy cest a validátorů poskytuje také řadu knihoven. Podporu při tvorbě vizuální stránky aplikace přináší vestavěný šablonový systém Blade doplňovaný rozsáhlou knihovnou kaskádových stylů frameworku Bootstrap. Mimoto jsou za pomoci Laravel vytvořeny i některé další aplikace projektu Tarzan, což usnadní eventuální integraci Demixeru do daného ekosystému.

Další z jeho výhod je úzká spjatost s architekturou MVC (neboli Model-View-Controller), kolem níž je koncipován. Hlavní myšlenkou je rozdělení projektů na tři oddělené části (nazývané právě trojicí slov z názvu architektury) na základě jejich zodpovědností. Přínosem tohoto přístupu je, že komponenty v ideálním případě zcela izoluje a v případě zásahu do jedné části tak není nutné měnit všechny. Segment označovaný jako *model* zodpovídá za reprezentaci datového modelu a zprostředkovává přístup k datům, nejčastěji z databáze, s níž je provázán. *View* („pohled“) má na starost vizuální prezentaci dat z modelu a zajišťuje obousměrnou komunikaci s uživatelem. *Controller* („řadič“) pak představuje jistou formu mezivrstvy, vykonávající aplikační logiku nad daty z modelu na základě požadavků a potřeb pohledu.

V případě frameworku Laravel je view tvořen sadou stránek, které se uživateli vykreslují v prohlížeči, a logikou na straně serveru, jež je generuje. Odesílání požadavků je řešeno formou HTTP dotazů směřovaných na konkrétní podadresy serveru. Ty jsou skrze tzv.

[1] https://laravel.com/

cesty (anglicky *routes*) interně mapovány na volání metod řadiče, které vykonají příslušnou obsluhu a jejich výstupem je nakonec opět pokyn k zobrazení konkrétního textu nebo HTML stránky. Modelové části bývají tradičně svázány s již zmíněnou databází. v případě této aplikace však budou data získávána externě, a to hned z několika zdrojů.

4.1 Architektura aplikace

Jelikož mixovacích služeb existuje celá řada a stále vznikají nové, je vhodné, aby se aplikace dala do budoucna snadno rozšiřovat. Stejně tak může být nestálá povaha externích služeb, které aplikace využívá. Z tohoto důvodu je implementace řešena zcela modulárně. O propojení modulů se stará centrální řadící třída `DemixerController`, která vybírá vhodné mutace klientů a předává je s využitím polymorfismu demixovací logice.

Moduly aplikace by se daly rozřadit do tří kategorií. `BlockchainClient` je podpůrná třída spadající do modelové části aplikace. Má za úkol zprostředkovávat informace z blockchainu, primárně data o transakcích. v současné implementaci má jediného zástupce, který čerpá data z kryptoměnových klientů provozovaných v rámci projektu Tarzan na serveru *Bexp*.

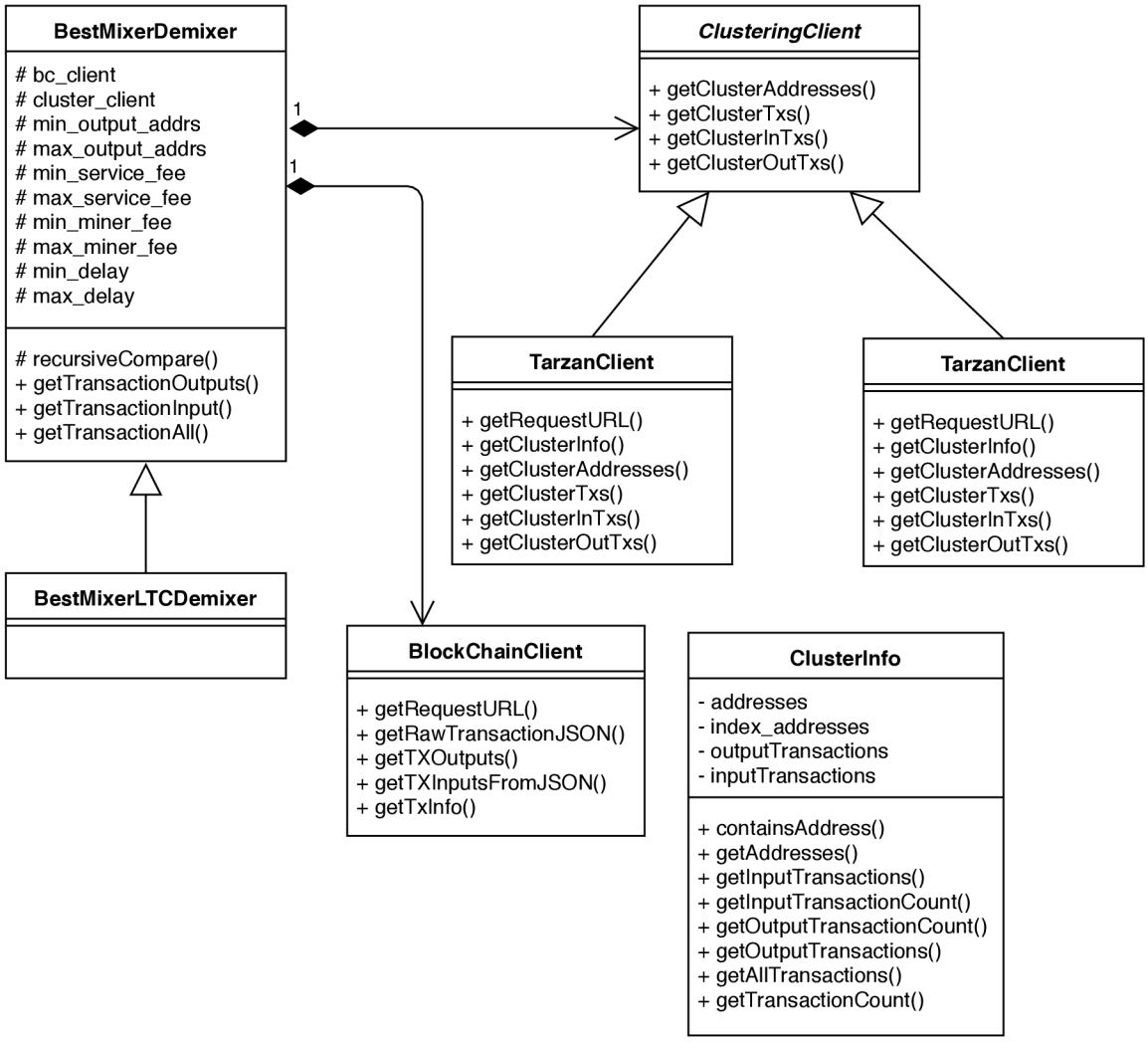
`ClusteringClient` je abstraktní třída zastřešující další klíčový segment modelové části, a to data o clusterech. Původně je měl poskytovat server WalletExplorer[2]. Komunikace s ním probíhá formou standardních HTTP dotazů GET s parametrem `?q=adresa_z_clusteru`. Odpovědi zasílá jako plnohodnotně formátované HTML s limitem 100 položek na stránku, v rámci třídy `WalletExplorerClient` je tedy třeba informace získávat zřetězením dotazů a následnou extrakcí dat skrze regulární výrazy. v průběhu vývoje se však ukázalo, že rychlost serveru je značně proměnlivá a v některých obdobích tak dochází k rapidnímu nárůstu dob odezvy, nezřídka ústícímu až ve vypršení platnosti požadavků. Kromě toho při nadměrném počtu dotazů odmítá spojení s kódem 403. To znemožňuje komunikaci v případech, kdy cluster obsahuje transakce, jejichž počet se pohybuje v řádech nad tisíc a je nutné projít velký počet stránek. Druhým nedostatkem je, že služba podporuje pouze síť Bitcoin, neumožňuje tedy otestovat heuristiku pro Litecoiny, pro něž by také měla být funkční. I proto byl jako alternativa přidán modul `TarzanClient`, komunikující s interním clusteringovým serverem projektu Tarzan. Požadavky jsou zasílány skrze parametry HTTP požadavku GET, odpovědí přicházejí ve formátu JSON.

