Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Ústav aplikované informatiky

Analýza a forenzní zkoumání kryptoměny Bitcoin

Bakalářská práce

Tadeáš Pekárek

Školitel: RNDr. Libor Dostálek

České Budějovice 2020

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÉ PRÁCE

Student: Tadeáš Pekárek , B16240
(jméno, příjmení, tituly)

Obor – zaměření studia: Aplikovaná informatika

Katedra/ústav PřF JU, kde bude práce vypracována a obhájena: UAI

Školitel: RNDr. Libor Dostálek
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Garant z PřF JU: .....
(jméno, příjmení, tituly, katedra – jen v případě externího školitele)

Školitel – specialista, konzultant:
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Téma bakalářské práce: Analýza a forenzní zkoumání kryptoměny Bitcoin

Úkoly práce:

• Vytvoření komplexní literární rešerše a analýza současného stavu v předmětné oblasti

1. Detailní objasnění fungování kryptoměny Bitcoin
2. Analýza způsobů ukládání a získávání Bitcoinu a jejich porovnání s alternativními kryptoměnami.

Cíle práce:

* Hlavní cíl: Vytvoření metodiky pro vyhledávání kryptoměny Bitcoin v počítačovém zařízení

* Dílčí cíl: Aplikování vytvořené metodiky, následné vyhodnocení získaných informací a porovnání s výsledky profesionálních forenzních nástrojů

Upřesnění cíle práce: Student vytvoří postup pro vyhledávání kryptoměny na počítačovém zařízení, kde vysvětlí a popíše, jakým způsobem a co bude vyhledávat, aby na daném počítačovém zařízení detekoval přítomnost kryptoměny. Tuto metodiku následně aplikuje, vyzkouší a zautomatizuje pomocí scriptu, který sám vytvoří. Následně použije dostupné forenzní nástroje na testovaných zařízení a porovná získané výsledky.

Základní doporučená literatura:

Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash Systém

Andreas M. Antonopoulos, Mastering Bitcoin

Michael Doran, A Forensic Look at Bitcoin Cryptocurrency

https://bitcoin.org/en/

Financování práce .....

Školitel práce .....podpis: .....

U externích vedoucích fakultní garant práce .....podpis: .....

Garant oboru bak. studia .....podpis: .....

Vedoucí katedry/ústavu PřF JU, kde proběhne obhajoba.....podpis: .....

Případný souhlas vedoucího ústavu AV .....podpis: .....

V Českých Budějovicích dne 4. 3. 2019 .....Podpis studenta .....

Bibliografické údaje

Pekárek Tadeáš, 2020: Analýza a forenzní zkoumání kryptoměny Bitcoin.
[Analysis and forensic investigation of Bitcoin cryptocurrency, Bc. Thesis, in Czech] – Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Abstrakt

Bakalářská práce „Analýza a forenzní zkoumání kryptoměny Bitcoin“ se zabývá tvorbou metodiky pro vyhledávání Bitcoinu v počítačovém zařízení, praktickou aplikací metodiky a porovnání získaných výsledků s profesionálními forenzními nástroji. Součástí práce je teoretická část obsahující detailní popis fungování kryptoměny Bitcoin, způsoby uložení a porovnání s alternativními kryptoměnami, které by z technologického hlediska bylo vhodnější využít k nevystopovatelným transakcím.

Klíčová slova

Bitcoin, kryptoměna, alternativní kryptoměny, forenzní, analýza, zkoumání, forenzní nástroje, metodika

Abstract

The bachelor’s thesis „Analysis and forensic investigation of Bitcoin cryptocurrency“ deals with creation of methodology for searching for Bitcoin on computer device, practical application of the methodology and comparison of obtained results with proffesional forensic tools. Theoretical part contains detailed description of how Bitcoin cryptocurrency works, it’s storage ways and comparison with alternative cryptocurriencies which would be, from technological aspect, more appropriate to use for non-tracable transactions.

Keywords

Bitcoin, cryptocurrency, alternative cryptocurrency, forensic, analysis, investigation, forensic tools, methodology

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury. Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 2. dubna 2020

Tadeáš Pekárek

Poděkování

Na tomto místě bych rád poděkoval RNDr. Liborovi Dostálkovi za cenné připomínky a odborné rady, kterými přispěl k vypracování této bakalářské práce.

Obsah

1 Úvod

S rychle rostoucím vývojem technologií a zejména příchodem internetu se objevila možnost realizace plateb online, která dala za vznik novým platebním systémům a samotným měnám v digitální podobě. Jedním typem těchto měn jsou právě kryptoměny, avšak v době vzniku této práce se dle zákonů České republiky nejedná o měnu, ale o nehmotnou movitou věc. V současnosti existují stovky kryptoměn, ale nejvíce využívanou a zároveň úplně první kryptoměnou je Bitcoin, který byl vytvořen anonymní osobou či skupinou pod názvem Satoshi Nakamoto v roce 2009 v reakci na to, že klasické převody peněz mezi bankami byly velmi pomalé, nákladné, netransparentní a neanonymní. Pro Bitcoin toto neplatí a vzhledem k tomu, že je předem stanovený konečný počet mincí, nepodléhá inflaci a je naopak deflační, čímž se stává populárním investičním nástrojem nazývaným digitální zlato. Bitcoin se dostal do povědomí lidí zejména kvůli raketovému růstu jeho ceny v posledních letech a následné silné medializaci. Rostoucí trend způsobil zájem lidí a společností o tuto platební technologii, ale také silné využití na temné straně internetu a na poli ilegálních internetových obchodů, jako byla například nechvalně proslulá Silk Road a s ní spojená mediální kauza s jejím původním zakladatelem Rossem Ulbrichtem.

Teoretická část této práce je zaměřena na detailní objasnění fungování kryptoměny Bitcoin, kde jsou popsány rozdíly mezi uvedenou kryptoměnou a tradičními měnami v elektronické podobě, využitá kryptografie, samotný průběh transakčních operací, decentralizovaná databáze blockchain, která řeší problém digitálních měn, a to problém dvojitého utrácení a konsensní algoritmus Proof-of-Work zajišťující dosažení shody uzlů v síti. Součástí teoretické části jsou dále způsoby uložení kryptoměny bitcoin s popisem všech druhů peněženek, jeho získávání včetně názorného příkladu těžby a porovnání s alternativními kryptoměnami a způsoby jejich získávání.

V praktické části vytvářím a detailně popisuji metodiku pro vyhledávání kryptoměny Bitcoin v počítačovém zařízení pro tři vybrané desktopové peněženky s cílem detekce klientů a samotných souborů záloh peněženek. Součástí metodiky je také její praktická implementace v podobě skriptu, který tento celý proces detekce automatizuje a získané informace zaznamenává. Výsledky jsou poté porovnávány s výsledky profesionálních forenzních nástrojů použitých při zkoumání počítačového zařízení na vybrané desktopové peněženky.

2 Bitcoin

Bitcoin je úplně první digitální kryptoměna umožňující přenos hodnoty mezi uživateli na stejnojmenné platební peer-to-peer síti, ta funguje nezávisle na jakékoliv centrální autoritě. Autorem je Satoshi Nakamoto, který dodnes zůstává v anonymitě. Ten dne 18. září 2008 zaregistroval doménu bitcoin.org a 31. října téhož roku publikoval k Bitcoinu whitepaper s názvem „Bitcoin: A Peer-to-Peer Electronic Cash System“. [1] Celá platební síť byla poté vytvořena 3. ledna 2009 vytěžením bloku 0, později nazývaným jako Genesis Block, samotným autorem Bitcoinu, ten ke coinbase transakci jako časové razítko přidal následující text: „The Times 03/Jan/2009 Chancellor on brink of second bailout for banks“, odkazující na článek z The Times z téhož dne. [2]

Rozdíly mezi Bitcoinem a tradičními měnami v elektronické podobě:

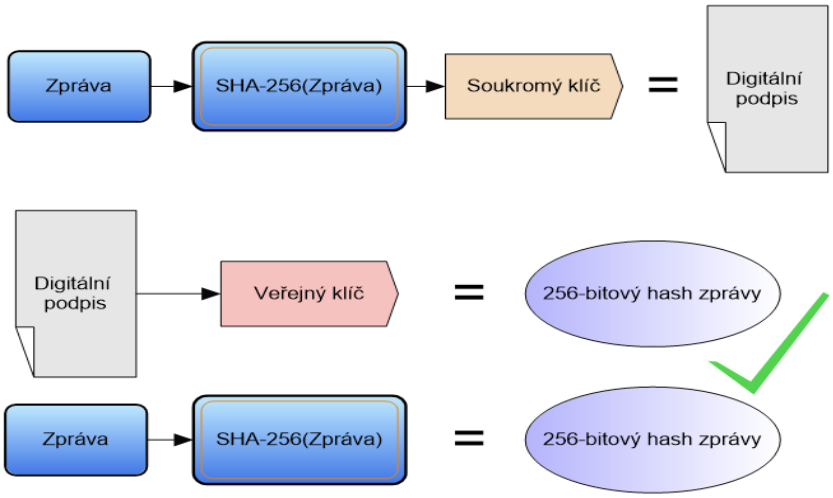
- **Decentralizace** – jedná se o nejdůležitější vlastnost celého Bitcoinu. Žádná centrální autorita nevydává nové mince, nekontroluje transakce a neřídí síť. Celý systém je peer-to-peer, emitace nových mincí je řešena formou odměn těžařům za potvrzování transakcí a síť se řídí konsensním algoritmem.
- **Transparentnost a neměnitelnost** – všechna data jsou transparentní, neměnná a navždy uložená v decentralizované databázi blockchain, tímto je také řešen problém dvojitého utrácení.
- **Ireverzibilita** – transakce jsou nevratné a neměnné.
- **Pseudonymita** – uživatelé neprokazují vlastní identitu, místo toho jsou reprezentováni alfanumerickým řetězcem znaků známým jako bitcoinová adresa, nicméně tento způsob není zcela anonymní vzhledem k tomu, že například burzy vyžadují verifikaci svých uživatelů a lze takto spojovat bitcoinové adresy s konkrétními osobami**.**
- **Dělitelnost** – bitcoin je možné dělit až na jednu miliontinu (0.00000001฿), ta se označuje podle autora jako 1 satoshi.
- **Deflace** – maximální počet bitcoinů je 21 milionů, čímž se stává deflačním oproti tradičním měnám, které můžou centrální banky emitovat dle potřeby.
- **Open-source** – celý Bitcoin je open-source, každý se může do kódu podívat a zjistit, jak funguje, či jej využít pro tvorbu vlastní kryptoměny. [3]

2.1 Princip fungování

Bitcoin je založen na decentralizaci a asymetrické kryptografii. Decentralizovaná bitcoinová síť nemá žádný centrální uzel, místo toho uzly komunikují a předávají si data přímo mezi sebou. Asymetrická kryptografie využívá Elliptic Curve Digital Signature Algorithm (ECDSA), tento algoritmus počítá ze soukromého klíče korespondující veřejný klíč násobením eliptické křivky. [4] Kolekce klíčů je spravována bitcoinovou peněženkou a slouží k vlastnictví a realizaci bitcoinových transakcí. Transakci je potřeba někam zapsat a ověřit, že její autor skutečně bitcoiny vlastní, to je řešeno na základě digitálního podpisu, který je ověřován ostatními uzly a transakce je nimi dále šířena po síti, dokud není speciálním uzlem nazývaným těžař zahrnuta do bloku a zapsána do veřejné databáze blockchain. Databáze rovněž není umístěna na žádném centrálním serveru, uzly si ukládají její kopii a dále ji mezi sebou distribuují. Celý decentralizovaný systém je pak založen na konsensním algoritmu, který zajišťuje dosažení dohody v síti.

2.1.1 Soukromý klíč

Soukromý klíč je náhodně vygenerované 256-bitové číslo, které je základem pro vlastnění bitcoinu a realizaci bitcoinových transakcí, jelikož slouží k vytváření digitálních podpisů, ty přímo prokazují, že autor transakce je skutečně držitelem soukromého klíče. Digitální podpis se skládá ze dvou funkcí, a sice z podepsání a ověření podpisu (obr. 1). [5]



Obrázek 1 Vytváření a ověřování digitálního podpisu (vlastní zpracování)

Pro lepší čitelnost a redukci délky se klíč převádí do takzvaného Wallet Import Format (WIF) využívající Base58Check kódování. Jedná se o vylepšené reverzní Base58 kódování, které převádí binární číslo na text, kde na konci textu je navíc přidaný kód pro detekci chyb. Klíč v této podobě má prefix L nebo K a neobsahuje znaky jako jsou: nula, velké písmeno O, I, malé písmeno l a všechny nealfanumerické znaky, aby nemohlo dojít k záměně. [6]

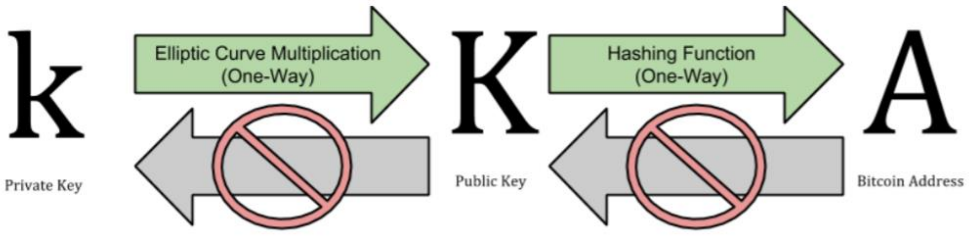
Ke každému soukromému klíči koresponduje právě jeden veřejný, z toho je jednosměrnou funkcí vypočítána bitcoinová adresa. Klíč je nutné udržovat v bezpečí a soukromí, protože ztráta či prozrazení může vést k nenávratné ztrátě bitcoinů.

Příklad náhodně vygenerovaného soukromého klíče ve WIF:

5K1j6otY1i4SRdeDddFZX3MVHMjExCVkuPzVo2trKvQ99SUv2LF

2.1.2 Veřejný klíč

Veřejný klíč je 256-bitové číslo, které na rozdíl od soukromého klíče není náhodně generováno, ale je z něj přímo jednosměrně matematicky vypočítáno násobením eliptické křivky. Veřejný klíč je reprezentován v podobě bitcoinové adresy, ta je z klíče derivována pomocí jednosměrné hashovací funkce. [7]

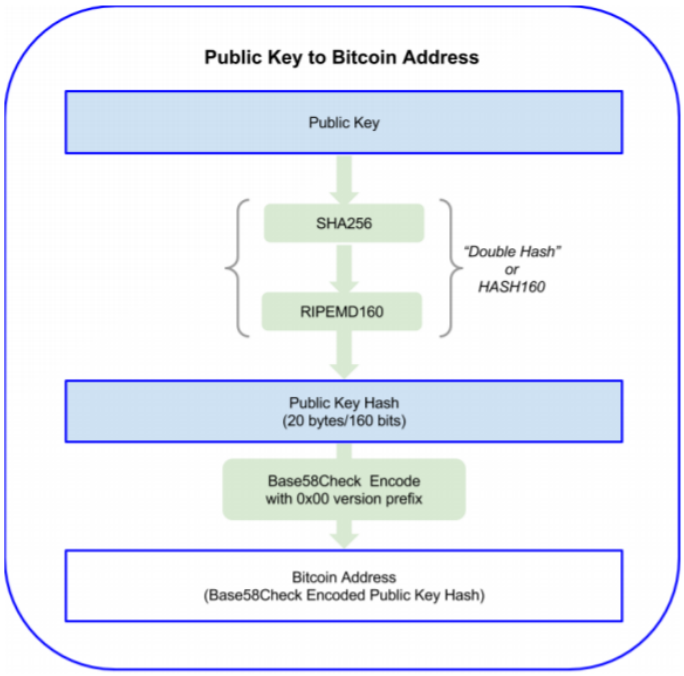


Obrázek 2 Soukromý klíč, veřejný klíč, bitcoinová adresa [7]

2.1.3 Bitcoinová adresa

Bitcoinová adresa slouží k přijímání či odesílání bitcoinů stejně jako při běžných bankovních transakcích číslo účtu příjemce a odesílatele. Adresa je jednosměrně přímo derivována z veřejného klíče za pomoci hashovací funkce SHA-256 a RIPEMD-160, kde výstupem je 160-bitový hash veřejného klíče, na ten je stejně jako na soukromý klíč aplikováno reverzní Base58Check kódování (obr. 3) a výsledkem je alfanumerický řetězec o délce 26-35 znaků. Bitcoinová adresa má tři formáty, které začínají 1, 3 nebo bc1. [7]

Speciálním typem adresy je vícepodpisová adresa, ta má dva a více soukromých klíčů. Zde platí vztah M:N, kde N je celkový počet soukromých klíčů a M je minimální počet soukromých klíčů potřebných k podepsání transakce. [8]



Obrázek 3 Derivace bitcoinové adresy z veřejného klíče a její kódování [7]

2.1.4 Transakce

Bitcoinová transakce je nejdůležitější operací celého platebního systému. Jedná se o přenos hodnoty mezi uživateli bitcoinové sítě. Hodnota není uložena v peněžence jako takové, ale je uložena právě v transakcích. Každá bitcoinová adresa si uchovává záznam o příchozích a odchozích transakcích, ty jsou transparentní a navždy uložené v blocích v databázi blockchain.

