Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Diplomová práce

2018 **Bc. Jakub Zimmel**

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Analýza současných kryptoměn se zaměřením na Bitcoin, zajištění výnosu z trestné činnosti.

Diplomová práce

Bc. Jakub Zimmel

Školitel: Ing. Jaroslav Kothánek, Ph.D.

České Budějovice 2018

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL MAGISTERSKÉ PRÁCE

Student: **Bc. Jakub Zimmel, *B13440***
(jméno, příjmení, tituly)
Obor – zaměření studia: **Aplikovaná informatika**

Katedra: **Ústav aplikované informatiky**

Školitel: **Ing. Jaroslav Kothánek, Ph.D.,** kothanek@it-znalec.cz
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Garant z PřF: .....
(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 současných kryptoměn se zaměřením na Bitcoin, zajištění výnosu z trestné činnosti.

Cíle práce:

1. Seznamte se s metodikou forenzního zkoumání informačních technologií.
2. Seznamte se se současnými kryptoměnami.
3. Popište jednotlivé kryptoměny mající vztah k trestné činnosti.
4. Popište možnosti a omezení forenzního zkoumání u zajištěné výpočetní techniky s podezřením na výskyt kryptoměny.
5. Navrhněte možnosti forenzního zkoumání u zajištěné výpočetní techniky s podezřením na výskyt kryptoměny.
6. Na základě získaných informací navrhněte optimální řešení forenzní zkoumání výpočetní techniky pro nalezení a zajištění uložených kryptoměn.
7. Vyhodnoťte získané informace

Základní doporučená literatura:

http://www.it-znalec.cz

https://bitcoin.org/en/

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

BRYCHTA, Jaroslav. Zkušenosti s virtuálními měnami: Bitcoin měna budoucnosti?

CAMPBELL, Gary. Making money from Litecoin for Beginners.

COMBS, Brett; MITSOFF, Tom, Bitcoin decoded: Bitcoin Beginner´s Guide To Mining And the Strategies To Make Money With Cryptocurrencies.

EDELSON, Rick. How to Buy, Trade and Profit with Bitcoin: A Jump - Start Guide.

Financování práce: .....

Vedoucí práce: Ing. Jaroslav Kothánek, Ph.D. podpis: .....

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

Garant oboru mgr. studia (nepožaduje se u zaměření „příprava na mag. studium biologie)

doc. RNDr. Iva Dostálková, Ph.D. podpis: .....

Vedoucí oddělení Forenzních věd a kriminalistiky
Ing. Jaroslav Kothánek, Ph.D. podpis: .....

V Českých Budějovicích dne 18. 12. 2017

Převzal/a dne..... podpis: .....

Bibliografické údaje:

Zimmel J., Analýza současných kryptoměn se zaměřením na Bitcoin, zajištění výnosu z trestné činnosti. [Analysis of current cryptocurrency with focus on Bitcoin, securing the proceeds of crime. Mgr. Thesis, in Czech.] 93p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Anotace:

Diplomová práce „Analýza současných kryptoměn se zaměřením na Bitcoin, zajištění výnosu z trestné činnosti“ se zabývá zajišťováním kryptoměn s důrazem na zajištění bitcoinu. V práci jsou popsány vybrané kryptoměny a jejich odlišnosti od Bitcoinu. Práce se orientuje na problematiku nalezení a zajištění kryptoměn ve zkoumaných zařízeních zadržených při trestné činnosti. Na základě výsledků zkoumání jsou navrhnuty optimální postupy pro zajišťování a forenzní analýzu kryptoměn.

Klíčová slova:

Bitcoin, Kryptoměna, Forenzní, Analýza

Annotation:

The thesis "Analysis of current cryptocurrency with focus on Bitcoin, securing the proceeds of crime." deals with the securing of cryptocurrency Bitcoin. The thesis describes selected current cryptocurrencies and their differences from Bitcoin. The thesis is focused on the issue of finding and securing cryptocurrencies in investigated devices detained in criminal activity. Based on the results of the research, optimal procedures for the provision and forensic analysis of cryptocurrencies are suggested.

Kkeywords:

Bitcoin, Cryptocurrency, Forensic, Analysis

Prohlašuji, že svoji diplomovou 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 diplomové 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.

České Budějovice, 18. dubna 2018

.....

podpis

Obsah:

1. Úvod

V současné době zažíváme mohutný technologický rozvoj, který přispívá k mnohým změnám lidského vnímání a zpracování informací. Za poslední roky se velmi výrazně zvýšila dosažitelnost elektronických zařízení a internetu. Díky větší dostupnosti informací si lidé začínají uvědomovat, jakým způsobem funguje monetární politika centrálních bank a obávají se tak důsledků uvolněné měnové politiky na jejich finanční prostředky. Znehodnocování peněz v důsledku inflace se snaží lidé předejít investicemi do různých komodit, například nemovitostí. I tyto investice ovšem podléhají mnoha omezením.

Rozvoj techniky a velké zpřístupnění internetu otevřelo na trhu prostor pro nové možnosti uložení peněz. Příležitosti využil Satoshi Nakamoto a začal pracovat na novém krypto-platebním systému, který byl představen v roce 2009. Na základě jeho práce byla specifikována první kryptoměna a to bitcoin. Nejednalo se ovšem o první koncept kryptoměny, ten publikoval Wei Dai již v roce 1998 jako novou možnost platby v budoucnosti.