Poslední skupinu modulů tvoří potomci třídy `Demixer`, obstarávající v rámci řadičové části párování vstupních a výstupních transakcí pro konkrétní mixovací služby. v rámci práce byly vytvořeny varianty `BestMixerBtcClient` a `BestMixerLtcClient`, lišící se výchozími parametry mixování.

4.2 Posloupnost činnosti

Následující řádky popisují funkční posloupnost činnosti aplikace od uživatelského vstupu až po výpis výsledků. Po otevření úvodní stránky je ihned načteno rozhraní pro základní vyhledávání, tedy takové, které využívá výchozí parametry mixérů. Realizováno je za pomoci pohledu `basic_search`. Formulář na stránce nabízí pouze možnost zadání identifikátoru transakce, podle níž budou vyhledávány odpovídající vstupy, resp. výstupy. Dále je zde přítomna volba, jestli mají být vyhledány transakce výstupní (a tedy je zadána vstupní transakce), nebo i vstupní (a tudíž je zadána výstupní transakce), o jakou se jedná měnu

[2] https://www.walletexplorer.com/



Obrázek 4.1: Diagram tříd aplikace

(Bitcoin, nebo Litecoin) a jaká služba bude využita pro získávání informací o clusterech (WalletExplorer, nebo interní server projektu). v případě přepnutí na pokročilé vyhledávání přes hlavní panel aplikace (pohled `advanced_search` je formulář rozšířen o nastavení parametrů mixování, konkrétně minimální a maximální hodnoty poplatku za služby (v procentech vstupní částky), minimální a maximální poplatek za jednotlivé výstupní adresu a dolní a horní hranici zpoždění mezi vstupem a výstupy. Odebrána byla naopak volba, jestli zadaný identifikátor přísluší vstupní, nebo výstupní transakci. Nahrazena byla samostatnými poli pro vstupní a výstupní adresy, přičemž počet polí je proměnlivý podle zvoleného počtu výstupních adres – dalšího z nových volitelných parametrů.

Po odeslání jsou v případě obou formulářů data metodou POST přepravena na podadresu `/search_request`, čímž jsou vnitřní cestou předána metodě `findMatchingTransactions` řadiče `DemixerController`, kde proběhne jejich zpracování. Na základě zvolených parametrů je vytvořena instance příslušného klienta pro získávání informací z clusteringového serveru, jejichž zaměnitelnost zajišťuje odvozenost od abstraktní třídy `ClusteringClient`. Současně, byť v této fázi neparametrizovaný, je vytvořen také klient pro extrakci dat o transakcích z blockchainu. Od uživatelské volby se odvíjí i jaký je vytvořen objekt pro

demixování zadaných transakcí. Ve všech variantách v konstruktoru přijímá dva výše zmíněné klienty, aby je mohl využívat bez znalosti konkrétních implementací. Následně už se chod programu větví na základě typu zadané transakce, tedy na vyhledávání podle vstupní (parametr `in`), výstupní (`in`), nebo kombinace (parametr `all`) předaný skrytým polem z formuláře pro pokročilé vyhledávání).

Hledání výstupních adres na základě vstupu implementuje v rámci demixerů metoda `getTransactionOutputs`. Jelikož se jedná o vstupní transakci, je nutné určit, která (a zda vůbec nějaká) z jejích výstupních adres přísluší vhodnému typu clusteru, a případně reagovat chybou. Zde přichází na řadu zjištění z analytické kapitoly 3, že se inkriminované služby vyznačují mnoha vstupními a jednou až dvěma výstupními transakcemi. Data o určeném clusteru jsou poté hromadně načtena jako objekt třídy `ClusterInfo` do lokální proměnné, aby se minimalizovaly zdlouhavé dotazy na server. Následně, opět ve snaze urychlit proces, jsou postupně načítány vstupní transakce clusteru a po prvotním profiltrování vznikne lokální seznam potenciálních výstupů. Kritérii jsou formát (1 vstup a 2 výstupy, kde druhý vstup směřuje do clusteru), vyplácený obnos menší nebo roven vstupnímu a čas pohybující se v mezích zvolených zpoždění. Přestože si tato část klade za cíl urychlit průběh následného párování, představuje současně úzké hrdlo programu. Na vině je klient pro komunikaci s blockchainem, od něhož musí být vyptány veškeré transakce. Vyřízení jednoho dotazu dle hodnot naměřených v rámci programu trvá v průměru 90 milisekund, v případě stovek transakcí tak může způsobit zdržení i řádech desítek sekund. Nad získaným seznamem je v cyklu volána rekurzivní párovací metoda nazvaná `recursiveCompare`, představující jádro demixeru.