Transakce se skládá ze vstupu a výstupu. Vstup každé nové transakce je vždy ukazatelem na výstup předchozí transakce, tímto je tvořen řetěz vlastnictví. Výstup transakce je označován jako Unspent Transaction Output (UTXO). Pokud uživatel obdrží nějaké množství bitcoinů, je tento výstup v blockchainu označen jako UTXO a registrován pro jeho adresu. Chce-li uživatel bitcoin odeslat, vytvoří transakci, která jako vstup použije UTXO (jeden nebo více) jeho adresy, podepíše ji svým soukromým klíčem a rozešle do sítě okolním uzlům. Uzly digitální podpis zkontrolují veřejným klíčem autora transakce a rozešlou ji svým okolním uzlům, tímto je zajištěno, že se sítí šíří pouze validní transakce. Transakce bere UTXO jako celek, pokud je tedy nějaký zbytek, vytvoří dva transakční výstupy, jeden ve prospěch nového majitele a druhý jako zbytek pro původního standardně na nově

vygenerovanou adresu. Tímto způsobem je možné bitcoin dělit až na jednu miliontinu (0.00000001₿), kde nejnižší možná jednotka se označuje 1 satoshi. Pokud ostatní uzly transakci potvrdí jako platnou, čeká se na to, až ji těžební uzel zahrne do bloku a vytěží, tím se transakce stává potvrzenou. [7] [9]

Součástí transakce je také poplatek těžařům za zahrnutí do bloku. Poplatek si uživatel většinou může upravit sám, čím vyšší je, tím dříve bude transakce zahrnuta do bloku a potvrzena, jelikož těžaři prioritně vybírají transakce s vyššími poplatky. [10]

2.1.5 Blok

Blok je datová struktura obsahující transakční data v daném čase. Lze si jej představit jako stránku v účetní knize, která je navíc pro všechny transparentní a lehce dostupná v každém blockchain prohlížeči. Bloky jsou za sebou řazeny lineárně od úplně prvního vytěženého bloku s pořadovým číslem 0. Tento blok se nazývá Genesis Block a každý další blok obsahuje odkaz na ten předchozí v podobě hashe předchozího bloku, čímž se tvoří řetěz – blockchain. Blok musí obsahovat minimálně jednu transakci, a sice coinbase transakci, ta slouží jako výplata pro těžaře za nalezení řešení nového bloku. Odměna začínala 3. ledna 2009 vytěžením Genesis Blocku samotným tvůrcem Bitcoinu Satoshi Nakamoto na 50 BTC + transakční poplatky všech transakcí v bloku a každých 210000 bloků (přibližně jedenou za 4 roky) se tato odměna půlí (halving). Blok může být identifikován kryptografickým hashem nebo výškou, to je numerické číslo od 0.

Do nedávna byla maximální velikost bloku 1 MB, avšak s implementací Bitcoin Improvement Proposals 141 (BIP 141) - Segregated Witness (SegWit) se velikost změnila. SegWit rozděluje transakci do dvou segmentů, kde první část obsahuje data odesílatele a příjemce a druhá vytváří strukturu witness, ta obsahuje transakční skripty a digitální podpisy. Byl přidán nový parametr weight units (WU) a z původní maximální velikosti bloku 1 000 000 bajtů může blok nyní mít 4 000 000 WU. U transakcí využívaných SegWit platí 1 bajt = 1 WU a u non-SegWit transakcí 1 bajt = 4 WU. [11]

Název	Velikost v bajtech
Velikost bloku	4
Hlavička bloku	80
Počet transakcí	1-9
Transakce	dle velikosti a počtu transakcí

Tabulka 1 Struktura bloku [12]

Hlavička bloku obsahuje:

- Verze – mění se se změnami v protokolu/softwaru, aktuálně se používá verze 4.
- Hash předchozího bloku – ukazatel na předchozí blok.
- Merkle Root – hash merkle stromu obsahující všechny transakce bloku.
- Čas - v sekundách od 1970-01-01 T:00:00 UTC.
- Cíl – obtížnostní číslo, kterému musí hash bloku vyhovovat.
- Nonce – číselná hodnota hledaná a přidávaná do bloku těžařem. [13]

Název	Velikost v bajtech
Verze	4
Hash předchozího bloku	32
Merkle Root hash	32
Čas	4
Cíl	4
Nonce	4

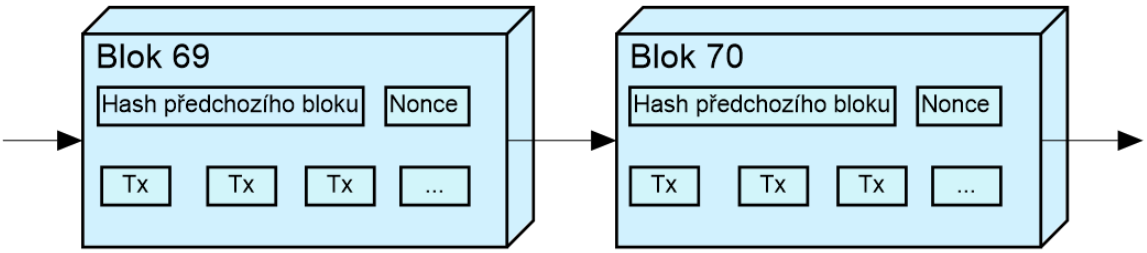
Tabulka 2 Hlavička bloku [13]

2.1.6 Blockchain

Blockchain je decentralizovaná distribuovaná databáze připomínající velkou účetní knihu obsahující záznamy o všech potvrzených transakcích v bitcoinové síti, toto umožňuje udržovat přehled stavů adres od jejich vzniku, tím je také vyřešen problém dvojitého utrácení. Decentralizovaná proto, že neexistuje žádná centrální autorita spravující blockchain a data se nedistribuují z jednoho serveru, jako tomu je u centralizovaných systémů (klient-server), ale jsou broadcastována a zaznamenávána všemi uzly v bitcoinové síti (klient-klient), které si uchovávají kompletní kopii celého blockchainu. Blockchain je složen z bloků, které nesou všechna transakční data s časovými razítky a zároveň odkazují na předešlé bloky (obr. 4), čímž tvoří dlouhý lineární řetěz. Všechna data v blockchainu jsou transparentní, auditovatelná a trvalá, jelikož jakákoliv zpětná změna je spíše jen teoreticky než prakticky možná, a to z toho důvodu, že pokud by chtěl útočník data bloku jakkoliv pozměnit, musel by ovládat nadpoloviční většinu výpočetního výkonu v síti a zpětně na bloku a všech po něm následujících vykonat práci znovu. Z ekonomického hlediska se více vyplatí věnovat výpočetní výkon k zabezpečení sítě než snaze ji poškodit.

Bloky do blockchainu přidávají těžaři řešením složitého matematického problému, který je ovšem zpětně pro všechny jednoduchý ke kontrole. Může se stát, že se blockchain rozvětví vytěžením dvou bloků ve stejný čas, v tomto případě uzly zařadí do blockchainu

jako aktivní ten blok, který k nim dorazí jako první a druhý uloží. Problém se vyřeší s vytěžením dalšího bloku, který naváže na jeden z bloků a vytvoří tím nejdelší řetěz. Uzly se řídí pravidlem, že nejdelší řetěz je ten platný. [14]



Obrázek 4 Řetězení bloků (vlastní zpracování) [1]

2.1.7 Proof-of-Work

Proof-of-Work („důkaz práce“ - PoW) algoritmus, který Bitcoin využívá, je konsensní algoritmus využívající Hashcash Proof-of-Work systému Adama Backa z roku 1997 navrženému k anti-DoS použití. [15] Proof-of-Work hraje u Bitcoinu zásadní roli v oblasti zabezpečení sítě a dosažení shody, bez toho by decentralizovaný systém nemohl fungovat.

PoW využívá výpočetní výkon k nalezení správného řešení pro blok. Blok obsahuje číselné pole s názvem nonce („number only used once“), to je 32-bitové číslo, které těžař do bloku přidává a počítá hash hlavičky bloku pomocí dvojité hashovací funkce SHA-256 tak, aby výsledný hash byl menší nebo roven aktuálnímu cíli obtížnosti s odpovídajícím počtem počátečních nulových bitů. Pokud výsledek obtížnosti nevyhovuje, těžař zvýší nonci o jedna a počítá znovu. Takto to dělá do doby, než nalezne správné řešení. Když je řešení nalezeno, rozešle ho ostatním uzlům, které si jej jednoduše dosazením nonce zkontrolují, uznají platným, zařadí do blockchainu a těžební uzel za nalezené řešení získá odměnu. Například Genesis Block má nonci 2 083 236 893, to znamená, že Satoshi musel více než dvou miliardkrát zvýšit nonci, aby hash bloku vyhovoval obtížnostnímu cíli. Může nastat situace, kdy těžař vyčerpá všechny možné kombinace od nuly a nenajde řešení. V této chvíli přichází na řadu takzvaná extra nonce. Extra noncí je myšleno pole coinbase data u coinbase transakce, do kterého lze libovolně dosadit jakékoliv číslo nebo text a tím změnit hash bloku. Po dosazení extra nonce se hash bloku počítá znovu s noncí od nuly, dokud není nalezeno správné řešení. Extra nonce může mít libovolnou velikost od 2 do 100 bajtů a zároveň musí splňovat kapacitní limit bloku.

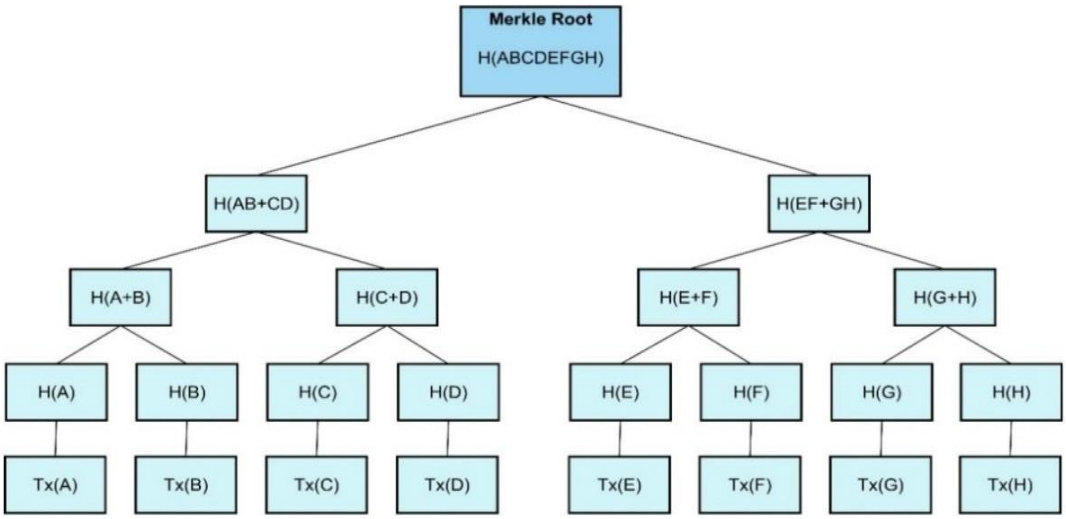
Tento způsob konsensu je nejvíce ekonomicky náročný, jelikož vyžaduje drahý výpočetní hardware, ten navíc spotřebovává nemalé množství elektrické energie. Také je zde větší šance 51% útoku oproti například Proof-of-Stake, protože je snazší vlastnit nadpoloviční většinu výpočetního výkonu než nadpoloviční většinu všech mincí. [16]

3 Získávání bitconů

3.1 Těžba

Těžba je proces potvrzování a přidávání transakcí do databáze blockchain. Těžař je speciální uzel v bitcoinové síti, který propůjčuje svůj výpočetní výkon k řešení matematického problému Proof-of-Work.

Těžební uzel funguje jako netěžební uzly, také přijímá, kontroluje a distribuuje příchozí transakce a nové bloky, navíc si ale všechny validní transakce ukládá v paměti do transakčního poolu (mempool). Těžař sestaví svého kandidáta na blok vytvořením hlavičky bloku, ta se skládá z šesti komponent, kde z transakčního poolu vybere transakce prioritně dle stáří a výše poplatku a hashuje je dvojitou hashovací funkcí SHA-256 do datové struktury Merkle Tree, dokud nezíská jediný Merkle Root hash (obr. 5). Jako první transakci do bloku vždy přidává coinbase transakci, ta slouží v případě úspěchu k vyplacení odměny na těžařovu peněženku. Když je kandidát na blok sestaven, přichází na řadu hledání řešení Proof-of-Work úpravou pole nonce a hashováním hlavičky bloku dvojitou hashovací funkcí SHA-256 tak, aby výsledný hash hlavičky bloku vyhovoval obtížnosti. Jestliže těžař uspěje a nalezne správné řešení, rozešle jej ostatním uzlům a získá odměnu v podobě nově emitovaných bitcoinů a transakčních poplatků. Pokud nalezne řešení dříve někdo jiný, transakce zahrnuté v bloku jsou potvrzené, těžební uzel si je zkontroluje, vymaže ze svého mempoolu a začne pracovat na řešení dalšího bloku. [7] [16]



Obrázek 5 Merkle Tree (vlastní zpracování) [16]

Každý blok obsahuje pole obtížnost, které musí vyhovovat. Obtížnost je v bitcoinové síti globální dynamický parametr ovlivňující dobu trvání nalezení řešení pro blok. To je obtížností dáno v průměru jednou za deset minut v závislosti na velikosti výpočetního výkonu v síti. Obtížnost se s narůstajícím výkonem zvyšuje nebo naopak snižuje. [17]

Pro obtížnost platí formule:
*Nová obtížnost = Stará obtížnost * (celkový čas za posledních 2016 bloků / 20160 minut)*

3.1.1 Příklad těžby

Pro názorný příklad byl vybrán již vytěžený blok s pořadovým číslem 123 456.
Hash bloku: *0000000000002917ed80650c6174aac8dfc46f5fe36480aaef682ff6cd83c3ca*

- Verze: *1 (dec) → 0x01 (hex)*
- Hash předchozího bloku:
  0000000000000b60bc96a44724fd72daf9b92cf8ad00510b5224c6253ac40095 (hex)
- Merkle Root hash:
  0e60651a9934e8f0decd1c5fde39309e48fca0cd1c84a21ddfde95033762d86c (hex)
- Čas: *1305200806 (dec) → 0x4dcbc8a6 (hex)*
- Cíl: *443192243 (dec) → 0x1a6a93b3 (hex)*
- Nonce: *2436437219 (dec) → 0x913914e3 (hex)*

Hlavička bloku je 80 bajtů dlouhý řetězec složený z: verze (4 B) + hash předchozího bloku (32 B) + Merkle Root hash (32 B) + čas (4 B) + cíl (4 B) + nonce (4 B) s využitím architektury uspořádání bajtů little-endian.