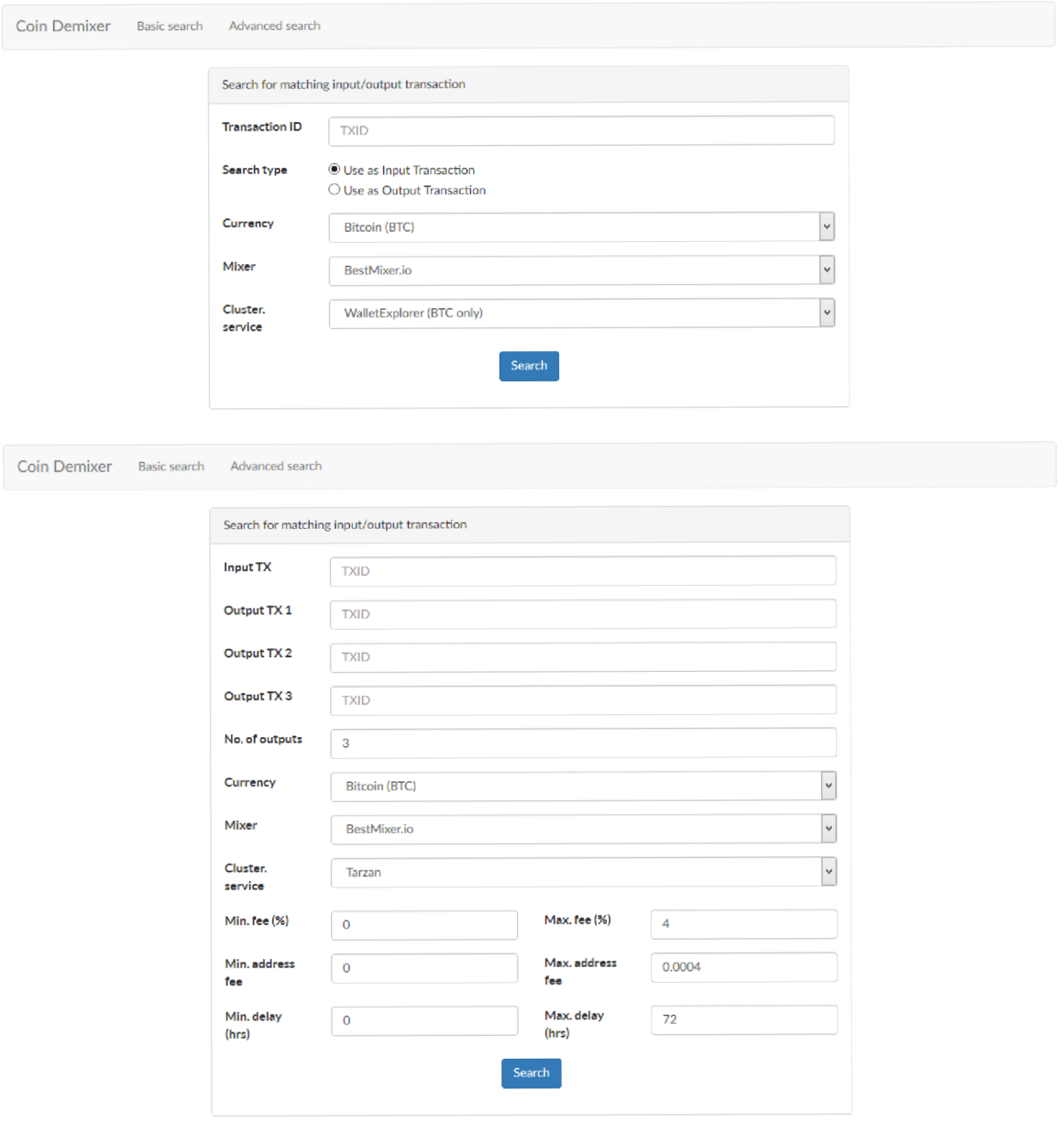
Její činnost je realizována jako průchod seznamem potenciálních transakcí, přičemž pro každou zkoumá, zdali její výstup spadá pod maximální výši stanovenou poplatky. Jestliže ano, je zavolána další úroveň průchodu, přičemž prohledávaný seznam je zúžen o již porovnané transakce z předchozích úrovní a částka srovnávaná s limitem je součtem všech v konkrétní posloupnosti. Pokud i na maximální úrovni – odpovídající počtu hledaných výstupních transakcí – součet spadá do intervalu udaného dolním i horním limitem poplatků, je posloupnost vyhodnocena jako možné řešení a postupným vynořováním a slučováním metoda vygeneruje pole s danou sadu transakcí představující jedno řešení. Celá činnost je postupně provedena několikrát pro zvětšující se maximální hloubku určenou nejvyšším povoleným počtem výstupních adres.

Vyhledávání vstupní transakce na základě výstupní je jednodušší proces, jelikož není třeba porovnávat transakce rekurzivně. Metoda `getTransactionInput`. Opět jsou získána data o zadané transakci a poslán dotaz na data z clusteru. Vzhledem k pevné struktuře výstupních transakcí však může být rovnou vybrána druhá adresa z výstupu bez předchozího určování. Stejně tak je snazší odhalit, pokud transakce ve skutečností není výstup clusteru, jelikož musí splňovat formát 1 vstup, 2 výstupy zmíněný výše. Z důvodů obecného řešení, které bude využito dále, však metoda podporuje párování i na základě více než jedné výstupní adresy. Proto je třeba u zbylých identifikátorů ověřit, zdali skutečně všechny patří platným transakcím ze stejného clusteru. Na základě zjištěných informací je následně vytvořen jeden souhrnný záznam transakcí, nesoucí nejranější a nejpozdější čas odeslání transakce, součet výstupních částek a počet zapojených transakcí. Záznam je poté postupně srovnáván se všemi transakcemi clusteru (skrz cenu ohraničenou poplatky, časové meze a identifikátor pro prevenci srovnávání s již známými výstupními transakcemi) a shody ukládány do seznamu řešení.

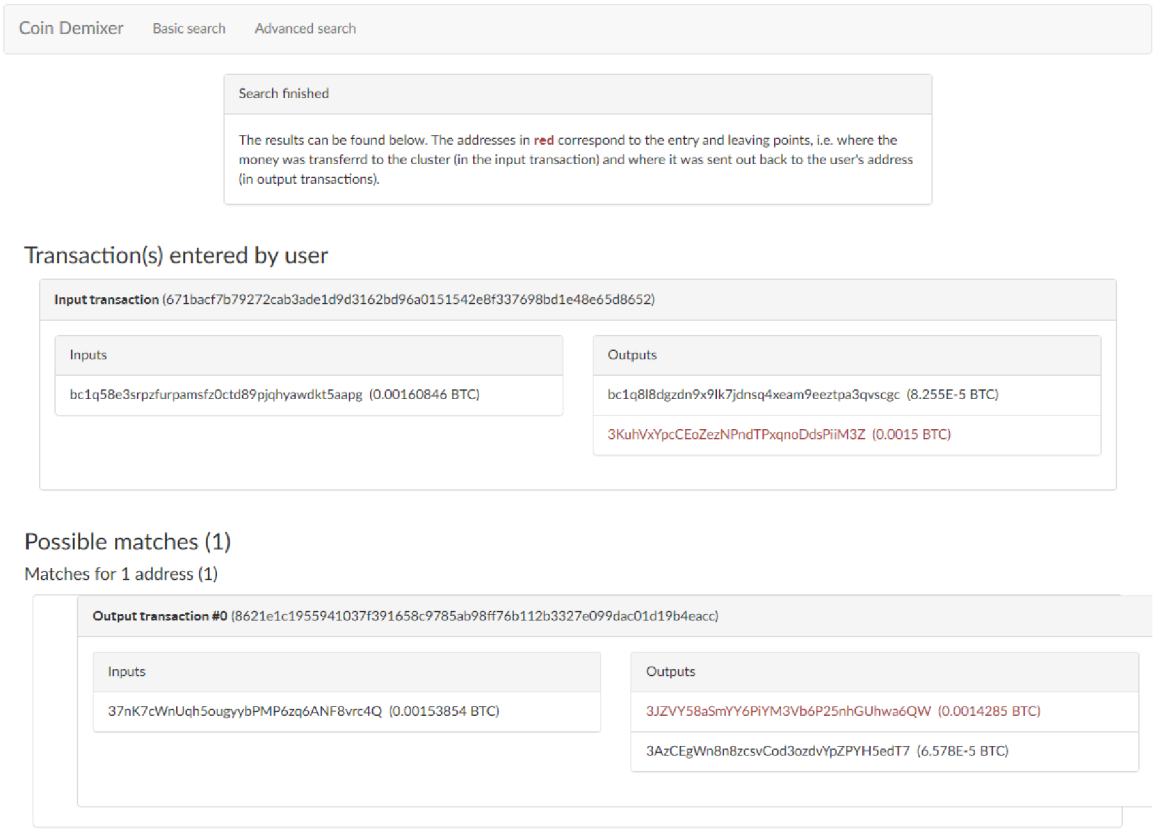
Nejsložitější úkol plní metoda `getTransactionAll`, vyhledávající na základě nepovinně zadaných vstupní a výstupních transakcí všechny zbylé. S ohledem na fakt, že zvláštní pří-