Každý blok má uložený dynamický parametr cíl ve zkrácené verzi 4 bajtů, v tomto případě *1a6a93b3*. Cíl se dosazuje do vzorce *c * 2 **(8*(e – 3))* [17]

Cíl pro obtížnost
c = 0x6a93b3;
e = 0x1a;
*0x6a93b3 * 2 **(8*(0x1a – 3)) =*
0000000000006a93b300000000000000000000000000000000000000000000

Sestavení hlavičky bloku s noncí 0

„01000000“ +

„9500c43a25c624520b5100adf82cb9f9da72fd2447a496bc600b000000000000“ +

„6cd862370395dedf1da2841ccda0fc489e3039de5f1ccddef0e834991a65600e“ +

„a6c8cb4d“ +

„b3936a1a“ +

„00000000“

Hash hlavičky bloku s noncí 0

010000009500c43a25c624520b5100adf82cb9f9da72fd2447a496bc600b0000000000006cd862370395dedf1da2841ccda0fc489e3039de5f1ccddef0e834991a65600ea6c8cb4db3936a1a00000000

Hashování hlavičky bloku s noncí 0

SHA256(SHA256(*010000009500c43a25c624520b5100adf82cb9f9da72fd2447a496bc600b0000000000006cd862370395dedf1da2841ccda0fc489e3039de5f1ccddef0e834991a65600ea6c8cb4db3936a1a00000000))* s kódováním little-endian

Výsledek nevyhovuje cíli

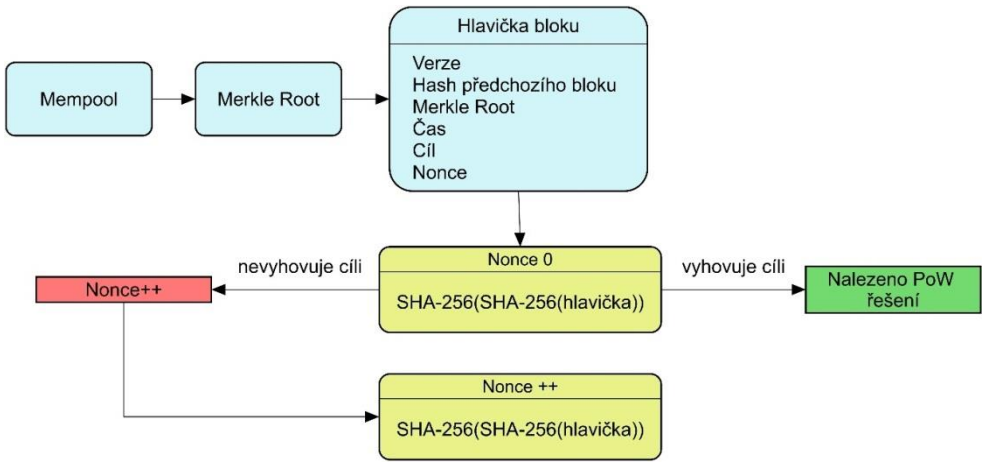
66637f4d9166fb477548a67f5f05d9bde2b7f30fd57b21661ca537723422dbc7 > 0000000000006a93b3000000000000000000000000000000000000000000000

Hashování hlavičky bloku s noncí 2 436 437 219

SHA256(SHA256(*010000009500c43a25c624520b5100adf82cb9f9da72fd2447a496bc600b0000000000006cd862370395dedf1da2841ccda0fc489e3039de5f1ccddef0e834991a65600ea6c8cb4db3936a1ae3143991))* s kódováním little-endian

Výsledek vyhovuje cíli

0000000000002917ed80650c6174aac8dfc46f5fe36480aaef682ff6cd83c3ca < 0000000000006a93b3000000000000000000000000000000000000000000000



Obrázek 6 Schéma těžby (vlastní zpracování)

3.2 Nákup a prodej

3.2.1 Burza a směnárna

Kryptoměnová burza funguje jako každá jiná na principu nabídky a poptávky. Uživatel si vytvoří na tradiční centralizované burze účet, kde bude nucen ověřit svou identitu pomocí kopie průkazu totožnosti a v některých případech i výpisem z bankovního účtu, jelikož společnosti provozující burzy se musí řídit stále přísnějšími směrnicemi známými jako KYC (Know Your Customer) vyžadujícími identifikaci svých zákazníků kvůli možnému riziku praní špinavých peněz. [18] Verifikace není nutná v případě burz, kde se směňují kryptoměny za kryptoměny. Po vytvoření a ověření účtu si na něj uživatel může převést tradiční měnu nebo kryptoměnu. Pro účet se vygeneruje bitcoinová adresa pro potřebné transakční operace. Soukromý klíč této adresy spravuje a vlastní třetí osoba, a sice provozovatel burzy, proto se doporučuje zde kryptoměnu držet pouze po dobu nezbytně dlouhou.

Alternativa burzy je směnárna, ta má narozdíl od burzy pevně daný kurz, za který lze bitcoin nakoupit či prodat a není zde žádná možnost smlouvání. Tento kurz je zpravidla o 10-20% vyšší než na burze. Vše je velmi jednoduché, na stránce směnárny zadáte množství BTC, které chcete nakoupit, emailovou adresu a bitcoinovou peněženku pro příjem. Poté stačí jen převést požadovanou částku v tradiční měně na účet směnárny a potvrdit aktuální kurz. Do 25 000,- Kč ze zákona nemusí uživatel směnárny provádět ověření totožnosti.

Pro vyhnutí se verifikaci a zachování soukromí lze využít decentralizovaných burz. Ty fungují jako takové tržiště, kde se setkává nákupce s prodejcem a mezi sebou si přímo dohodnou způsob obchodu. Jednou z takových burz je například Bisq. Tento plně

decentralizovaný software se po instalaci a spuštění připojí k ostatním uzlům přes síť Tor a ihned získá seznam všech aktuálních nabídek. V případě nákupu stačí vybrat nabídku a zahájit obchod. Kupující bude vyzván k zaslání Bisq poplatku a bezpečnostního depozitu na 2:2 multisignature adresu (soukromý klíč vlastní prodávající i kupující), která slouží jako escrow, z toho vyplývá, že i kupující musí vlastnit nějaké množství BTC k vratným bezpečnostním depozitům při nakupování na Bisq. Prodávající rovněž zašle poplatek, dohodnuté množství v BTC a bezpečnostní poplatek (ten může být z bezpečnostního hlediska až několikanásobně vyšší než prodávané množství BTC) na multisignature adresu. Kupující provede platbu dohodnutým způsobem, ke které přiloží ID obchodu a potvrdí, že platbu odeslal. Protistrana potvrdí, že platbu obdržela a z multisignature adresy se uvolní smluvené množství BTC společně s vratnými bezpečnostními depozity. V případě, že by se rozhodla jedna strana podvádět, je přizván refund agent, ten po předložení důkazů rozhodne, která strana je v právu a tu poté odškodní z Bisq poplatků. Toto se ovšem děje jen zřídka, kvůli bezpečnostním depozitům jsou účastníci obchodu motivováni nepodvádět.

3.2.2 Bitcoin ATM

Bitcoin ATM je dalším ze způsobů nákupu či prodeje bitcoinu, který rovněž nevyžaduje verifikaci uživatele do 25 000,- Kč a vzhledem k tomu, že bankomat pracuje s tradiční měnou v hotovosti, se tento způsob stává do výše uvedené částky anonymním. Rozmístění bankomatů lze zjistit dle mapy Bitcoin ATM v České republice. [19] Nevýhodou je vyšší kurz oproti burzám, menší dostupnost a v případě směny na české koruny i poměrně zdlouhavý proces oproti tradičním bankomatům, které peníze vydají téměř okamžitě.

Pro nákup bitcoinu stačí do bitcoinmatu naskenovat QR kód bitcoinové adresy, kam bude částka v BTC odeslána a vložit požadovanou hotovost. Pokud kupující žádnou bitcoinovou adresu nevlastní, systém mu k tomuto účelu nabídne možnost vytištění papírové peněženky.

Prodej bitcoinu v bankomatu funguje tak, že prodávající zadá, jakou částku chce směnit a bankomat mu vytiskne lístek se dvěma QR kódy. Jeden slouží jako bitcoinová adresa pro příjem částky v BTC a druhý jako heslo pro budoucí výběr hotovosti. Transakce musí být odeslána do 45 minut a musí získat minimálně jedno potvrzení. Jakmile je transakce potvrzena, prodejce naskenuje QR kód pro výběr a je mu vyplacena hotovost. Celý tento proces zabere zhruba 15 až 30 minut v závislosti na nastavené výši poplatku síti za odchozí transakci.

3.3 Služby

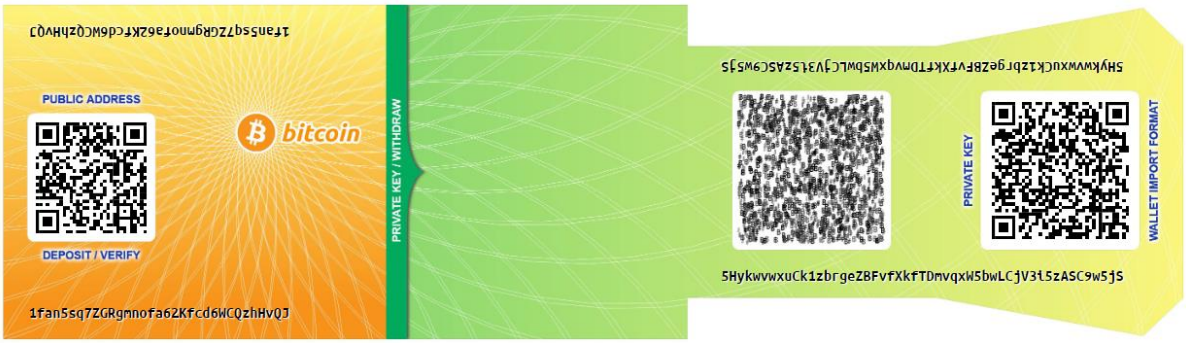
Posledním způsobem získávání bitcoinů je formou platby za poskytnuté služby. Čím dál tím více obchodníků a firem začíná za svůj produkt akceptovat platby v kryptoměně. Mezi největší firmy v České republice patří internetový obchod Alza, ale i mnoho menších podniků jako jsou například restaurace, kavárny, hotely nebo i dokonce oční klinika. Dle coinmap je Praha na prvním místě na světě v počtu poskytovatelů služeb, kteří přijímají platby formou kryptoměn. [20]

Poskytovatelé služeb a obchodníci nejčastěji využívají k přijímání plateb nějakou kryptoměnovou platební bránu. Jde o službu třetí strany, se kterou mají poskytovatelé služeb smlouvu. Zákazník odešle platbu na platební bránu a ta je ihned považována za provedenou. Platební brána poté vyplácí finanční prostředky v dohodnuté formě na účet či peněženku poskytovatelům služeb. Zákazník může k platbě využít například litecoin a platební brána jej v aktuálním kurzu vyplatí protistraně v bitcoinu nebo nějaké z tradičních měn jako jsou EUR či USD. [21]

4 Způsoby uložení bitcoinů

4.1 Papírová peněženka

Jak z názvu vyplývá, papírová peněženka je jednoduše kus vytištěného papíru (obr. 7), na kterém se nachází bitcoinová adresa a soukromý klíč vytištěné ve WIF formátu s odpovídajícím QR kódem, tímto je možné papírovou peněženku pohodlně naskenovat QR scannerem do některé z mobilních peněženek a provádět transakční operace. Výhodou papírové peněženky je, že se jedná o cold storage typ, to znamená, že soukromý klíč není nikde digitálně uložen a bitcoiny dané adresy jsou v bezpečí před kybernetickým útokem. Osoba vlastnící peněženku s ní může nakládat defacto jako s peněžní bankovkou. Nevýhodou je, že ztráta papírové peněženky bez příslušné zálohy jejího soukromého klíče se rovná nenávratné ztrátě jako v případě právě zmíněné bankovky. Papírovou peněženku je možné vytvořit například pomocí webového generátoru jako je bitcoinpaperwallet, který umožňuje náhodné vytvoření soukromých klíčů a k nim příslušných bitcoinových adres. Při vytváření a tištění papírové peněženky je doporučeno dodržet bezpečnostní postup, a to nejlépe na čistém operačním systému, který běží z USB disku, aby se předešlo odhalení soukromého klíče spywarem a následným tiskem na tiskárně, která nemá přístup k internetu. [22]



Obrázek 7 Papírová peněženka [22]

4.2 Softwarové peněženky

4.2.1 Počítačová peněženka

Počítačová neboli desktopová peněženka je softwarová aplikace stažená a nainstalovaná na počítačovém zařízení, která soukromé klíče ukládá přímo na pevném disku většinou v šifrované podobě. Uživatel se zde nemusí spoléhat na žádnou třetí stranu a ze softwarových peněženek se jedná o nejbezpečnější typ, avšak stále se připojuje k internetu, čímž se stává potencionálně zranitelnou.

Desktopová peněženka má dva typy, a to full node klient (plný uzel) a light node klient (odlehčený uzel). Plný uzel stahuje a udržuje celou kopii databáze blockchain na disku aktuální, to je pro běžného uživatele kapacitně náročnější řešení, jelikož bitcoinový blockchain má v době psaní této práce okolo 300 GB a stále se rozrůstá, výhoda plného uzlu je v bezpečnosti, nemusí se spoléhat na žádnou třetí stranu. Oproti tomu odlehčený klient je pro běžného uživatele přívětivější, místo celého blockchainu stahuje pouze hlavičky bloků a využívá Simplified Payment Verification (SVP). SVP umožňuje ověřování transakcí bez nutnosti mít celou kopii blockchainu staženou. Spoléhá se na plné uzly v bitcoinové síti, kterých se na vše dotazuje, toto s sebou však nese jistá bezpečnostní rizika, jelikož se zde zapojuje třetí strana. [23]

4.2.2 Mobilní peněženka

Mobilní peněženka je oproti desktopové jednodušší a méně kapacitně náročná aplikace nainstalovaná na zařízení. Lze ji mít neustále u sebe a snadno využívat k všedním platbám kdekoliv. Jedná se o typ peněženky hot wallet, to znamená, že je neustále online připojená k internetu, čímž se stává potencionálně zranitelnou. Mobilní peněženky využívají SVP, protože z kapacitního hlediska mobilních zařízení plný uzel nedává smysl. Ukládání soukromých klíčů je řešeno operačním systémem zařízení, který má na citlivé informace, jako jsou kryptografické klíče speciálně vyhrazené místo Keystore u Androidu [24] a Keychain u iOS [25] .

4.2.3 Webová peněženka

K webovým peněženkám může uživatel přistupovat z jakéhokoliv zařízení a prohlížeče, protože jsou neustále online na serverech provozovatelů. Soukromé klíče spravuje rovněž provozovatel peněženky a uživatel k nim v drtivé většině případů nemá

vůbec přistup. Jejich bezpečnost závisí na zabezpečení serveru a může zde nejsnadněji dojít k jejich odcizení a tím k nenávratné ztrátě bitcoinu, proto se tento způsob uložení řádí k nejméně bezpečným. Vzhledem k tomu, že soukromé klíče jsou vlastněny třetí stranou, může dojít k omezení či pozastavení transakčních operací nebo úplnému zamezení přístupu uživateli k peněžence ze strany provozovatele.

Webová peněženka se nejčastěji používá tam, kde dochází ke směně kryptoměn za jiné kryptoměny či fiat měny a většinou se zde aktiva uchovávají pouze po dobu nezbytně dlouhou, poté se přesouvají do peněženek s vyšší mírou zabezpečení.

4.3 Hardwarová peněženka

Hardwarová peněženka je speciální typ peněženky, která uchovává soukromé klíče v zabezpečeném hardwarovém zařízení. Stejně jako u papírové peněženky se jedná o cold storage typ, jelikož soukromé klíče se nikde nenacházejí online a nelze je z hardwarového zařízení vyexportovat v plain textu. Dosud nejsou žádné známé případy odcizení kryptoměn z hardwarových peněženek, čímž se stává nejbezpečnější peněženkou současnosti.

Mezi nejznámější a nejvíce rozšířené výrobce hardwarových peněženek patří Trezor a Ledger. Všechny hardwarové kryptopeněženky jsou svými atributy stejné nebo velice podobné a liší se pouze způsobem provedení.

Trezor je v České republice asi nejrozšířenější hardwarová peněženka, a to zejména proto, že se jedná o český výrobek, který v současné době podporuje více než tisíc kryptoměn a celá platforma je v češtině. Jde o malé hardwarové zařízení (obr. 8), které se připojuje přímo do počítače pomocí USB-C kabelu. Po připojení do počítače si zařízení automaticky stáhne plugin s názvem Trezor Bridge, ten umožňuje komunikaci s online peněženkou MyTrezor, ta je vyvinuta speciálně pro toto zařízení a nabízí stejné služby jako jakákoliv jiná peněženka s tím rozdílem, že podepisování probíhá v samotném zařízení. Po instalaci pluginu požaduje Trezor vytvoření PINu, který slouží k ochraně zařízení a potvrzování transakcí. Přihlašování funguje tak, že se na displeji Trezoru zobrazí 3x3 tabulka s čísly, stejná tabulka se zobrazí i na monitoru počítače, kde jsou místo čísel jen otazníky a uživatel kurzorem myši zadává PIN dle čísel na Trezoru, čímž je zařízení chráněno proti keyloggeru zaznamenávajícím činnost klávesnice. Každé špatné zadání PINu vede k tomu, že se čas dalšího pokusu zdvojnásobuje, to zařízení chrání před pokusy o uhodnutí PINu. Další důležitou věcí při instalaci je vytvoření zálohy neboli Recovery Seedu. Standartně se jedná o 12 (nebo 18 a 24) náhodně vybraných anglických slov

umožňující obnovu peněženky při resetovaní, poškození nebo ztracení zařízení. Důrazně se doporučuje provést zálohu Seedu na papír, jelikož z bezpečnostního hlediska při záloze na zařízení s přístupem k internetu může dojít k jeho prozrazení. Při vytváření zálohy je ovšem ještě možné vytvořit takzvanou Passphrase Encryption, to je jednoduché heslo, bez kterého nebude umožněno provést obnovu zálohy.

Obrázek 8 Hardwarová peněženka Trezor [26]

5 Alternativní kryptoměny

Pojmem alternativní kryptoměny jsou myšleny všechny kryptoměny, které vznikly po Bitcoinu, ať už jako jeho klon, nebo jako úplně nové měny se svými vlastními zdrojovými kódy. V dnešní době existují tisíce měn, jejichž přehled je dostupný například na stránce coinmarketcap, které se snaží svými vlastnostmi cílit na specifická odvětví využití. [27]

V této kapitole popisuji alternativní způsoby dosažení konsensu k Proof-of-Work a kryptoměny implementující různé anonymizační technologie, které by bylo vhodné využít k přenosu hodnoty bez možnosti vystopovat či trasovat transakce uživatelů sítě.

5.1 Alternativní způsoby konsensu a získávání kryptoměn

Kryptoměny jsou decentralizované a k validaci transakcí nepoužívají žádnou centrální autoritu, která by o nich rozhodovala. Nicméně absencí centrální autority vzniká problém, komu mohou uzly sítě důvěřovat. Tento problém je řešen právě konsensním algoritmem, ten je nenahraditelným jádrem každého blockchainu zabezpečující dosažení shody všech uzlů sítě. Od vzniku Bitcoinu, který jako konsensní algoritmus používá právě Proof-of-Work, přicházejí vývojáři se stále novými alternativními algoritmy ve snaze efektivně a ekologicky zabezpečit fungování sítě. Principem všech algoritmů je dojít ke shodě všech uzlů v síti, že právě daný blok je ten správný a pravý. Celému procesu přidávání bloků do blockchainu předchází forma jisté investice do sítě, ať už je to výpočetním výkonem nebo mincemi samotnými. K této investici udržující síť decentralizovanou, bezpečnou a agilní, musí být uzel motivován, a to odměnou v podobě nově emitovaných mincí a transakčních poplatků.

5.1.1 Proof-of-Stake

Nejrozšířenější alternativou k distribuovanému konsensu Proof-of-Work je právě Proof-of-Stake (v překladu „důkaz o vsazení“ - PoS) algoritmus. U PoS konsensu nejsou v síti těžaři využívající svůj výpočetní výkon k vytěžení nového bloku, místo nich jsou zde takzvaní validátoři, ti netěží, ale vytváří. Validátorem se může stát jakýkoliv uzel v síti, který uzamkne svoji kryptoměnu jako depozit, čímž získá právo na ověřování transakcí. Čím větší množství kryptoměny validátor uzamkne, tím větší má šanci být vybrán se stát tvůrcem a vytvořit nový blok, za který získá odměnu. Odměna je většinou jen ve formě poplatků

za zahrnuté transakce v bloku, protože PoS kryptoměny bývají předtěžené a žádné nové mince se negenerují. Pokud se validátor rozhodne skončit, jednoduše svoji měnu znovu odemkne a může s ní nakládat dle libosti. Dvě nejčastější metody vybírání tvůrce jsou náhodný výběr a výběr dle stáří mince, nicméně kryptoměny využívající PoS si tyto pravidla pozměňují a vytváří svojí vlastní verzi PoS. [28]

Náhodný výběr tvůrce spočívá v tom, že algoritmus v síti vybere náhodně validátora s nejnižší hodnotou hashe pro blok společně s nejvyšším množstvím uzamčené kryptoměny.

Metoda výběru dle stáří mince vybírá validátory podle doby uzamčení kryptoměny. Doba stáří je počítána z počtu uzamčených mincí krát počet uzamčených dnů. Pokud je validátor vybrán jako tvůrce, tak se po vytvoření nového bloku jeho doba stáří mince resetuje na nulu a musí znovu čekat, než na něj přijde řada. Výhoda této metody je v tom, že uspět může i validátor s nižším depozitem. [29]

PoS patří k nejekonomičtějším způsobům dosažení konsensu a v porovnání s PoW i teoreticky méně centralizovaný, s čímž je spojena i nižší hrozba 51% útoku na síť, avšak velké množství uživatelů má své mince uschované ve webových peněženkách burz, to s sebou přináší riziko. Burzy se mohou domluvit a prostředky svých uživatelů propůjčit třetím stranám k poškození sítě.

5.1.2 Proof-of-Burn

Proof-of-Burn (v překladu „důkaz o pálení“ – PoB) algoritmus funguje na principu využívání kryptoměny jako „paliva“ pro těžbu. Těžař pošle kryptoměnu na speciální kryptoměnovou adresu určenou pro pálení mincí a výměnou získá právo pro těžení a ověřování transakcí. Tato adresa je generována automaticky a soukromý klíč není vlastněn nikým, kryptoměna na této adrese se stává navždy neutratitelnou = spálenou. K pálení může být využita kryptoměna fungující na stejném nebo i jiném blockchainu, odměnou jsou ale vždy mince PoB blockchainu. Stejně jako platí u PoW, čím více výpočetního výkonu těžař má, tím větší má šanci vytěžit nový blok, tak i u PoB platí, čím více kryptoměny těžař spálí, tím více má pomyslného virtuálního výpočetního výkonu a větší šanci být vybrán jako tvůrce nového bloku. Tento virtuální výpočetní výkon s každým novým vytvořeným blokem slábne, stejně jako zastarává výpočetní technologie, proto je nutné provádět investiční „upgrade“ v podobě pálení dalších mincí, toto zabezpečuje a udržuje síť agilní. [30]

PoB je samo o sobě energeticky nenáročné řešení dosažení konsensu, nicméně mu musí předcházet použití nějakého jiného algoritmu (nejčastěji právě PoW) k získání kryptoměny k pálení.

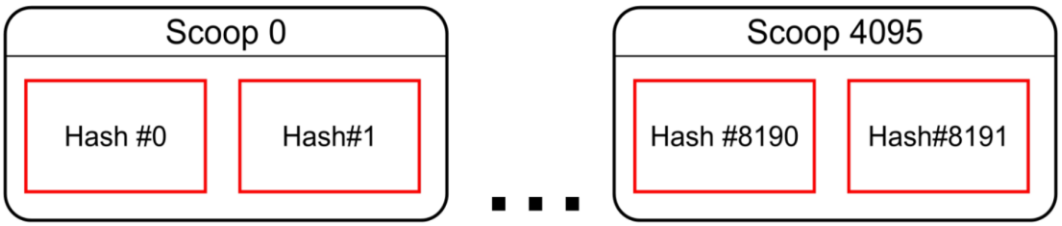
5.1.3 Proof-of-Capacity

Proof-of-Capacity (v překladu „důkaz o kapacitě“ – PoC) je konsensní algoritmus využívající kapacitního místa na disku. Stejně jako u předchozích způsobů i zde platí, čím více tím lépe. Čím více má těžař k dispozici kapacitního prostoru, tím má větší šanci vytěžit blok a získat odměnu. Celý princip PoC se skládá ze dvou částí, a to z plottingu a těžby.

Plotting vytváří na disku kapacitně náročný data set hodnot nonce hashováním dat včetně adresy uzlu, tím má každý uzel svůj unikátní data set. Každá nonce obsahuje 8192 hashů řazených po dvojicích za sebou do takzvaných scoopů, těch nonce obsahuje od 0 do 4095 (obr. 9). Celý proces plottingu může trvat i týdny v závislosti na dostupné kapacitě, čím vetší je kapacita, tím více má těžař vypočítaných noncí.

Druhá část je těžba, kde se vypočítá číslo scoopu od 0 do 4095, toto číslo se použije pro scoop všech noncí uložených na disku a z každého se vypočítá čas označovaný jako deadline. Po vypočítání hodnot deadlinů všech scoopů noncí se vybere ten s nejnižší hodnotou v sekundách a odešle se do sítě. Deadline reprezentuje čas, který musí uplynout od vytvoření posledního bloku předtím, než je těžaři povoleno vytvořit nový blok. Pokud má těžařův deadline nejnižší čas v sekundách, dostane od sítě povolení k vytvoření bloku, za který získá odměnu. [31]

Výhody tohoto způsobu oproti PoW je levná pořizovací cena kapacitních úložišť v porovnání s cenou ASIC minerů a malá spotřeba energie, jelikož není třeba dělat neustále se opakující energeticky náročné výpočty.



Obrázek 9 Proof-of-Capacity nonce (vlastní zpracování) [31]

5.2 Monero

Monero je decentralizovaná open-source alternativní kryptoměna založená na protokolu CryptoNote, ten je zaměřen na úplnou anonymitu uživatelů v reakci na ne zcela anonymní Bitcoin.

Monero vzniklo v dubnu roku 2014 a jeho vývojářský tým zůstává z větší části v anonymitě. Na rozdíl od většiny alternativních kryptoměn není klonem Bitcoinu a má svůj zcela vlastní kód, jediné, co mají společné, je konsensní algoritmus Proof-of-Work. Místo Hashcash ale využívá CryptoNight, který je náročný na paměť, čímž znemožňuje těžbu ASIC minerů a tím pádem velkých těžebních společností, to je prioritou vývojářů, ti chtějí, aby hlavně běžní uživatelé mohli využívat svůj výpočetní výkon k těžbě. Použitá hashovací funkce je zde Keccak-256, ta se řadí do skupiny SHA-3. Každý nový blok je vytěžen průměrně jednou za 2 minuty a oproti fixní velikosti bloku Bitcoinu má Monero velikost dynamickou. Velikost se dynamicky mění s počtem nepotvrzených transakcí v síti, čím více jich je, tím je blok větší a poplatky za transakce nižší nebo naopak. Toto řeší problém škálovatelnosti, který Bitcoin má. Odměna za blok činí 5 monero (XMR) + transakční poplatky a měna nemá konečný počet mincí, místo toho se odměna sníží na 0,6 XMR poté, co se se dostane do oběhu 18 132 000 mincí. Rozdílem oproti bitcoinu je také zaměnitelnost mincí monera. Bitcoinové transakce lze z blockchainu trasovat až k úplně první coinbase transakci a není možné jednotlivé mince zaměnit, tím je zpětně možné zjistit, že daný obnos v bitcoinu byl například v minulosti použit k páchání trestné činnosti, praní špinavých peněz apod. Jako u běžných fiat peněz lze zaměnit jednu minci za druhou, monero se svým soukromým blockchainem má tuto možnost také, tím jsou monero transakce netrasovatelné. [32]

Monero v současnosti využívá tři klíčové technologie zajišťující anonymitu transakcí a samotných uživatelů sítě:

- Ring Signature
- RingCT
- Stealth Adresses

Ring Signature

Ring Signature (kruhový podpis) je typ digitálního podpisu, který může být vytvořen jakýmkoliv členem ze skupiny, kde každý vlastní klíč. Není zpětně možné zjistit, který klíč

ze skupiny byl použit k vytvoření podpisu. Tímto je odesílatel transakce chráněn a zůstává tak v naprosté anonymitě. [33]

RingCT

Ring Confidential Transaction (tajná kruhová transakce) implementace vylepšuje kruhové podpisy a přináší ještě větší míru anonymity. Skrývá přenášené množství XMR a počáteční i cílovou destinaci. [34]

Stealth Adresses

Monero využívá čtyři klíče místo obvyklých dvou a sice:

- Public view key
- Public spend key
- Private view key
- Private spend key

Adresa Monera začíná číslicí 4 a je složena z 95 znaků, které v sobě mají zakomponovány public view key a public spend key. Odesílatel transakce použije tyto dva klíče z adresy příjemce k vytvoření unikátního jednorázového veřejného klíče pro výstup – Stealth Adress (skrytá adresa). Příjemce poté prohledá Monero blockchain svým private view key, když je výstup detekován a načten peněženkou příjemce, vypočítá se k jednorázovému veřejnému klíči jednorázový soukromý klíč a pomocí private spend key je možné výstup utratit. Private view key může být poskytnut třetí straně, ta pak může auditovat všechny příchozí i odchozí transakce adresy, zatímco private spend key, stejně jako soukromý klíč u Bitcoinu, slouží k vytváření digitálních podpisů a utrácení kryptoměny. Stealth adress slouží k udržení příjemce v anonymitě. [35]

Monero je nejvíce rozšířenou anonymní kryptoměnou, jejíž prioritou je soukromí uživatelů, mezi kterými zajišťuje plně soukromé a nevystopovatelné transakce, tím se stává více vhodnější alternativou k páchání trestné činnosti než pseudonymní Bitcoin.

5.3 Dash

Dash je decentralizovaná open-source kryptoměna vycházející ze zdrojového kódu Bitcoinu a Litecoinu. Jak již z názvu měny Digital cash vyplývá, Dash se svými instantními a privátními transakcemi nabízí v digitálním světě stejnou funkci jako cash v reálném.

Autor kryptoměny Dash Evan Duffield si uvědomoval nedostatky Bitcoinu v oblasti anonymity a rychlosti transakcí, které se snažil řešit, bohužel jeho návrhy komunita vývojářů Bitcoinu nepřijala. V reakci na to v lednu 2014 vytvořil na základě zdrojového kódu Bitcoinu vlastní kryptoměnu. Dash využívá v blockchainu dvě vrstvy architektury. První vrstva funguje stejně jako u Bitcoinu na principu Proof-of-Work s využitím hashovacího algoritmu X11 rezistentnímu proti ASIC minerům. Těžaři vytěží blok průměrně každé 2,5 minuty a z odměny za něj získají pouze 45%. Aktuální odměna za blok činí 3,11 DASH a maximální počet mincí je pouze 18,9 milionu.

V Bitcoinové síti si jsou všechny uzly rovny, to u Dashe neplatí. Zde jsou dva druhy uzlů, a to klasické uzly, ty stejně jako u Bitcoinu ověřují transakce, a master uzly (masternodes), které tvoří druhou vrstvu. Masternodes také ověřují transakce, navíc mají ale oprávnění k vykonávání dalších funkcí, za které jim náleží, stejně jako těžařům, 45% odměny z bloku. Tento koncept přidaný k Proof-of-Work se nazývá Proof-of-Service. Aby se uzel stal master uzlem, musí vlastnit minimálně 1000 mincí DASH, plný uzel a připojení k síti. Vysoká počáteční investice zajišťuje ochranu před Sybil útokem a centralizací.

Masternodes funkce:

- Instantní transakce
- Privátní transakce
- Návrhy na vylepšení sítě

Instantní transakce

Vytěžení jednoho bloku trvá 2,5 minuty, a to je příliš dlouhá doba na potvrzení transakce. Vzhledem k tomu, že se Dash prezentuje jako cash v digitálním světě, je funkce instantních transakcí nutností. Uživatel vybere jako možnost instantní transakci, ta se za vyšší poplatek odesílá přímo masternodům, kteří hodnotu uzamknou, aby nemohlo dojít ke dvojímu utracení a potvrdí ji. Celý tento proces potvrzení trvá nejvýše několik vteřin a transakce je následně přidána do nejnovějšího bloku.

Privátní transakce

Privátní transakce zajišťují soukromí uživatelů kombinací identických vstupů více uživatelů do jedné velké transakce s více výstupy na nově vygenerované adresy uživatelů. Toto rovněž zajišťují master uzly, ty za poplatek sestavují mixovací transakce mezi uživateli. Procesem mixování je docíleno toho, že není možné zjistit, komu mince v minulosti patřily.