pady hledání výstupů podle vstupu a naopak vstupu podle výstupu jsou již řešeny v předchozích funkcích, je v těchto situacích párování přenecháno jim. v případě kombinovaného hledání vstupů a výstupů je postup směsí dříve zmíněných. Seznamy transakcí jsou tentokrát vytvořeny dva, pro vstupy a výstupy. Vstupy jsou finančně omezeny jen zdola kvůli neznámým obnosům výstupů, časové limity stanoveny podle známých transakcí. Výstupní seznam má podmínky podobné, navíc k nim přibývá tradiční kontrola formátu. Jádro znovu představuje `recursiveCompare`, krom vnitřní smyčky procházející jednotlivé hloubky (nyní zdola omezené počtem známých adres) nově celý algoritmus iteruje nad seznamem potenciálních vstupů.

Výstupem všech tří metod je struktura se třemi poli – zadané vstupní transakce, zadané výstupní transakce a seznam možných řešení řešení, který se obsahem liší podle typu hledání. O vizualizaci se stará pohled `search_results`. Stránka s výsledky je rozdělena do dvou sekcí. v horní části jsou zobrazeny transakce zadané uživatelem včetně adres a částek svých vstupů a výstupů. v dolní části jsou pak bloky s vyobrazením jednotlivých řešení. Veškeré transakce spadající do jednoho řešení jsou umístěny ve společném panelu, dále jsou pak textově odděleny množiny řešení pro jednotlivé počty výstupních adres. Mezi výstupy každé transakce je možné najít adresy vyznačené červenou barvou. Toto značení obecně vyznačuje adresy interakce s mixovací službou, význam se ale mírně liší podle typu transakce. v případě, že se jedná o transakci vstupní, symbolizuje zvýraznění adresu clusteru, na niž byly peníze uloženy (a v závorce konkrétní obnos). v případě výstupní transakce je vyznačena adresa, na kterou byly zaslány vyprané peníze, tedy adresa zákazníka, opět včetně konkrétní částky.



Obrázek 4.2: Náhled rozhraní obou verzí stránky vyhledávání – základního (nahoře) a pokročilého (dole).



Obrázek 4.3: Ukázka stránky s výpisem výsledků.

Kapitola 5

Validace řešení

Ústředním bodem práce bylo dosud zanalyzování vybraných mixovacích služeb spolu s technikami, které používají pro anonymizaci, a vyvození závěrů, jak by proti nim bylo možné bojovat. Byly navrženy heuristiky, na jejichž základě vznikla implementace řešení v podobě webové aplikace. Tvorba heuristik však není exaktní disciplína, vyvíjí a ladí se empiricky, z dostupných informací a experimentů, jak ostatně dokazuje postupná proměna návrhu v kapitole 3. Z toho důvodu je nutné jakákoliv řešení otestovat, než mohou být prohlášena za platná, a právě tomu se bude věnovat tato kapitola.

Testování bude rozděleno do dvou hlavních oddílů, věnujících se jednotlivým variantám podporovaných služeb, tedy BestMixer.io pro Bitcoin, BestMixer.io pro Litecoin. v rámci nich poté bude zkoumána úspěšnost deanonymizace na sadě transakcí získaných při zkoumání služeb.

5.1 BestMixer.io pro Bitcoin

BestMixer.io nabízí několik režimů mixování a volitelně také velké množství výstupních adres. Testovací případy se tedy pokusí pokrýt alespoň takové kombinace, které byly v rámci testovací sady dostupné. Pokud nebude uvedeno jinak, probíhalo vyhledávání v plném rozsahu parametrů, tedy poplatek 1 až 4 % a prodleva do 72 hodin. Dobovou horní mez poplatku za jednu výstupní adresu představuje 0,00005 BTC, současnou pak 0,0004 BTC.

Test a – Míchání s 1 výstupem, zásoba Alpha

Vstupní transakce:	671bacf7b79272cab3ade1d9d3162bd96a0151542e8f337698bd1e48e65d8652		
Vstupní adresa:	3KuhVxYpcCEoZezNPndTPxqnoDdsPiiM3Z		
Výstupní transakce:	8621e1c1955941037f391658c9785ab98ff76b112b3327e099dac01d19b4eacc		
Výstupní adresa:	3JZVY58aSmYY6PiYM3Vb6P25nhGUhwa6QW		
Poplatek: 1 %		**Zpoždění:**	2 h 40 min
Vložená částka:	0,0015 BTC	**Čas:**	8.1.2019 16:07:54

První pár transakcí pochází z počátečních experimentů v lednu 2019. Jednalo se o přímočaré mixování s jednou výstupní adresou, minimálním poplatkem 1 % a výchozím zpožděním 2 hodiny a 40 minut. v použitém clusteru se v době vypršení jeho platnosti nacházelo 57 transakcí, z toho jedna výstupní. Z časového hlediska spadá známá vstupní transakce zhruba do třetiny životnosti clusteru, číslo se tedy při hledání výstupů dále zredukuje.

V případě vyhledávání transakce na základě známého vstupu byl výsledek správný, tedy právě jedna výstupní transakce odpovídající předpokládanému výstupu. Pokus byl

opakován jak pro dobový poplatek 0,00005 BTC za adresu, tak současných 0,0004 BTC, průběh byl bez rozdílu.

Druhá zkoumaná situace byla vyhledávání vstupní transakce na základě výstupu. Zde se nabízí několik variant předpokládaných znalostí. Známe-li přesný počet výstupů, v tomto případě jeden, můžeme vstup vyhledávat přímo. Při dobovém poplatku byl proces opět úspěšný a aplikace nalezla právě jednu očekávanou adresu. Při zvýšení na současný poplatek už však možné výsledky byly dva, byť jeden z nich stále byl onen správný. Nepomohla ani redukce procentuálního poplatku na horní mez pro zásobárnu Alpha, tedy 2 %.

Je nicméně třeba předpokládat i situace, kdy uživatel zná pouze jednu výstupní transakci, avšak neví, zda není jen jedna z mnoha. Pro hledání vstupní adresy pro 1 až N výstupních adres při znalosti jedné bylo z důvodu velkého množství potenciálních výsledků postupováno postupně. Už při dvou vzrostl počet možných vstupů 6 transakcí, přičemž 5 nesprávných předpokládalo jednu další výstupní transakci. Při použití současné výše poplatku počet nalezených řešení rapidně vzrostl. Nalezeno bylo 21 možných vstupů a 33 různých kombinací transakcí. Redukce horní hranice poplatku na 2 % dopad měla, avšak nevalný – výsledkem bylo 19 vstupních adres a 30 kombinací. Stropu růst dosáhl při 5 výstupních adresách, kdy možné vstupy dosáhly počtu 24 při 160 kombinacích. Vyšší adresní poplatek pak kombinace navýšil na 167.