Návrhy na vylepšení sítě

Jak již bylo zmíněno 45% odměny je určeno pro těžaře, 45% pro masternody a zbylých 10% se vyhrazuje na rozpočet právě pro vývoj a vylepšení sítě Dash. Kdokoliv může za poplatek zveřejnit jakýkoliv návrh na zlepšení sítě. Pro návrhy poté hlasují masternody, ty takto určují směr vývoje. Pokud návrh projde, obdrží jeho autor odměnu vyplacenou v superbloku z rozpočtu pro vývoj. [36]

5.4 Zcash

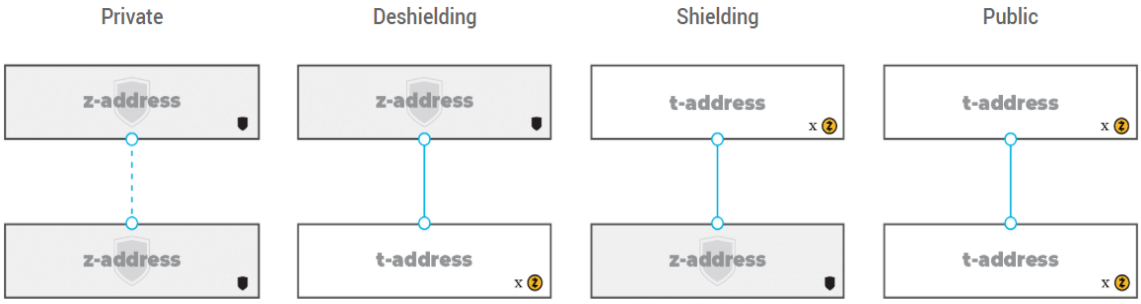
Zcash je rovněž decentralizovaná open-source kryptoměna přímo vycházející ze zdrojového kódu Bitcoinu zaměřená na ochranu soukromí uživatelů sítě.

K oficiálnímu spuštění došlo v říjnu roku 2016 a zakladatelem je Zooko Wilcox. Zcash vzhledem k tomu, že přímo vychází z Bitcoinu, se mu také velmi podobá. Využívá rovněž Proof-of-Work s algoritmem Equihash, který je velmi náročný na paměť, což jej činí rezistentním proti ASIC minerům. Kapacita bloku je 2 MB s průměrnou dobou těžby 1,25 minuty a odměnou 6,25 ZEC + transakční poplatky. Maximální počet mincí je stejný jako u Bitcoinu a to 21 milionů. Hlavní přidanou hodnotou je zde implementace zero-knowledge protokolu. Konkrétně se jedná o zn-SNARKs (zero-knowledge Succinct Non-interactive Argument of Knowledge). Protokol s nulovou znalostí je ověřovací metoda, kde jedna strana prokazuje té druhé, že tvrzení je pravdivé bez toho, aniž by o něm odhalila jakékoliv informace. Monero používá k zajištění soukromí ring signatures a stealth adresy, Dash mixuje transakce uživatelů a Zcash mění způsob, jakým jsou transakční data sdílena. Nicméně tato funkce není implicitně nastavena a uživatel si jí musí zvolit sám. [37]

Zcash má dva typy adres a sice transparentní, které začínají písmenem „t“ a privátní začínající písmenem „z“. S tímto jsou také spojeny typy transakcí (obr. 10).

Privátní transakce (z-z) zajišťuje anonymitu obou stran. V blockchainu se tato transakce zobrazí, ale je v ní skryto množství, zbytek, odesílatel i příjemce a viditelný je pouze transakční poplatek síti. Součástí této transakce je také memo pole, to slouží autorovi k odeslání krátké zprávy příjemci v rámci transakce, ta je kompletně šifrována a může si ji zobrazit pouze příjemce či strana disponující viewing key. Viewing keys fungují obdobně jako u Monera, vlastní je majitelé privátních adres, kteří je mohou poskytovat třetím stranám k auditu. Transakce z privátní adresy na transparentní (z-t) skrývá transakční vstup včetně odesílatele a zbytku, kde na výstupu je viditelný pouze příjemce a hodnota. V opačném případě (t-z) je to jen naopak, viditelný je vstup a skrytý výstup. Posledním typem je

transakce mezi transparentními adresami, ta funguje úplně stejně jako u Bitcoinu, je znám odesílatel, příjemce, hodnota i zbytek. [38]



Obrázek 10 Zcash - typy transakcí [39]

6 Metodika vyhledávání kryptoměny Bitcoin v počítačovém zařízení

Cílem kapitoly Metodika vyhledávání kryptoměny Bitcoin v počítačovém zařízení je navrhnout a prakticky implementovat postup pro detekci vybraných peněženek a jejich záloh v počítačovém zařízení. Kapitola se skládá z následujících částí:

1. Analýza bitcoinových peněženek
2. Návrh metodiky pro vyhledávání analyzovaných peněženek
3. Praktická implementace metodiky

6.1 Analýza bitcoinových peněženek

Tato kapitola obsahuje analýzu a detailní popis následujících bitcoinových peněženek:

- Bitcoin Core 0.19.0.1
- Electrum 3.3.8
- Bither 1.4.7

6.1.1 Bitcoin Core

Bitcoin Core je originální bitcoinová peněženka a výtvor samotného Satoshi Nakamoto spuštěná v roce 2009 s bitcoinovým blockchainem. Jedná se o open-source projekt, který ke svému fungování využívá full node s lokálně uloženou kopií blockchainu. Při každém spuštění se klient automaticky připojuje k ostatním uzlům přímo a získává od nich aktualizace. Validace transakcí a sdílení dat funguje přesně tak, jak byl Bitcoin navržen – bez nutnosti využívat a důvěřovat třetím stranám, to Bitcoin Core peněženku řadí mezi nejdůvěryhodnější a nejbezpečnější desktopové peněženky, avšak její bezpečnost stále závisí na zabezpečení operačního systému a internetové sítě.

Podporované operační systémy	Windows 7 a vyšší (pouze 64-bit), OS X, Linux
Podporované kryptoměny	pouze Bitcoin
Typ klienta	full node
Programovací jazyk	C++
Potřebná kapacita na disku	300 GB
Generování klíčů	Deterministicky z extended private masterkey

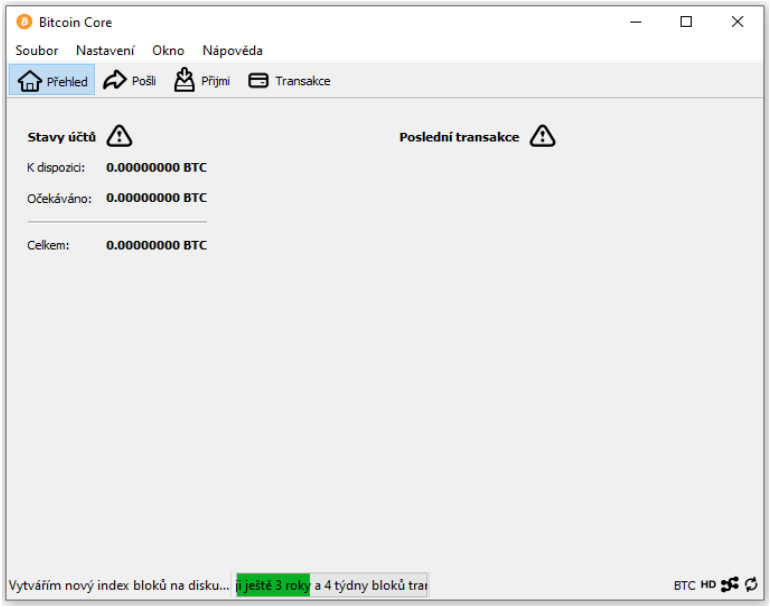
Tabulka 3 Bitcoin Core – přehled

Nastavení Bitcoin Core

1. Stažení – Z oficiální stránky Bitcoin Core. [40]

2. Instalace – Po stažení a spuštění instalačního souboru je uživatel dotázán na cílové místo instalace klienta, implicitně je to *C:\Program Files\Bitcoin*. S instalací klienta se vytváří v kořenovém klíčí *HKEY_CURRENT_USER\Software* podregistr *Bitcoin Core (64-bit),* ten obsahuje hodnotu *Path* s údajem umístění nainstalovaného klienta.

3. Spuštění - Při prvním spuštění klienta se uživateli zobrazí okno s cílovým umístěním data directory, implicitně v lokaci *C:\Users\"username"\AppData\Roaming\Bitcoin*, nicméně i zde má uživatel možnost cílovou destinaci změnit. Bitcoin Core data directory obsahuje všechna data, se kterými klient pracuje včetně celého bitcoinového blockchainu. Stejně jako při instalaci klienta i zde se vytváří v kořenovém klíči *HKEY_CURRENT_USER\Software* podregistr *Bitcoin\Bitcoin-Qt* obsahující hodnotu *strDataDir* s údajem umístění Bitcoin Core data directory. Po zvolení umístění je automaticky spuštěn samotný klient (obr. 11), který ihned započne synchronizaci se sítí a aktualizaci své kopie blockchainu od ostatních uzlů. Celý tento proces může trvat několik dnů, nicméně na funkci peněženky to nemá vliv a uživatel ji může bez problému využívat, zatímco se aktualizace provádí na pozadí.



Obrázek 11 Bitcoin Core klient

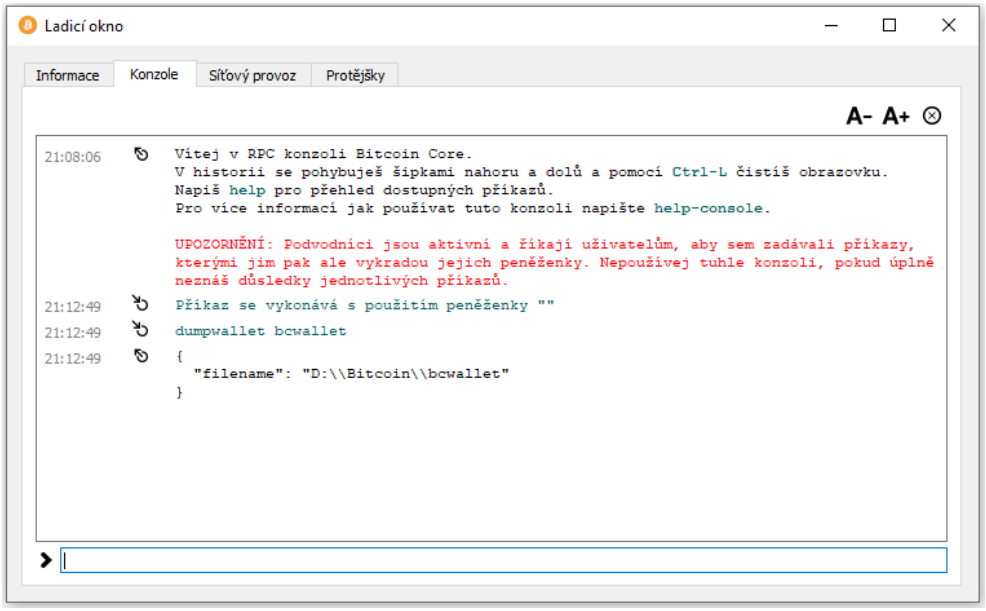
Záloha peněženky

Záloha peněženky se vytváří automaticky při prvním spuštění klienta ve zvolené lokaci data directory v podsložce *wallets*. Záloha je embedded databáze BerkeleyDB a má pevně daný formát *wallet.dat*. Pokud je soubor z výchozího umístění smazán, přesunut či přejmenován, klient při spuštění vytvoří zálohu pro novou peněženku. Soubor po vytvoření obsahuje velké množství rezervovaných adres, ty jsou předgenerovány z jediného private masterkey a v budoucnu využívány uživatelem při generování nové adresy v klientu pro příjem či zbytkovou transakci.

Záloha může být šifrována uživatelským heslem, ovšem tato funkce není implicitní. V případě, že je peněženka uživatelským heslem chráněna, jsou šifrovány pouze soukromé klíče, je tedy z importu zálohy možné zjistit stav účtu, transakční historii a aktivní adresy, pokud ale záloha šifrovaná není, lze ji i se soukromými klíčí vyexportovat v plain textu.

Konzole Bitcoin Core

Bitcoin Core konzole, která je součástí klienta, nabízí velké množství pokročilých možností včetně exportu všech adres s jejich soukromými klíči v plain textu. K tomu slouží příkaz *dumpwallet „filename“* (obr. 12), případně *dumpprivkey „adresa“* pro zobrazení soukromého klíče pro jednu konkrétní adresu. Pokud je záloha šifrována, oba příkazy vyžadují uživatelské heslo.



Obrázek 12 Bitcoin Core konzole

Obrázek 13 Exportované adresy a soukromé klíče ze zálohy Bitcoin Core peněženky

6.1.2 Electrum

Electrum je jednoduchá a velmi uživatelsky přívětivá open-source softwarová peněženka dostupná nejen pro desktopová zařízení, ale i pro mobilní. Peněženka využívá Simplified Payment Verification a při každém jejím spuštění se náhodně připojuje k některým z Electrum serverů, kterých se dotazuje na informace a zároveň jim předává autorem podepsané transakce při jejich realizaci. Tento způsob umožňuje, že není nutné celou databázi blockchain uchovávat lokálně. Electrum servery nemají v žádném případě přístup k žádným ze soukromých klíčů uživatele, nicméně dotazováním se na stav adres peněženky jim uživatel odhaluje svojí IP adresu.

Podporované operační systémy	Windows 7 a vyšší, OS X, Linux, Android, iOS
Podporované kryptoměny	pouze Bitcoin
Typ klienta	light node
Programovací jazyk	Python
Potřebná kapacita na disku	150 MB
Generování klíčů	Deterministicky z mnemonické fráze

Tabulka 4 Electrum - přehled

Nastavení Electrum

1. Stažení – Z oficiální stránky Electrum. [41]

2. Instalace – Po spuštění instalačního souboru je uživatel dotázán na cílové místo instalace klienta, implicitně je to *C:\Program Files (x86)\Electrum*. Data directory se nachází v lokaci *C:\Users\"username"\AppData\Roaming\Electrum* a uživatel nemá možnost tuto výchozí lokaci změnit. Současně s tím se v kořenovém klíči registru *HKEY_CURRENT_USER\Software* vytváří podregistr *Electrum* s údajem hodnoty umístění nainstalovaného klienta.

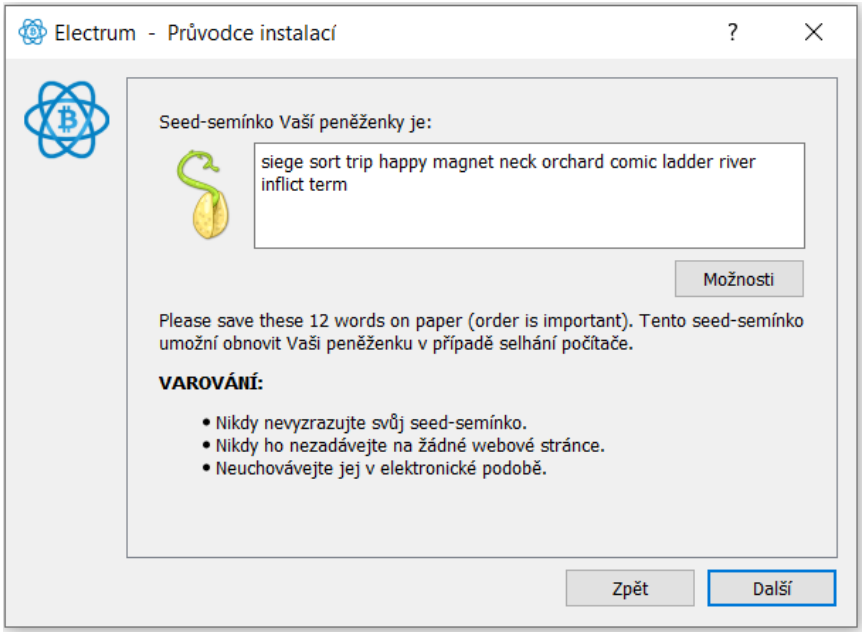
3. Spuštění – Při spuštění má uživatel možnost si vytvořit novou peněženku s vlastním či implicitním názvem *default_wallet*, popřípadě načíst zálohu již dříve vytvořené peněženky a zadat uživatelské heslo. Výchozí umístění ukládání a načítání souborů záloh peněženek je v data directory v podsložce *wallets*, nicméně tato lokace pro ukládání či načítání není pevně daná.

   Při vytváření peněženky má uživatel několik možností:

   - Standardní peněženka
   - Peněženka s dvoufázovým ověřením
   - Vícepodpisová peněženka
   - Import bitcoinových adres nebo soukromých klíčů

   Vytvořením nové peněženky se vygeneruje mnemonická fráze – seed (obr. 14) skládající se z 12 anglických slov dle standardu BIP39 s možností rozšíření o vlastní

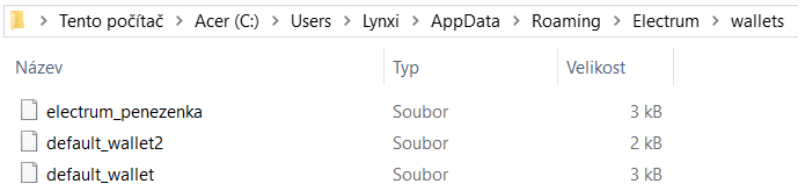
slova. [42] Seed slouží pro obnovu peněženky a generování deterministických klíčů. Lokálně umístěný soubor peněženky je vždy chráněn uživatelským heslem.



Obrázek 14 Electrum – mnemonická fráze

Záloha peněženky

Výchozí umístění zálohy peněženky je v data directory v lokaci *C:\Users\"username"\AppData\Roaming\Electrum\wallets*, ale soubory se mohou nacházet a být spouštěny z jakékoliv lokace. Soubor standardně obsahuje symetrickou AES-256-CBC šifru seedu a soukromých klíčů, které je možné dešifrovat pouze uživatelským heslem, bez něhož přístup k jakýmkoliv informacím (aktivní adresy, šifrované podoby klíčů, zůstatek apd.) peněženky není možný, v případě nálezu zálohy se tedy soubor musí stát předmětem dešifrování. Záloha dále nemá žádnou konkrétní příponu a volba názvu je ponechána uživateli (implicitně *default_wallet*).



Obrázek 15 Electrum - zálohy

6.1.3 Bither

Bither je jednoduchá open-source bitcoinová peněženka dostupná pro většinu operačních systémů včetně těch mobilních. Stejně jako Electrum i Bither je light node klient s využitím Simplified Payment Verification. Na informace se dotazuje Bither serverů, při čemž jim rovněž odhaluje uživatelovu IP adresu a předává jim podepsané transakce.

Podporované operační systémy	Windows 7 a vyšší, OS X, Linux, Android, iOS
Podporované kryptoměny	pouze Bitcoin
Typ klienta	light node
Programovací jazyk	JAVA
Potřebná kapacita na disku	120 MB
Generování klíčů	Deterministicky z mnemonické fráze, náhodně

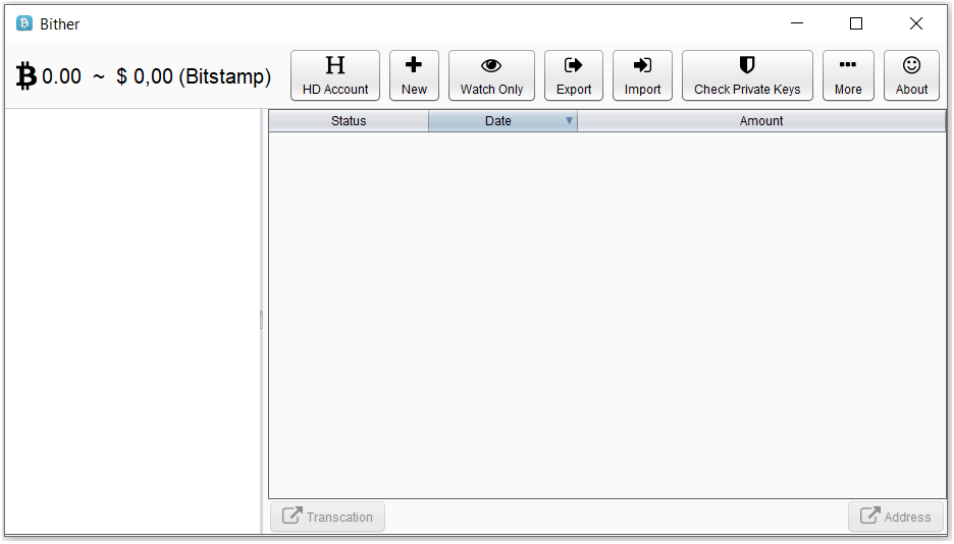
Tabulka 5 Bither - přehled

Nastavení Bither

1. Stažení – Z oficiální stránky Bither. [43]

2. Instalace – Spuštěním instalačního souboru se peněženka Bither automaticky nainstaluje do výchozí lokace *C:\Users\"username"\AppData\Roaming*, kde vytvoří soubory *JWrapper-Bither* a *Bither*. Soubor *JWrapper-Bither* obsahuje klienta peněženky a *Bither* je data directory se zálohou peněženky. Bither klient funguje pouze pokud se nachází v této pevně dané lokaci a uživatel nemá možnost ji nijak měnit. Při instalaci ani po ní Bither do registrů nezapisuje žádné využitelné hodnoty.

3. Spuštění – Při spuštění se uživateli zobrazí grafické rozhraní (obr. 16), které nabízí několik základních funkcí. Bither umožňuje jak účet s generováním klíčů z mnemonické fráze, tak generování klíčů jednorázově zcela náhodně. Zvolením jedné z těchto funkcí je uživatel vyzván k nastavení uživatelského hesla, to je poté vyžadováno k veškerým operacím s peněženkou. Aktivní adresy a jejich stav je dostupný bez uživatelského hesla.



Obrázek 16 Bither klient

Záloha peněženky

Záloha Bither peněženky je SQLite 3 databáze s pevně daným názvem *address.db*, která se nachází a automaticky vytváří (pokud neexistuje) v data directory v lokaci *C:\Users\"username"\AppData\Roaming\Bither*. Soubor obsahuje adresy a veřejné klíče v nešifrované podobě, soukromé klíče a seed jsou implicitně šifrovány uživatelským heslem. Z importované zálohy je možné bez hesla zjistit aktivní adresy a jejich stav, pro jakoukoliv manipulaci je ovšem heslo nezbytné.

6.2 Návrh metodiky pro vyhledávání analyzovaných peněženek

Metodika pro vyhledávání klientů a záloh bitcoinových peněženek je navržena na základě informací získaných z provedené analýzy v předchozí kapitole a je nezbytnou součástí implementace.

6.2.1 Detekce klienta peněženky

Bitcoin Core

Bitcoin Core při instalaci a spuštění zapisuje dva důležité klíče do kořenového klíče *HKEY_CURRENT_USER*:

1. *HKEY_CURRENT_USER\Software\Bitcoin Core (64-bit)*
2. *HKEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt*

První z klíčů se zapisuje do registru pří instalaci Bitcoin Core klienta a obsahuje hodnotu *Path* typu REG_SZ s údajem hodnoty umístění nainstalovaného klienta (např. *D:\Program Files\Bitcoin*).

Druhý klíč obsahující hodnotu *strDataDir* typu REG_SZ s údajem hodnoty umístění data directory pro Bitcoin Core se do registru zapisuje až po prvním spuštění klienta a zvolení umístění uživatelem.

Pokud se ani jeden z uvedených klíčů ve Windows registrech nenachází, znamená to, že peněženka Bitcoin Core s jejím data directory není na zařízení nainstalována, pokud se na zařízení nachází pouze první klíč, je peněženka nainstalována, ale nebyla ještě spuštěna.

Electrum

Peneženka Electrum při instalaci rovněž v kořenovém klíči zapisuje klíč *HKEY_CURRENT_USER\Software\Electrum* s jedinou hodnotou *(Výchozí)* typu REG_SZ s údajem hodnoty umístění nainstalovaného klienta.

Data directory má u Electrum pevně dané umístění v *C:\Users\"username"\AppData\Roaming\Electrum* a vytváří se ihned při instalaci.

Bither

Bither při instalaci do registru nezapisuje žádný důležitý klíč pro detekci, ale má pevně danou instalační lokaci i umístění data directory.

Klient je vždy nainstalován ve složce *JWrapper-Bither* v pevně dané lokaci *C:\Users\"username"\AppData\Roaming*.

Data directory se nachází ve stejné lokaci akorát v jiné složce s názvem *Bither*.

6.2.2 Detekce zálohy peněženky

Bitcoin Core

Jak již bylo popsáno v kapitole Analýza bitcoinových peněženek, Bitcoin Core záloha je v pevně daném formátu *wallet.dat* standardně umístěná v data directory v podsložce *wallets* a jedná se o BerkeleyDB obsahující klíčové hodnoty v binára. Pro čtení

zálohy jsem použil hex editor PSPad 5.0.3 a nalezl jsem několik klíčových hodnot společných pro všechny zálohy (magic value), které jsem využil k jejich detekci:

key! – 0x6B657921 (hex)
– následující sekvence v databázi značí nešifrovaný soukromý klíč

ckey! – 0x636B657921 (hex)
– následující sekvence v databázi značí šifrovaný soukromý klíč

keymeta! – 0x6B65796D65746121 (hex)
– následující sekvence značí veřejný klíč + metadata

pool – 0x706F6F6C (hex)
– oblast pro ukládání rezervovaých klíčů

Záloha vždy obsahuje hodnoty: *pool*; *keymeta!*; *ckey!* a nebo *key!*. Pokud jsou v souboru přítomny hodnoty *ckey!*, jedná se o šifrovanou zálohu, v případě že obsahuje jen *key!*, soukromé klíče jsou v nešifrované podobě – není chráněna heslem.

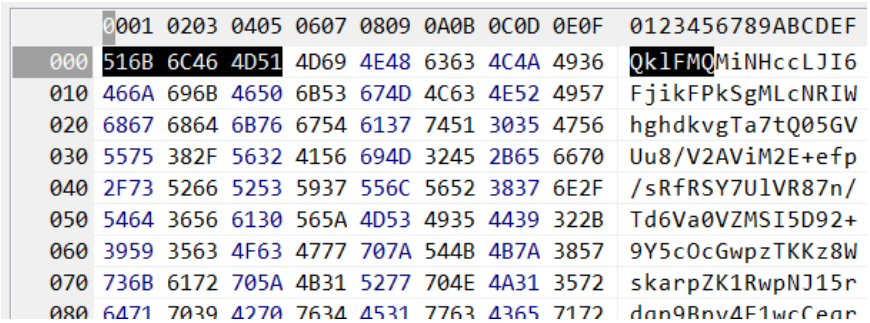
Pro redukci času při hledání zálohy je také důležité brát v úvahu velikost souboru, na kterou má vliv, zdali je záloha uživatelským heslem chráněna či nikoliv. V případě, že není šifrována, její velikost se pohybuje mezi 1300-1450 kB, v šifrované podobě je to 1000-1100 kB.

Prohledáváním souborů na přítomnost výše zmíněných hexadecimálů je možné naleznout zálohy peněženek alternativních kryptoměn využívajících zdrojového kódu Bitcoin Core. S tím se bohužel nedá nic dělat, nicméně při dalším zkoumání importem do data directory a spuštěním klienta se jednoduše zjistí, zdali se jedná o zálohu peněženky Bitcoin Core.

Electrum

U peněženky Electrum je to složitější. Záloha nemá žádný fixní název, ten je volen uživatelem a nemá ani žádnou příponu. Lokace pro ukládání a načítání je rovněž v režii uživatele a soubor je implicitně šifrován uživatelským heslem.

Soubor je možné zobrazit v plain textu v jakémkoliv textovém editoru a obsahuje AES-256-CBC šifru seedu a soukromých klíčů. Velikost souboru se pohybuje okolo 3 kB. Vytvořil jsem si velké množství Electrum peněženek a zkoumal jsem podobnost souborů záloh. Našel jsem mezi nimi magic value společnou pro všechny zálohy, a sice prvních 6 bajtů, které jsou u všech záloh stejné (obr. 17). Hledáním hodnoty *QklFMQ* – *0x516B6C464D51* na pozici prvních 6 bajtů je možné naleznout zálohu peněženky Electrum, ta byla tímto způsobem detekována bezchybně ve všech případech.



Obrázek 17 Electrum záloha v textovém editoru

Bither

Záloha Bither peněženky má fixní název *address.db* a nachází se v data directory v pevně dané lokaci *C:\Users\"username"\AppData\Roaming\Bither*. Záloha je SQLite 3 databáze, která neobsahuje klíčové hodnoty stejně jako například BerkeleyDB u Bitcoin Core, nicméně při zobrazení v hex editoru obsahuje několik SQL příkazů *CREATE TABLE*. Kombinací těchto příkazů se dá efektivně dosáhnout nalezení zálohy Bither peněženky. Velikost souboru zálohy je okolo 20 kB.

Pro nalezení zálohy jsem v souborech hledal následující hodnoty příkazů:

CREATE TABLE password_seed
0x435245415445205441424C452070617373776F72645F73656564

CREATE TABLE hd_seeds
0x435245415445205441424C452068645F7365656473

CREATE TABLE hdm_bid
0x435245415445205441424C452068646D5F626964

CREATE TABLE hd_account
0x435245415445205441424C452068645F6163636F756E74

6.3 Praktická implementace metodiky

6.3.1 Požadavky skriptu

Skript je vytvořen pomocí programovacího jazyku Python a je určen pro operační systém Windows 7 a vyšší. Systém Windows byl vybrán na základě statistiky ze stránky statcounter za uplynulých 12 měsíců, podle které je tento systém nainstalován na 76% všech zařízeních. [44] K jeho fungování je nutná lokální instalace Python 3.8 obsahující i integrované vývojové prostředí IDLE, které bylo použito při vývoji. Nezbytnou součástí je také instalace dodatečných knihoven *pypiwin32* a *bitstring*. Skript nemá grafické rozhraní a je spouštěn z příkazové řádky.

6.3.2 Přehled funkcí

getRegistry(path, name)

Funkce getRegistry s parametry path (cesta) a name (název hodnoty) slouží k načítání hodnot z kořenového klíče HKEY_CURRENT_USER. V případě nálezu je funkcí vrácena hodnota klíče, v opačném případě je vrácena hodnota None.

bitcoinCoreRegistry()

Tato funkce přímo využívá getRegistry(path, name) a slouží k načítání Bitcoin Core registrů a vypsání údajů jejich hodnot, které obsahují umístění Bitcoin Core klienta a jeho data directory.

electrumRegistry()

Stejně jako bitcoinCoreRegistry() i tato funkce využívá getRegistry(path, name) k načítání údaje hodnoty s umístěním klienta peněženky Electrum. Dále slouží ke kontrole pevně dané lokace umístění Electrum data directory.

bitherDefaultFolder()

Vzhledem k tomu, že Bither má pevně danou lokaci umístění klienta a data directory, je funkcí kontrolována přítomnost těchto složek v této implicitní lokaci.

backupSearch(fn)

Jedná se o hlavní funkci pro hledání záloh peněženek rozdělenou na rychlé a hloubkové prohledávání.

Při rychlém prohledávání hledá pouze soubory s názvem *wallet.dat* pro Bitcoin Core, v kterých kontroluje příslušné hexadecimály. U záloh peněženky Bither funguje funkce podobně jako pro Bitcoin Core, hledá soubory s názvem *address.db*, které při nalezení rovněž kontroluje na přítomnost příslušných hexadecimálů.

Hloubkové prohledávání prohledává všechny soubory bez ohledu na jejich název či příponu a kontroluje v nich magic value v hexadecimálu příslušnou pro konkrétní zálohy peněženek.

V obou případech jsou navíc prohledávané soubory ohraničeny velikostí z důvodů redukce času.

fastElectrum()

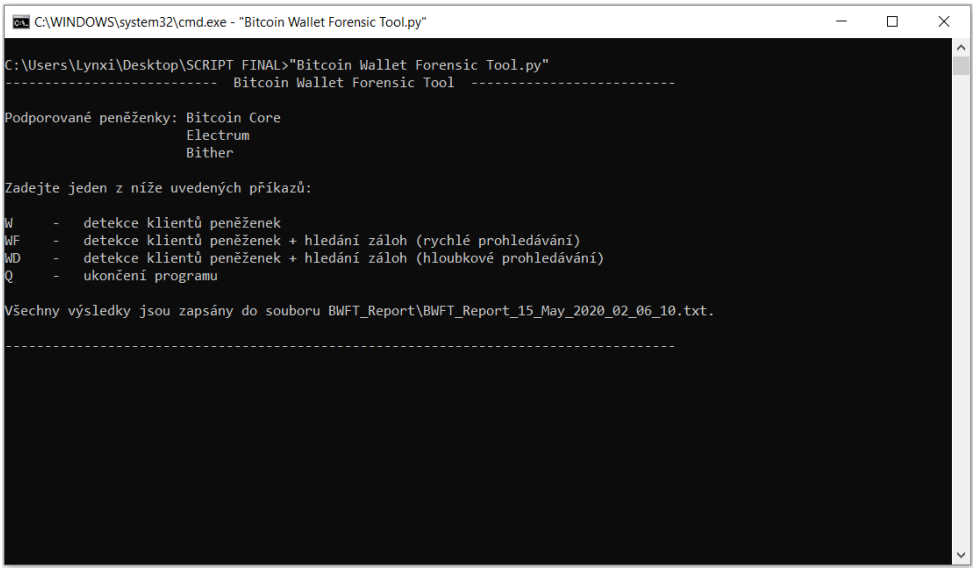
Funkce pro rychlé hledání zálohy peněženky Electrum kontroluje výchozí pevně danou lokaci data directory a její podsložku *wallets*, kde se implicitně ukládají zálohy. Ve složce jsou pomocí funkce folderSearch() a backupSearch(fn) procházeny všechny soubory a kontrolovány na přítomnost magic value pro Electrum.

driveSearch() & folderSearch()

Dvojice funkcí sloužící k postupnému prohledávání všech nalezených logických disků a následné prohledávání jednotlivých disků rekurzivně od kořenové složky.