Test B – Míchání se 2 výstupy, zásoba Alpha

Vstupní transakce:	c5b452b31c2534fccb331c1837ed200b0b36437052ea5230c3d02ea6c56655e2		
Vstupní adresa:	13a3hJNN9HzqrC6B5caTxoaB5UGwA8w5kA		
Výstupní transakce:	d3bf0904cadd9416c1167e8ff80e7ff88019429200635 05e7ef71f96d36b6d7e b9c183785845c59dcce05cd3d629256ae5b91482e6ca90275961fdebc45b778e		
Výstupní adresy:	3KGVsRKZKD7aj5Qr9uyqcVHE3mNFFDTqau 3CKf9CMPShkrEY9YXgZ4mv6Dmhv8a2rb3j		
Poplatek: 1 %		**Zpoždění:**	2 h 40 min / 4 h 40 min
Vložená částka:	0,002 BTC	**Čas:**	28.2.2019 21:52

V druhém testu byly transakce hned tři, jelikož se jednalo o mix se dvěma výstupními adresami. Proběhl na přelomu února a března, opět s poplatkem 1 %. Zpoždění byla výchozí 2 hodiny a 40 minut pro první, 4 hodiny a 40 minut pro druhou adresu. Cluster tentokrát obsahovat 130 transakcí, z toho 128 vstupních, z toho transakce se vkladem časově připadalo zhruba do čtvrtiny, obtížnost tedy byla potenciálně vyšší.

Stejně jako u předchozího testu bylo prvním krokem pokusit se vyhledat na základě vstupní transakce výstupy. Výsledkem byl v případě dobového adresního poplatku (0,00005 BTC) úspěch. Nalezeno bylo jedno řešení obsahující obě výstupní adresy. Přechodem na současný poplatek (0,0004 BTC) se však řešení rozmělnila na tři možnosti, byť všechna tvořena dvěma adresami. Omezení procentního rozsahu na Alphu bylo bez účinku.

V opačném směru, jak se ukázalo, hraje velkou roli míra známých informací. Dvě výstupní adresy při testování nabízejí řadu kombinací, jež je třeba pokrýt. Nejjednodušší z nich je hledání vstupu na základě dvou známých adres. v případě dobové ceny výsledek nebyl zcela jednoznačný, jelikož byly nalezeny dvě transakce s podobnou vstupní hodnotou. Po navýšení limitu adresního poplatku na aktuální variantu bylo vzhledem ke vzniklému rozptylu řešení nalezeno 5, a to i po zredukování procentního rozsahu. Naproti tomu hledání chybějící výstupní transakce na základě kombinace vstupní a jedné výstupní při dobovém stropu poplatků vyústilo v právě jedno správné řešení. Současný strop vedl v řešení dvě.

Alternativní situaci představuje znalost pouze jedné adresy a hledání vstupu a druhého výstupu. v případě menšího adresního poplatku bylo pro první výstup nalezeno 9 vstupů

a celkem 20 možných kombinací s výstupními transakcemi. Redukce procentuálního rozsahu tentokrát pomohla a přinesla 13 kombinací pro 6 vstupů. Rapidní nárůst způsobil přechod na současný adresní poplatek. Výsledkem bylo 64 kombinací při 25 možných vstupech, po úpravě na Alpha rozsah klesly kombinace na 62. v případě druhé výstupní transakce byly hodnoty obdobné. V obecném testu, kdy byl vyhledáván vstup pro 1 až N výstupů se znalostí jediné vstupní adresy, pro dobový poplatek počet řešení začal být konstantní od 3 výstupních adres při 39 řešeních a 8 možných vstupech, po redukci 29 a 5. Současný strop adresního poplatku vedl k tomu, že růst začal stagnovat až na 4 adresách, přičemž dosáhl 25 vstupních adres a 109 možných kombinací, po redukci snížených na 102.

Test C – Míchání s 1 výstupem, zásoba Beta

Vstupní transakce:	29a484238d2d642702b1c559f4b613c011fe67444ea2131b95510d0848ab7585		
Vstupní adresa:	36YNn7G23RFYZMHBLfNHjevWiAQs4nrhs9		
Výstupní transakce:	7b0843e05c6f0e315808ed010b5bd6a9fd7252b45ed10564eca52d512e14b92e		
Výstupní adresa:	3AEJxHHT1iuVkDNbBrcxFRHwiVDjpVzkti		
Poplatek: 2 %		**Zpoždění:**	2 h 0 min
Vložená částka:	0,0015 BTC	**Čas:**	27.1.2019 20:12

Pro třetí test byla zvolena transakce operující se zásobárnou Beta, testovaná v lednu s jediným výstupem, minimálním 2% poplatkem a dvouhodinovým zpožděním. Cluster obsahoval 158 transakcí, z toho 1 výstupní.

Komplikace se vyskytly již při základním párování vstupní adresy na jeden výstup. Při dobovém stropu (0,00005 BTC) byla výsledkem správná transakce, při současném (0,0004 BTC) však už byly určeny dvě. Při otevřeném hledání jednoho až deseti výstupů s dobovým poplatkem pak došlo k nalezení hned 7 výstupních variant (po upravení dolního stropu procentuálních poplatků na 2 % odpovídající Betě zredukováno na 6). Při využití současné hodnoty adresního poplatkového stropu se počet vyšplhal na 25 (po redukci 24).

V opačném směru byla bilance lepší. Při fixní jedné výstupní adrese vyšel se starým poplatkem jediný, správný vstup. Změna na současný poplatek ovšem opět rozmělnila řešení mezi 4 možnosti.

Počet výsledků při hledání výstupů s horním stropem 10 (tedy maximum služby) v tomto případě narůstá enormně. Pro starý poplatek se počet možných variant blíží 4000, se současným přesahuje množství 11 tisíc.

5.2 BestMixer.io pro Litecoin

Nabídka i chování služby BestMixer.io pro Litecoin se z dostupných informací zdají takřka totožné s bitcoinovou variantou. Jediným rozdílem je výše poplatků, a to jak za dílčí adresy, tak procentuální odvod z celku. Sumy jsou v jeho případě řádově větší a procentuální odvody jsou trojnásobné, což může zvýšit variabilitu částek v transakcích. Naproti tomu je síť Litecoin méně aktivní, a je tedy pravděpodobné, že bude v rámci clusterů menší počet transakcí, které by párování komplikovaly. Vstupní předpoklad tedy je, že budou výsledky podobné jako u předchozí části, možná lepší.