6.3.3 Popis a ovládání

Skript je bez grafického rozhraní spouštěn přímo z příkazové řádky, kde jsou uživateli v konzoli zobrazeny podporované peněženky a dostupné příkazy s jejich stručným popisem (obr. 18).



Obrázek 18 Skript při spuštění v příkazovém řádku

Dostupné jsou následující čtyři příkazy:

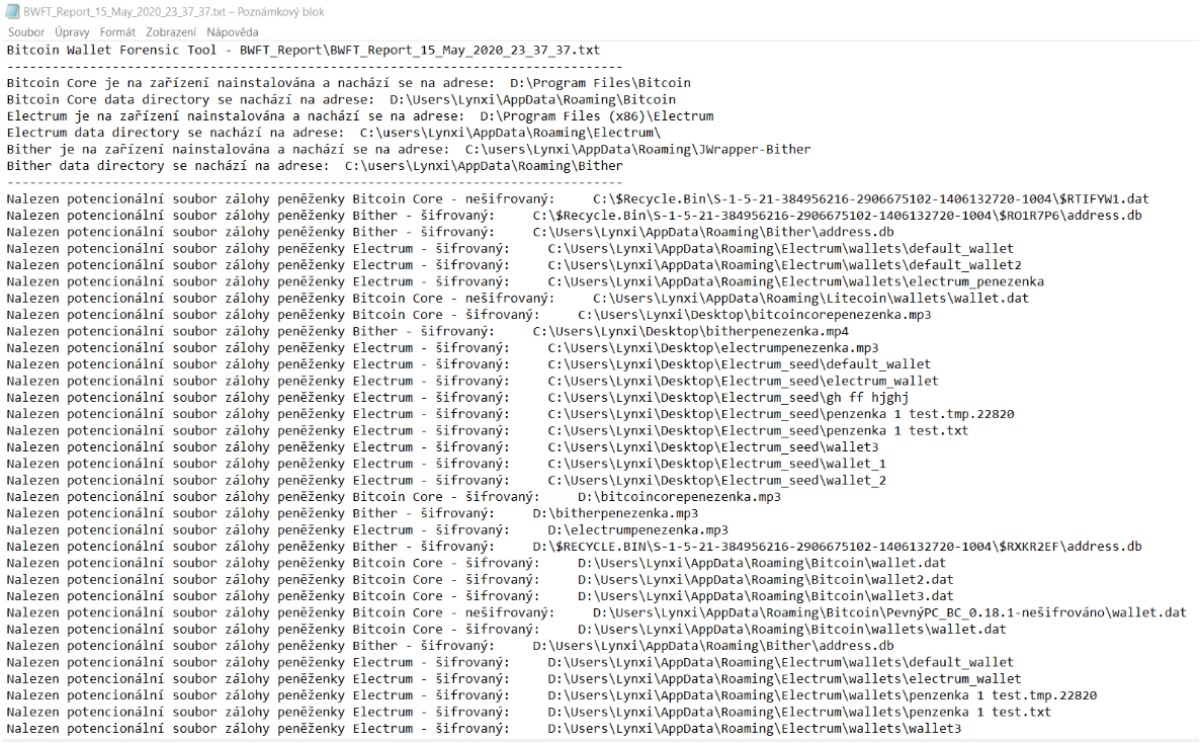
W – příkaz detekující klienty peněženek a jejich data directory. Při úspěšném nalezení jsou do konzole a reportu vypsány lokace umístění, v opačném případě je vypsáno, že konkrétní peněženky nebyly nalezeny. Program se po vykonání příkazu neukončí.

WF – spuštěním tohoto příkazu je provedena detekce peněženek stejně jako u příkazu *W*, navíc se ale spustí hledání záloh všech peněženek metodou rychlého prohledávání, to trvá v řádech minut. Všechny výsledky jsou poté zapsány do reportu a program je po 5 vteřinách po dokončení prohledávání automaticky ukončen.

WD – tento příkaz rovněž detekuje peněženky jako ty předchozí, dále pak metodou hloubkového prohledávání hledá zálohy všech peněženek. Vykonání tohoto příkazu je nejvíce časově náročné ze všech, trvá několik desítek minut v závislosti na kapacitě prohledávaných disků. Nalezené výsledky jsou zapsány do reportu a program je po 5 vteřinách od dokončení hledání automaticky ukončen.

Q – poslední z příkazů je určený k manuálnímu ukončení programu.

Spuštěním skriptu je automaticky v lokaci jeho umístění vytvořena složka (pokud neexistuje) s názvem *BWFT_Report* určena pro ukládání reportů z hledání. Reporty s názvem *BWFT_Report_"+str(timestampStr)+".txt* se generují automaticky při každém spuštění skriptu. Jedná se o textový soubor s časovým razítkem obsahující záznam z prohledávání (obr. 19).



Obrázek 19 Výsledky z prohledávání skriptem zapsané v reportu

7 Testování

Testování bylo prováděno zejména autorem, a to jak během praktické implementace, tak i po ní, další osoby byly do testování zapojeny až po dokončení skriptu. Cílem testování bylo ověřit funkčnost a spolehlivost programu na více zařízeních s operačním systémem Windows.

Operační systém	**Počet testovaných zařízení**
Windows 10 (64-bit; 32-bit)	12 (10x fyzicky + 2x virtuálně)
Windows 8 (64-bit; 32-bit)	3 (1x fyzicky + 2x virtuálně)
Windows 7 (64-bit; 32-bit)	6 (4x fyzicky + 2x virtuálně)

Tabulka 6 Přehled testovaných zařízení

Předmětem testování byl OS Windows 7 a vyšší, starší verze nejsou samotnými peněženkami podporovány. Využita byla jak fyzická zařízení, tak i virtuální pomocí VM VirtualBox ve verzi 6.1.4 od společnosti Oracle. K potřebám testování bylo dále autorem vytvořeno více než 150 záloh každé z testovaných peněženek.

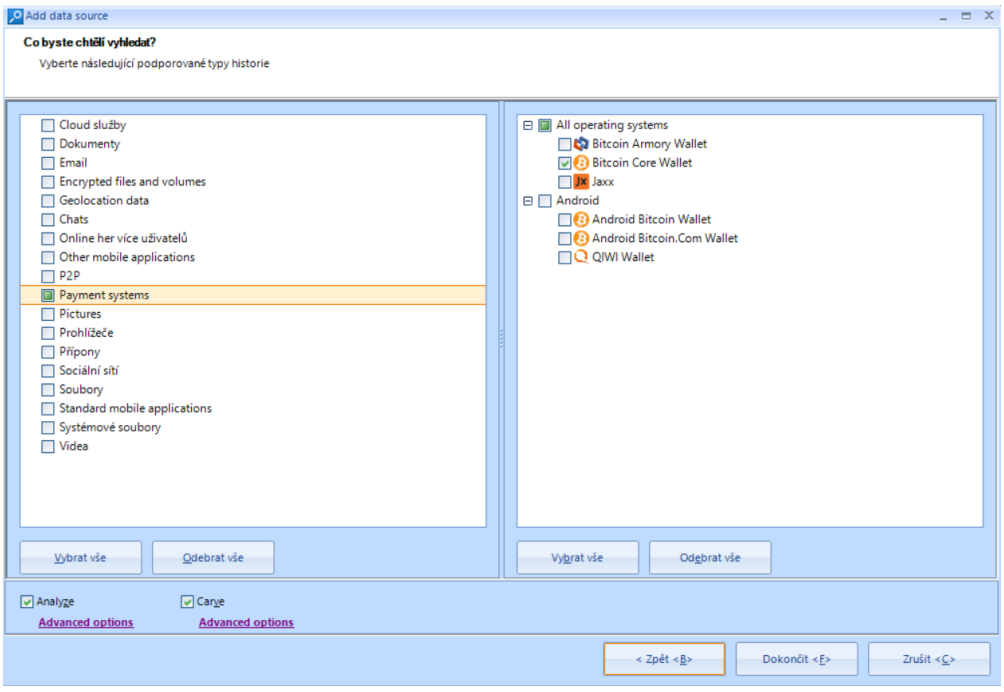
Skript byl úspěšný při detekci klientů a nalezení všech vytvořených záloh peněženek nacházejících se v úložišti, a to jak autorem, tak i osobami třetí strany.

8 Zkoumání počítačového zařízení forenzními nástroji

Ke zkoumání počítačového zařízení jsem použil dva profesionální komerční forenzní nástroje s podporou vyhledávání kryptoměny na počítačovém zařízení, a to Belkasoft Evidence Center 9.9.4662 od společnosti Belkasoft a Magnet AXIOM Process 3.11.0.19007 od Magnet Forensics, jejichž dočasné licence jsem pro potřeby mé bakalářské práce získal po vzájemné elektronické komunikací s jednotlivými společnostmi. Získané licence mi umožnily všechny funkce plných verzí softwarů a při zkoumání jsem nebyl nijak omezen.

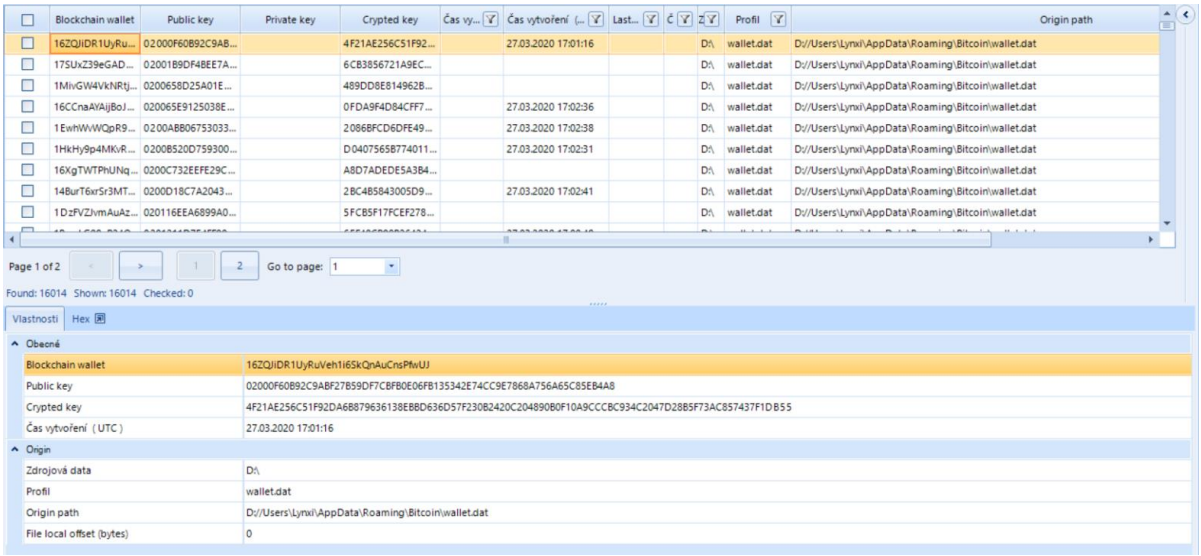
8.1 Belkasoft Evidence Center

Prvním z použitých forenzních nástrojů je software Belkasoft Evidence Center (dále jen Belkasoft). Nástroj při zkoumání počítačového zařízení podporuje pouze tři peněženky (obr. 20) a to: Bitcoin Core, Bitcoin Armory (tato peněženka ke svému fungování vyžaduje spolupráci s plným uzlem – Bitcoin Core) a Jaxx. Pro potřeby mého zkoumání tedy podporuje pouze peněženku Bitcoin Core.



Obrázek 20 Belkasoft - výběr peněženek

Při zkoumání zařízení pro peněženku Bitcoin Core je Belkasoft schopen naleznout všechny její zálohy pouze ve formátu *wallet.dat*. Ze záloh poté automaticky vyexportuje všechny veřejné klíče aktivních i rezervovaných adres peněženky a k nim příslušné soukromé klíče (Obr. 21), a to buď v šifrované nebo nešifrované podobě v závislosti na tom, zdali je záloha chráněna heslem. Veřejné klíče jsou v obou případech vždy nešifrované. Z veřejných klíčů Belkasoft vypočítává blockchainové adresy s prefixem 1, který značí nejstarší formát adres, nicméně Bitcoin Core používá standardně adresy s prefixem 3 popřípadě bc1. Pokud tedy Belkasoft počítá z veřejných klíčů adresy, měl by vypočítat všechny tři formáty a nikoliv pouze jeden, který navíc ani Bitcoin Core pro nově generované adresy nepoužívá. Pokud se na zařízení nachází zálohy ve formátu *wallet.dat* jiných peněženek vycházejících ze zdrojového kódu Bitcoin Core jako je například Litecoin Core a jiné, Belkasoft z nich rovněž vyexportuje všechny klíče s adresami (opět s prefixem 1) společně se všemi ostatními zálohami. Při mém zkoumání bylo tedy výsledkem něco přes patnáct tisíc nalezených adres z několika různých peněženek, kde Belkasoft nedělá rozdíly mezi rezervovanými a aktivními adresami, aktivní adresa může z těch všech být třeba pouze jedna. Výsledný výstup v pdf formátu měl přes patnáct tisíc stránek s jednotlivými adresami a jejich klíči.

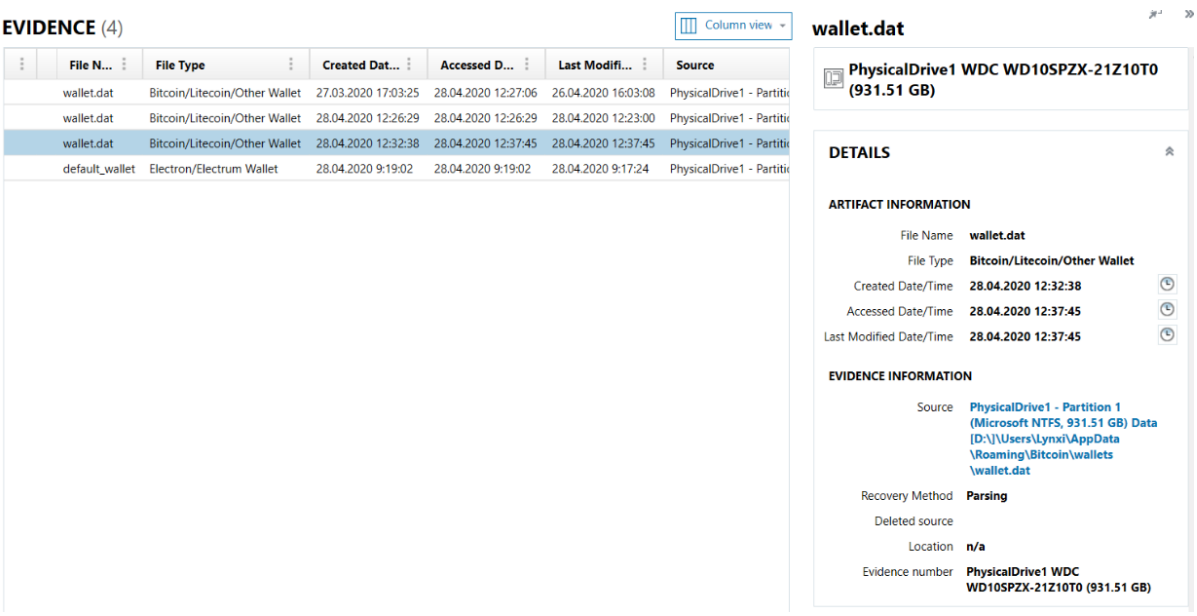


Obrázek 21 Belkasoft - výsledek zkoumání

8.2 Magnet AXIOM Process

Druhým použitým forenzním nástrojem je Magnet AXIOM Process (dále jen Magnet AXIOM). Magnet AXIOM podporuje širší spektrum bitcoinových peněženek a výsledky zkoumání jsou uspokojivější než v případě nástroje od společnosti Belkasoft. Všechny tři použité peněženky jsou nástrojem podporovány.