Test a – Míchání s 1 výstupem, zásoba Alpha

Vstupní transakce:	70fa6b0f6568cf0770148d7316fe722d30efd01faba68ea2b5c83455cdb48861		
Vstupní adresa:	MKFAMU5kjNKcGYbtFdD1zU1pZMFigHLQ2s		
Výstupní transakce:	9dac4e8084a91baf469fefa451367671fda1d81dfdf1c8df5cfd5378b2ea022c		
Výstupní adresa:	MQ56ftvkBcSKYwxQbNpbyMwRQ3dNyTnSEz		
Poplatek: 1 %		**Zpoždění:**	2 h 25 min
Vložená částka:	0,1 BTC	**Čas:**	8.12.2018 23:39

První dvojice transakcí pochází z prosince 2018 a její cluster čítá pouhých 10 transakcí. Minimální poplatek v dané době činil 1 % částky plus 0,0011 LTC za adresu oproti současným 0,015 LTC. Zpoždění bylo zvoleno na 2 hodiny a 25 minut. Účelem testu je vzhledem k velikosti clusteru spíše k ověření funkčnosti algoritmů nad alternativní měnou než testování, jak si heuristika poradí se záludnými daty.

Nad daty byly provedeny standardní testy analogické k postupu u Bitcoinu. Párování s výstupem na základě vstupní transakce proběhlo dle očekávání správně a jednoznačně bez ohledu na povolený počet cílových adres. Podobně i dohledání vstupní transakce na základě výstupu proběhlo v pořádku. Algoritmus si poradil také s dohledáním možných kombinací vstupů a výstupů na základě jedné vstupní adresy a zobrazil jednoznačný výsledek. Tím dosáhl pro tento test stoprocentní úspěšnosti.

Test B – Míchání se 2 výstupy, zásoba Alpha

Vstupní transakce:	9d6d70a2eff2b2e8ff87ea1824976bfd98688e7471766e9c6737e2d517458d5b		
Vstupní adresa:	MJBJESYLM4htsVzzYjC7TQaSyNZLV3i35K		
Výstupní transakce:	0e1d5ae32117895582856660dbbfe12247756f3c66eb10390dac490cc026c451 1d3b634e54e9baa5535b940ba920c08d58a9cf4c5e22330b6978a1841d6a1af2		
Výstupní adresy:	MFJDQLc3bZ4GudE77k2iPsWWnzggCdVN4F MQ56ftvkBcSKYwxQbNpbyMwRQ3dNyTnSEz		
Poplatek: 1 %		**Zpoždění:**	1 h 46 min / 5 h 0 min
Vložená částka:	0,01 BTC	**Čas:**	1.1.2019 22:01

Druhým, tentokrát už reprezentativní reprezentativním zástupcem měla být trojice transakcí z dalšího z mixování s rozvětveným výstupem provedeného v lednu. Vstupních 0,01 BT bylo po přeprání rozesláno na dvě adresy s odstupem 1 hodiny 46 minut a 5 hodin. Poplatek byl stanoven na minimum zásobárny Alpha, tedy 1 %. Cluster obsahoval 80 transakcí, z toho jednu výstupní. Známá uživatelská vstupní transakce byla provedena mezi prvními, a tedy je třeba ve všech směrech pracovat takřka se všemi. Při základním hledání výstupních transakcí na základě vstupu nebylo nalezeno žádné řešení, a to ani po zvětšení rozptylu poplatků za služby a adresy. Při hledání v opačném směru se situace opakovala, a to ať už pro omezený počet výstupních adres, nebo neomezený. v rámci snahy o nalezení příčiny byly prozkoumány záznam transakcí v blockchainu a adresy konzultovány s clusteringovou databází. Ukázalo se, že jedna z výstupních transakcí nesplňuje předpokládaný formát. Je sice tvořena dvěma výstupními a jednou vstupní adresou, přičemž jedna z výstupních náleží zákazníkovi, adresa pro drobné ovšem nevedla do clusteru, ale na další transakci. Jelikož s tímto vzorcem se v ostatních vzorcích neoperovalo, nebylo možné bez dalšího výzkumu ani navrhnout řešení.

Test C – Míchání se 2 výstupy, zásoba Alpha

Vstupní transakce:	e570bd71e36980039a7515094d0085668464c37a117d44fed10f7d3085802540		
Vstupní adresa:	MKadQAmdc4oJrQnFDrSTMDvqMfYL9Bxwp2		
Výstupní transakce:	ab618d49eede17914dc885837e146ee556e4605326d54c03322965af1223219d 47f601105dc36a86ffa5fc70733d6654e4185c37412d1bd15b19866da5eaf9e6		
Výstupní adresy:	MCSiZHD1xD5h5Cz5zfEtB8tNzDXVVpiRRt MFibHBe3pGWyyrmSo7u3Mpzizcq8nUH3Es		
Poplatek: 1 %		**Zpoždění:**	2 h 5 min / 4 h 43 min
Vložená částka:	0,01 BTC	**Čas:**	29.4.2019 22:11

Třetím vzorkem je dubnová operace rozesílající s výstupem na dvě adresy, první se zpožděním 2 hodiny a 5 minut, druhou po 4 hodinách a 43 minutách. Poplatek byl zvolen na minimum, tedy 3 %. v clusteru je podle databáze přítomno 109 transakcí, takže se na první pohled jedná o reprezentativní data.

Naneštěstí se aplikaci nepodařilo určit žádné řešení, a to ani pro základní případy jako hledání výstupu podle vstupu nebo hledání vstupu podle daných výstupů. Výsledkem dlouhého ladění bylo zjištění, že se jedna o chybu na straně clusteringového serveru a jedna z výstupních transakcí není v jeho databázi zaregistrovaná. Bližší pohled přes webový prohlížeč Litecoin blockchainu ukázal, že výstup transakce ve směru k uživateli nebyl dosud vybrán. Zde možná tkví potenciální zdroj komplikací.

5.3 Zhodnocení poznatků

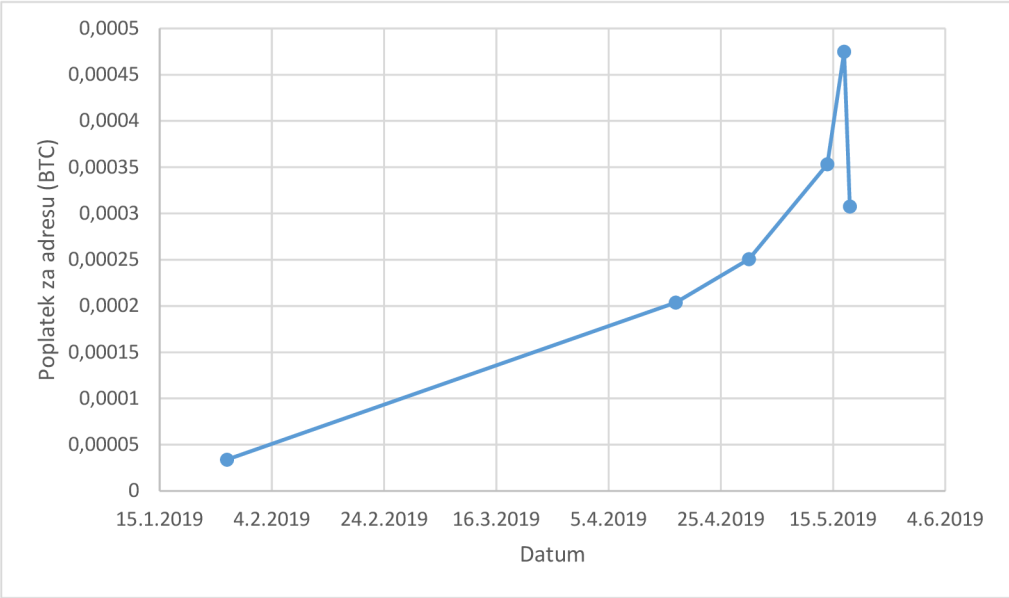
Cílem této kapitoly bylo ověřit dosavadní poznatky, návrhy a na jejich základě vytvořené aplikační řešení pro deanonymizaci praní špinavých peněz využívající mixovací služby. Jak se v testech ukázalo, úspěšnost algoritmu je závislá na mnoha faktorech, z nichž některé jsou ovlivnitelné, jiné nikoli. Nejvíce faktor náhody zasahuje do samotného obsahu clusteru, resp. do přítomných transakcí. Pro snadnou párovatelnost je třeba, aby byly přenášené obnosy dostatečně rozlišitelné. Pakliže mají všechny transakce stejný tvar a na výstupy totožnou částku, je jejich záměna přes sebelepší heuristiku nevyhnutelná. Započítáme-li navíc proměnlivou povahu poplatků, je pro korektní určení mezi částkami nutný dostatečný odstup. Roli může sehrát také velikost clusteru, daná množstvím zákazníků, kteří po dobu jeho životnosti službu využili. v provedených testech se však přímá souvislost neprokázala.

Tím se dostáváme k otázce parametrů, jež se naopak pro přesnost výsledků ukázaly jako zásadní. Některé, jako například maximální doba zpoždění, se podílí měrou menší – clustery mají krátkou životnost, transakce oddělují malé časové intervaly, a množinu potenciálních transakcí tedy příliš nezužují. Zvláště pak jejich význam klesá, přihlédneme-li k faktu, že v některých případech podobnou, byť ne stejnou funkci plní kritérium časové posloupnosti, tedy že vstupy musí předcházet výstupům. Větší vliv na výsledek mají poplatky, jež mohou citelně zvětšit prohledávaný cenový interval. v provedených testech se výrazně projevovaly především limity poplatků za jednotlivé výstupní adresy. Tento efekt byl dán především faktem, že byly do mixéru zasílány pouze malé obnosy, z nichž pak testovaná sada vycházela. Dá se však předpokládat, že u velkých částek by měl zásadnější dopad právě druhý parametr týkající se poplatků, a to odměna mixovací službě určovaná v procentech vložené částky. Klíčový z hlediska počtu výsledků je nicméně parametr omezení počtu výstupních adres, jenž zvláště při párování na základě výstupní transakce bez znalosti vstupu nebo počtu výstupů může množství výsledků posunout o celé řády.

Z výše uvedeného vyplývá, že pro úspěšnou negaci činnosti mixéru je důležité znát co nejvíce informací ať už o příslušném mixéru, nebo konkrétní analyzované finanční transakci.

Vzhledem k tomu, v běžných situacích je cílem mixování zahladit stopu o původu peněz, jsou možnosti upřesnění parametrů konkrétní operace značně omezené. Proto je perspektivnější soustředit se na vlastnosti samotného mixéru, o což se tato práce pokoušela v rámci kapitoly 3. Zde však nastává komplikace.

Mixovací služby jsou už ze své povahy nestálé, neustále vznikají, zanikají nebo se transformují, musí navíc reagovat i na momentální situaci v kryptoměnové síti. Udržet s nimi kompatibilitu na základě jednorázově zjištěných hodnot je takřka nemožné, jelikož žádné univerzální hodnoty zkrátka neexistují. Příkladem budiž vývoj poplatků za dílčí výstupní adresy ve službě BestMixer.io při mixování Bitcoinů, vynesený přibližně na grafu 5.1 na základě hodnot mimoděk nasbíraných během zkoumání služby. v posledních měsících prudce narůstá, zřejmě v souvislosti s růstem výše poplatků za transakce[6], a od ledna se více než zdesetinásobil.



Obrázek 5.1: Graf vývoje poplatků za dílčí výstupní adresy u služby BestMixer.io

Přesto je pro něj z důvodu nedostatku informací v současném řešení aplikace zvolena fixní výchozí hodnota snažící se vyhovět všem možnostem, přičemž uživatel může při vyhledávání zadat jinou. Dlouhodobým řešením by mohlo být v pravidelných intervalech snímat aktuální hodnotu poplatků z webu služby a vytvořit databázi mapující je na konkrétní časy. Stejným způsobem se v čase mění i procentuální poplatky za použití služby, avšak k tomu dochází pozvolněji. Podobným proměnlivým faktorem, jež se při zkušebních transakcích vyskytl, avšak nebylo dost vzorků pro jeho konkrétní zařazení, byla proměna formátu adres mixéru. v době počátku zkoumání používal segwitové varianty adres začínající znakem 3, někdy v průběhu února však došlo k přechodu na klasické adresy začínající 1. Při podrob-

nějším zdokumentování a časovém zařazení by se opět mohlo jednat o zpřesňující prvek při párování transakcí.

Jak se však ukázalo při testech v síti Litecoin, prospěla by projektu i rozsáhlejší testovací sada umožňující odhalit další specifické obměny v transakcích a toku peněz. v mantinelech práce však bohužel byly možnosti omezeny dostupnými finančními prostředky, jelikož poplatky jsou vysoké a v tuto chvíli stále narůstají. Z toho důvodu chyběly například testy více než dvou výstupních adres.

I přes nedostatky však heuristika funguje a minimálně v bitcoinové variantě pro rozmanitější sady transakcí při správně nastavené výší poplatků funguje úspěšně. Z logiky věci sklízí lepší výsledky u situací, kdy jsou známy všechny vstupní, případně výstupní adresy, jelikož při dohledávání obou stran vzniká mnohonásobně více možností, které je třeba uvážit a mohou působit zaměnitelně.

Kapitola 6

Závěr

V rámci práce byly nastudovány principy a provozní praxe kryptoměn se zaměřením na jejich metody obfuskace informací o přenesených penězích. Zvláštní pozornost při tom byla věnována kryptoměnám Bitcoin, Litecoin a Ethereum. Popsán byl také koncept clusterizace a způsoby, jakými se vůči ní ve snaze o anonymizaci bojuje.

Následně byla vybrána a analyzována šestice portálů poskytujících službu mixování transakcí. Na základě prvotních zjištění byly pro službu BestMixer.io navrženy heuristiky, s jejichž pomocí by mělo být možné obnovit přerušenou vazbu mezi penězmi na vstupu a na výstupu. Zvolená služba byla dále testována a na základě nových poznatků byly vytvořena modifikovaná heuristiky umožňující exaktnější párování transakcí. Dalším krokem bylo navrhnout aplikační řešení, které by umožnilo heuristiky validovat a zároveň umožňovalo pozdější praktické začlenění do projektu Tarzan, zaměřeného na boj proti kybernetické kriminalitě. Řešení bylo realizováno jako webová aplikace vytvořená za pomoci PHP frameworku Laravel. Prostřednictvím vzniklého programu bylo nakonec provedeno ověření funkčnosti řešení na sadě testovacích transakcí, jež byly shromážděny při zkoumání mixovací služby. Na základě částečných úspěchů jsou v závěru předposlední kapitoly analyzovány vlastnosti a úskalí deanonymizace mixovacích služeb a navržena řešení, jakými funkčnost heuristik zlepšit.