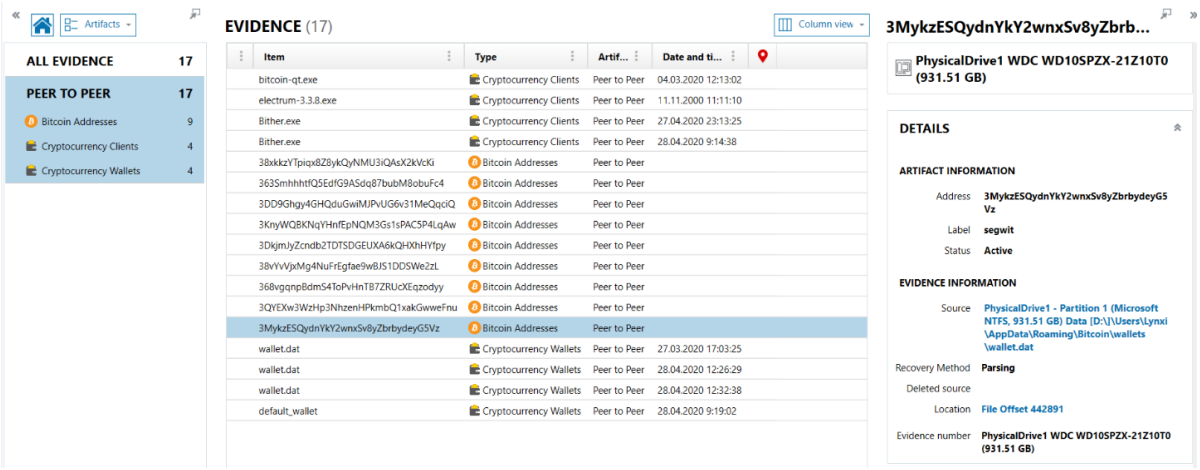
Nejlepších výsledků zkoumání dosáhl Magnet AXIOM pro peněženku Bitcoin Core. Software detekoval Bitcoin Core klienta a nalezl na zařízení všechny zálohy, stejně jako Belkasoft, pouze ve formátu *wallet.dat* a i v tomto případě byly nalezeny zálohy jiných kryptoměnových peněženek vycházejících ze zdrojového kódu Bitcoin Core, nicméně Magnet AXIOM u výsledků zkoumání sám uvádí, že se může jednat o zálohu jakékoliv peněženky typu Bitcoin Core (obr. 22). Software ze záloh získal pouze aktivní adresy, což je z pohledu zkoumání lepší než všechny rezervované adresy. Zde se ale objevuje podobný problém jako u Belkasoftu. Exportované aktivní adresy jsou ve správném formátu, který Bitcoin Core standardně generuje, tedy s prefixem 3, nicméně pokud je vygenerovaná aktivní adresa v novějším formátu s prefixem bc1, neobjevuje se ve výsledku zkoumání. Soukromé ani veřejné klíče nejsou exportovány v žádné formě.



Obrázek 22 Magnet AXIOM – výsledek hledání záloh peněženek

Klient peněženky Electrum byl softwarem úspěšně na zařízení detekován. Co se zálohy týče, byla nalezena pouze ve formátu s implicitním názvem *default_wallet*, který si uživatel může při vytváření peněženky nastavit dle libosti, pokud záloha nese jiný než implicitní název, není forenzním nástrojem nalezena. Soubor je implicitně šifrován uživatelským heslem.

Bither klient byl nástrojem rovněž bez problému detekován, nicméně záloha peněženky nebyla v žádném zkoumání objevena.



Obrázek 23 Magnet AXIOM - výsledek zkoumání

8.3 Porovnávání výsledků zkoumání forenzními nástroji s navrženou metodikou

Forenzní nástroj Belkasoft Evidence byl schopen detekovat pouze soubory záloh peněženky Bitcoin Core ve formátu *wallet.dat*, z nichž bez rozdílu vyexportoval všechny aktivní i rezervované veřejné klíče s adresami (v nestandardním formátu pro Bitcoin Core) a jejich soukromé klíče v šifrované či nešifrované podobě. Pro peněženky Electrum a Bither nebyly žádné výsledky, jelikož nejsou forenzním nástrojem podporovány.

Magnet AXIOM Process detekoval na zařízení klienty všech zástupců testovaných peněženek, ale pouze u peněženky Bitcoin Core byl schopný naleznout její zálohy, a to opět pouze ve formátu *wallet.dat*, ze kterých vyexportoval jen aktivní adresy bez veřejných či soukromých klíčů, ale pouze v jednom ze dvou standardních formátů Bitcoin Core s prefixem 3, pokud byla aktivní adresa ve formátu s prefixem bc1, nebyla softwarem označena a exportována. Při hledání záloh peněženek Electrum a Bither nebyl software úspěšný.

Skript vytvořený na základě navržené metodiky byl schopný detekovat klienty všech zástupců testovaných bitcoinových peněženek a hlavně nalezl všechny jejich zálohy, a to v jakémkoliv formátu. Při další práci s nalezenými soubory záloh bylo možné u Bitcoin Core zjistit všechny aktivní adresy, transakční historii a v případě, že zálohy nebyly šifrovány i soukromé klíče všech adres. U nalezených záloh peněženky Electrum nebylo možné zjistit žádné informace, jelikož zálohy jsou implicitně šifrovány heslem uživatele a musely by se stát předmětem dešifrování. Zálohy peněženky Bither jsou rovněž implicitně šifrovány heslem, nicméně bez hesla bylo pomocí klienta možné zjistit všechny aktivní adresy včetně transakční historie.

Detekce klienta peněženky	Belkasoft Evidence Center	Magnet AXIOM Process	Script
Bitcoin Core	✓	✓	✓
Electrum	X	✓	✓
Bither	X	✓	✓

Tabulka 7 Porovnání získaných výsledků - detekce klienta peněženky

Detekce zálohy peněženky	Belkasoft Evidence Center	Magnet AXIOM Process	Script
Bitcoin Core	✓	✓	✓
Electrum	X	X	✓
Bither	X	X	✓

Tabulka 8 Porovnání získaných výsledků - detekce zálohy peněženky

9 Závěr

Závěrem bych chtěl shrnout obsah a cíle celé mé bakalářské práce a možnosti jejího rozšíření v budoucnu.

Cílem teoretické části bylo detailní vysvětlení principu fungování kryptoměny Bitcoin. Zde bylo vysvětleno vlastnictví bitcoinu a realizace transakcí na základě asymetrické kryptografie, ukládání transakcí do bloků, decentralizovaná distribuovaná databáze blockchain a konsensní algoritmus Proof-of-Work. Dalším z cílů teoretické části byla analýza způsobů ukládání a získávání bitcoinu a porovnání s alternativními kryptoměnami, kde byly popsány všechny druhy peněženek s možnostmi získávání bitcoinu nákupem, prodejem služeb a těžbou. Pro porovnání byly vybrány a popsány alternativní kryptoměny implementující anonymizační technologie vhodné k realizaci nevystopovatelných transakcí a alternativní způsoby dosažení konsensu k Proof-of-Work a tím získávání kryptoměny.

Praktická část měla za cíl vytvořit metodiku pro vyhledávání kryptoměny Bitcoin v počítačovém zařízení a její praktickou implementaci. Metodika byla sestavena ze třech částí, a sice z detailní analýzy třech vybraných desktopových peněženek určených pro Bitcoin, návrhu detekce a praktické implementace automatizující celý proces vyhledávání. Implementace byla na základě statistky o rozšíření operačních systémů navržena pro operační systém Windows a jejím výstupem byl plně funkční a otestovaný skript napsaný v programovacím jazyce Python. Skript je bez grafického rozhraní spouštěn přímo z příkazové řádky a ovládán několika příkazy. Všechny výsledky hledání jsou zapisovány do textového souboru. Skript je schopný detekce všech tří klientů peněženek a jejich záloh, a to v jakémkoliv formátu. Součástí praktické části bylo také využití profesionálních forenzních nástrojů a porovnání získaných výsledků s vytvořeným skriptem. Zde byly použity forenzní nástroje Belkasoft Evidence Center a Magnet AXIOM Process, kde skript dosahoval lepších výsledků detekce, a to zejména u záloh peněženek.

Navrženou metodiku lze v budoucnu rozšířit o více bitcoinových peněženek a implementovat pro ostatní operační systémy, navrhnout grafické rozhraní a s dalšími formálními náležitostmi vytvořit plnohodnotný forenzní nástroj pro vyhledávání klientů desktopových bitcoinových peněženek a jejich záloh.

Literární a internetové zdroje

[1] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. 2009 [cit. 2020-05-03]. Dostupné z: https://bitcoin.org/bitcoin.pdf

[2] Genesis block. *Bitcoin Wiki* [online].[cit. 2020-05-03]. Dostupné z: https://en.bitcoin.it/wiki/Genesis_block

[3] ACHESON, Noelle. *What is Bitcoin?* [online]. 2013 [cit. 2020-05-03]. Dostupné z: https://www.coindesk.com/learn/bitcoin-101/what-is-bitcoin

[4] SULLIVAN, Nick. *ECDSA: The digital signature algorithm of a better internet* [online]. 2014 [cit. 2020-05-03]. Dostupné z: https://blog.cloudflare.com/ecdsa-the-digital-signature-algorithm-of-a-better-internet/

[5] SHARMA, Toshendra Kumar. *How does blockchain use public key cryptography?* [online]. 2018 [cit. 2020-05-03]. Dostupné z: https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/

[6] What is WIF? *All private keys* [online]. [cit. 2020-05-03]. Dostupné z: https://allprivatekeys.com/what-is-wif

[7] ANTONOPOULOS, Andreas. *Mastering Bitcoin* [online]. Sebastopol, United States: O'Reilly Media, Inc, USA, 2015, 298 s. [cit. 2020-05-03]. 1st ed. ISBN 9781449374044. Dostupné z: https://unglueitfiles.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf

[8] Multisignature. *Bitcoin Wiki* [online]. [cit. 2020-05-03]. Dostupné z: https://en.bitcoin.it/wiki/Multisignature

[9] WALKER, Greg. *UTXO* [online]. 2017 [cit. 2020-05-03]. Dostupné z: https://learnmeabitcoin.com/guide/utxo

[10] *Bitcoin Fees for Transactions* [online]. [cit. 2020-05-03]. Dostupné z: https://bitcoinfees.earn.com

[11] LOMBROZO, Eric, Johnson LAU a Pieter WUILLE. BIP 141: Segregated Witness. *GitHub* [online]. [cit. 2020-05-03]. Dostupné z: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[12] Serialized Blocks. *Bitcoin - Open source P2P money* [online]. [cit. 2020-05-03]. Dostupné z: https://bitcoin.org/en/developer-reference#serialized-blocks

[13] Block Headers. *Bitcoin - Open source P2P money* [online]. [cit. 2020-05-03]. Dostupné z: https://bitcoin.org/en/developer-reference#block-headers

[14] VOSHMGIR, Shermin. *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*. BlockchainHub Berlin, 2019. ISBN 3982103827.

[15] BACK, Adam. *Hashcash - A Denial of Service Counter-Measure* [online]. 2002 [cit. 2020-05-03]. Dostupné z: http://www.hashcash.org/papers/hashcash.pdf

[16] NADEEM, Subhan. *How Bitcoin mining really works* [online]. 2018 [cit. 2020-05-03]. Dostupné z: https://www.freecodecamp.org/news/how-bitcoin-mining-really-works38563ec38c87/

[17] Difficulty. *Bitcoin Wiki* [online]. [cit. 2020-05-03]. Dostupné z: https://en.bitcoin.it/wiki/Difficulty

[18] LAW, Crypto. *What is KYC?* [online]. 2017 [cit. 2020-05-03]. Dostupné z: https://medium.com/@woodforklaw/what-is-kyc-b8fc42ea4df

[19] *Bitcoin ATM Czech Republic* [online]. [cit. 2020-05-03]. Dostupné z: https://coinatmradar.com/country/57/bitcoin-atm-czech-republic/

[20] *Crypto ATMs & merchants of the world* [online]. [cit. 2020-05-03]. Dostupné z: https://coinmap.org/view

[21] SHOBHIT, Seth. *Are Bitcoin Payment Services Similar to Credit Cards?* [online]. 2019 [cit. 2020-05-03]. Dostupné z: https://www.investopedia.com/tech/bitcoin-payment-services-introduction/

[22] *Bitcoin Paper Wallet Generator* [online]. [cit. 2020-05-03]. Dostupné z: https://bitcoinpaperwallet.com

[23] BLAGOJEVIC, Dobrica. *What Is the Difference between a Full Node and a Light Client?* [online]. 2018 [cit. 2020-05-03]. Dostupné z: https://captainaltcoin.com/full-node-vs-light-client/

[24] *Android keystore system* [online]. [cit. 2020-05-03]. Dostupné z: https://developer.android.com/training/articles/keystore.html

[25] *Keychain Services* [online]. [cit. 2020-05-03]. Dostupné z: https://developer.apple.com/documentation/security/keychain_services

[26] *Trezor Hardware Wallet* [online]. [cit. 2020-05-03]. Dostupné z: https://trezor.io

[27] *Cryptocurrency Market Capitalizations* [online]. [cit. 2020-05-03]. Dostupné z: https://coinmarketcap.com

[28] FRANKENFIELD, Jake. *Proof of Stake (PoS)* [online]. 2019 [cit. 2020-05-03]. Dostupné z: https://www.investopedia.com/terms/p/proof-stake-pos.asp

[29] LINDSEY, Nick. *Proof of Stake (PoS): What Is It and How Does It Work?* [online]. [cit. 2020-05-03]. Dostupné z: https://blocklr.com/guides/proof-of-stake-pos/

[30] PRIYESHU, Garg. *What is a Coin Burn? Beginner's Guide to Proof of Burn* [online]. 2018 [cit. 2020-05-03]. Dostupné z: https://blockonomi.com/proof-of-burn/

[31] SCOTT, Andrew. *Proof-of-Capacity, The Green Alternative?* [online]. 2018 [cit. 2020-05-03]. Dostupné z: https://hackernoon.com/burst-part-3-proof-of-capacity-the-green-alternative-8e2651211671

[32] GALVÁNEK, Matej. *Monero* [online]. 2018 [cit. 2020-05-03]. Dostupné z: https://www.alza.cz/monero

[33] *Ring Signature* [online]. [cit. 2020-05-03]. Dostupné z: https://web.getmonero.org/resources/moneropedia/ringsignatures.html

[34] NOETHER, Shen. *Ring Confidential Transactions* [online]. 2015 [cit. 2020-05-03]. Dostupné z: https://eprint.iacr.org/2015/1098.pdf

[35] *Stealth Address* [online]. [cit. 2020-05-03]. Dostupné z: https://web.getmonero.org/resources/moneropedia/stealthaddress.html

[36] ROSIC, Ameer. *What is Dash Cryptocurrency?* [online]. [cit. 2020-05-03]. Dostupné z: https://blockgeeks.com/guides/what-is-dash/

[37] ROSIC, Ameer. *What is Zcash?* [online]. 2018 [cit. 2020-05-03]. Dostupné z: https://blockgeeks.com/guides/zcash/

[38] Addresses and Value Pools in Zcash. *Zcash Documentation* [online]. [cit. 2020-05-03]. Dostupné z: https://zcash.readthedocs.io/en/latest/rtd_pages/addresses.html

[39] How It Works. *Privacy-protecting digital currency Zcash* [online]. [cit. 2020-05-03]. Dostupné z: https://z.cash/technology/

[40] Bitcoin Core :: Download - Bitcoin. *Bitcoin Core* [online]. [cit. 2020-05-03]. Dostupné z: https://bitcoincore.org/en/download/

[41] Electrum Bitcoin Wallet. *Electrum Bitcoin Wallet* [online]. [cit. 2020-05-03]. Dostupné z: https://electrum.org/#download

[42] PALATINUS, Marek, Pavol RUSNAK, Aaron VOISINE a Sean BOWE. BIP 39: Mnemonic code for generating deterministic keys. *GitHub* [online]. 2013 [cit. 2020-05-03]. Dostupné z: https://github.com/bitcoin/bips/blob/master/bip0039.mediawiki

[43] Bither - a simple and secure Bitcoin wallet. *Bither* [online]. [cit. 2020-05-03]. Dostupné z: https://bither.net

[44] Desktop Operating System Market Share Worldwide. *Statcounter GlobalStats* [online]. 1999 [cit. 2020-05-03]. Dostupné z: https://gs.statcounter.com/os-market-share/desktop/worldwide

Seznam obrázků

Seznam tabulek

Přílohy

Příloha 1 – Vytvořený skript pro detekci peněženek

Příloha 2 – Soubory záloh peněženek