Literatura

[1] *EOS.IO Technical White Paper v2.* [Online; navštíveno 25.01.2018].
URL https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[2] *Ouroboros Proof of Stake Algorithm.* [Online; navštíveno 26.01.2018].
URL https://cardanodocs.com/cardano/proof-of-stake/

[3] *Proof of Work vs Proof of Stake: Basic Mining Guide.* [Online; navštíveno 10.12.2018].
URL https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

[4] *What Is Stellar?* [Online; navštíveno 25.01.2018].
URL https://cryptocurrencyfacts.com/what-is-stellar/

[5] *Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference.* 2018, [Online; navštíveno 27.01.2018].
URL https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block

[6] Canellis, D.: *Bitcoin miners earn $305M in April as transaction fees jump 250%.* Apr 2019, [Online; navštíveno 21.05.2019].
URL https://thenextweb.com/hardfork/2019/05/07/bitcoin-miners-305-million-transactions-segwit-cryptocurrency/

[7] Chong, N.: Ethereum (ETH) Developers Cut Block Rewards By 33% To Curb Inflation. *Ethereum World News*, Aug 2018, [Online; navštíveno 23.01.2018].
URL https://ethereumworldnews.com/ethereum-developers-cut-rewards-curb-inflation/

[8] Detrixhe, J.: Bitcoin drops as China renews crackdown on cryptocurrency. *Quartz*, Jan 2018, [Online; navštíveno 05.01.2018].
URL https://qz.com/1180326/bitcoin-btc-price-drops-on-chinas-cryptocurrency-crackdown/

[9] Dexter, S.: *Longest Chain – How Are Blockchain Forks Resolved?* [Online; navštíveno 7.01.2018].
URL https://www.mangoresearch.co/blockchain-forks-explained/

[10] Ermilov, D.; Panov, M.; Yanovich, Y.: Automatic Bitcoin Address Clustering. In *Machine Learning and Applications (ICMLA), 2017 16th IEEE International Conference on*, IEEE, Dec 2017, s. 461–466.

[11] Fernando, J.: *Bitcoin Vs. Litecoin: What's The Difference?* [Online; navštíveno 18.01.2018].
URL https://www.investopedia.com/articles/investing/042015/bitcoin-vs-litecoin-whats-difference.asp

[12] gmaxwell: *CoinJoin: Bitcoin privacy for the real world.* [Online; navštíveno 26.01.2018].
URL https://bitcointalk.org/?topic=279249

[13] Hopwood, D.; Bowe, S.; Hornby, T.; aj.: *Zcash Protocol Specification.* [Online; navštíveno 25.01.2018].
URL https://github.com/zcash/zips/blob/master/protocol/protocol.pdf

[14] Kaiser, B.; Jurado, M.; Ledger, A.: The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin. *CoRR*, ročník abs/1810.02466, 2018, 1810.02466.
URL http://arxiv.org/abs/1810.02466

[15] Linzerd: *EOS Centralized Government Can Rollback Transactions.* [Online; navštíveno 26.01.2018].
URL https://coinspice.io/eos/centralized-eos-rollback-transactions/

[16] Lombrozo, E.; Lau, J.; Wuille, P.: *Segregated Witness (Consensus layer).* Dec 2015, [Online; navštíveno 14.03.2019].
URL https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[17] Mangal, A.: *What Is Monero (XMR)? | An In-Depth Guide to the Privacy Coin.* [Online; navštíveno 25.01.2018].
URL https://coincentral.com/what-is-monero/

[18] Marley, N.: *Dash: A Payments-Focused Cryptocurrency.* [Online; navštíveno 10.12.2018].
URL https://github.com/dashpay/dash/wiki/Whitepaper

[19] Matonis, J.: *A Taxonomy of Bitcoin Mixing Services for Policymakers.* [Online; navštíveno 26.01.2018].
URL
https://www.coindesk.com/taxonomy-bitcoin-mixing-services-policymakers

[20] Nakamoto, S.: *Bitcoin: A Peer-to-Peer Electronic Cash System.* [Online; navštíveno 07.01.2018].
URL https://www.bitcoin.com/bitcoin.pdf

[21] Narayanan, A.; Bonneau, J.; Felten, E. W.; aj.: *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press, 2016.

[22] Nick, J. D.: *Data-Driven De-Anonymization in Bitcoin.* Diplomová práce, ETH Zürich, 2015.
URL https://doi.org/10.3929/ethz-a-010541254

[23] Noether, S.; Mackenzie, A.; Monero Research Lab, T.: Ring Confidential Transactions. *Ledger*, ročník 1, 12 2016: s. 1–18, doi:10.5195/LEDGER.2016.34.
URL https://www.researchgate.net/publication/311865049_Ring_Confidential_Transactions

[24] Parsons, M.: *Cardano: A Blockchain with Privacy and Regulation*. [Online; navštíveno 26.01.2018].
URL https://medium.com/@BitcoinByte/a-blockchain-with-privacy-and-regulation-cardano-3606e1288bc2

[25] Percival, C.; Josefsson, S.: *The scrypt Password-Based Key Derivation Function*, RFC7914. 2016, [Online; navštíveno 20.01.2018].
URL https://tools.ietf.org/pdf/rfc7914.pdf

[26] Peterson, P.: *Anatomy of A Zcash Transaction*. [Online; navštíveno 25.01.2018].
URL https://z.cash/blog/anatomy-of-zcash/

[27] Poon, J.; Dryja, T.: *The Bitcoin Lightning Network: Scalable Off-Chain Instant PaymentsThe Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Jan 2016, [Online; navštíveno 14.03.2019].
URL https://lightning.network/lightning-network-paper.pdf

[28] Ray, J.: *A Next-Generation Smart Contract and Decentralized Application Platform*. Aug 2018, [Online; navštíveno 20.01.2018].
URL https://github.com/ethereum/wiki/wiki/White-Paper

[29] Thake, M.: *What is Proof of Stake? (PoS)*. Jul 2018, [Online; navštíveno 15.01.2018].
URL
https://medium.com/nakamo-to/what-is-proof-of-stake-pos-479a04581f3a

[30] Tsihitas, T.: *Ripple vs Bitcoin Comparison*. [Online; navštíveno 25.01.2018].
URL https://coincentral.com/ripple-vs-bitcoin/

Příloha A

Obsah CD

Přílohou diplomové práce je CD s následujícím obsahem:

demixer Zdrojové kódy projektu.

text-src Zdrojové kódy textové části práce.

README.txt Popis pro zprovoznění aplikace.

xanton03.pdf Textová část práce.