Největší růst ceny zaznamenal bitcoin roce 2017, kdy za několik posledních měsíců tohoto roku jeho cena vzrostla ze 4000 dolarů na více než 15 000 dolarů. Za růstem pravděpodobně stojí rozsáhlé kvantitativní uvolňování, ale celkové příčiny růstu jsou zřejmě složitější.

Cílem této diplomové práce je zmapování problematiky současných kryptoměn, které je možné využívat v trestné činnosti. Z toho důvodu se zaměřím pouze na kryptoměny, se kterými je možné obchodovat a existuje u nich možnost převodu na fyzické peníze. Nejvíce se budu věnovat bitcoinu, protože se jedná o nejrozšířenější kryptoměnu a ostatní kryptoměny vycházejí z jeho pojetí. U dalších kryptoměn budou popsány odlišnosti od sítě Bitcoin. Vzhledem k tomu, že kryptoměny pracují na konceptu decentralizované měny, která nespadá pod správu žádné vlády ani organizace a nepodléhá žádným regulacím, lze usuzovat, že by mohly být užívány jako vhodný platební nástroj při trestné činnosti.

V teoretické části práce bude popsáno, co znamená pojem kryptoměna. Seznámíme se s historií kryptoměny bitcoin, na jakém principu kryptoměny fungují, jak se uskutečňují transakce, apod.

Praktická část je zaměřena na možnosti využití kryptoměn, je popsán platební styk s využitím kryptoměn. Další důležitou součástí je analýza anonymity při jejich používání. Bude zpracován postup detekce kryptoměny na forenzně zkoumaných zařízeních. V poslední části práce uvedu, na základě zjištění z předchozích zkoumání, jaká data je možné získat ze zkoumaných zařízení a jaké jsou další kroky využití nebo zabavení nalezené kryptoměny. Tato data budou vyhodnocena a převedena do podoby použitelné v dalším zkoumání.

2. Kryptoměna

Kryptoměna je jednou z digitálních měn. Digitální měnou se rozumí měna taková, která je vytvářena a uložena pouze digitálně a tudíž nemá žádnou fyzickou formu na rozdíl od konvenčních peněz, které jsou sice částečně uchovávány digitálně, ale mají fyzickou podobu – hotovost. V začátcích nebylo kryptoměnu možné směnit na fyzické peníze a nebylo možné s ní platit. To se za posledních let několik let změnilo. Nicméně v některých zemích, například v České Republice, nejsou zatím ze zákona kryptoměny považovány za měnu, ale za věc nehmotnou, movitou a zastupitelnou, jelikož nenaplňují znaky měny dle zákona o platebním styku (č. 284/2009 Sb.).

Mohlo by se zdát, že kryptoměna je nový termín, který je používán pouze několik posledních let, není to ale pravda. První teze digitálního platebního systému byla publikována již v roce 1998 v práci nazvané „b-money“ [1]. Na základě první teze pak stavěla práce vydaná krátce poté. Práce se jmenovala „bit gold“ (nejedná se o současnou kryptoměnu BitGold) a byla publikována Nickem Szabo. Oproti konceptu b-money, který se zabýval pouze myšlenkou platebního systému, byla myšlenka bit gold více podobná dnešním kryptoměnám. Koncept, který stál na pozadí bit gold, byl inspirován těžbou zlata. Autor popisuje i princip získávání této měny. Základní postup je velmi podobný metodě získávání dnešních kryptoměn, kdy je těžař odměňován za poskytnutí výpočetního výkonu a po spočítání určité požadované sekvence je odměněn právě jednou jednotkou dané měny. Z toho je vidět, že podobnost s těžbou zlata je zřejmá - horník odkopává bezcennou zem a po odklizení určité části je odměněn nálezem zlata. Ani jeden z nápadů (b-money, bit gold) se v době svého vzniku neujal, takže koncepce a jakýkoliv další rozvoj byly opuštěny až do roku 2008, kdy se na vývoji kryptoměny opět začalo pracovat. Právě v roce 2008 začala vznikat nejstarší a v dnešní době nejznámější kryptoměna Bitcoin [2].

Další prací, kterou je možné považovat za příspěvek k současnému systému fungování kryptoměn, je práce s názvem „Hashcash“ [3], kterou vypracoval britský specialista na šifry a hacker Adam Black. Jednalo se o protiopatření na zneužívání sítě k útokům DDoS (Distributed Denial of Services) a princip fungování dal také vzniknout dnešnímu systému CAPTCHA [4]. Ačkoliv to tak na první pohled nevypadá, fungování mělo podobné rysy jako těžba kryptoměny. Prvotní Hashcash, před vylepšeními a dalšími úpravami, fungoval na principu „něco za něco“. Uživatel požadující službu od serveru dostal vyřešit úkol, takové složitosti, která nepřesahovala režii dané služby, po vyřešení uživatel zaslal řešení zpět na server a server poskytl službu. Stejným způsobem funguje i systém CAPTCHA, který uživateli dá jednoduchý úkol, aby si ověřil, že není robot, ale člověk, a podle výsledku ho nechá pokračovat. Když se tato funkcionalita vezme obecně, je velmi podobná těžení kryptoměny, kdy za vykonanou práci těžař dostane odměnu v podobě jednotky kryptoměny.

Výše uvedené teze a myšlenky, které se na první pohled jeví jako nesourodé a neprovázané, daly vzniknout dnešním kryptoměnám a jejich přidruženým platebním systémům.

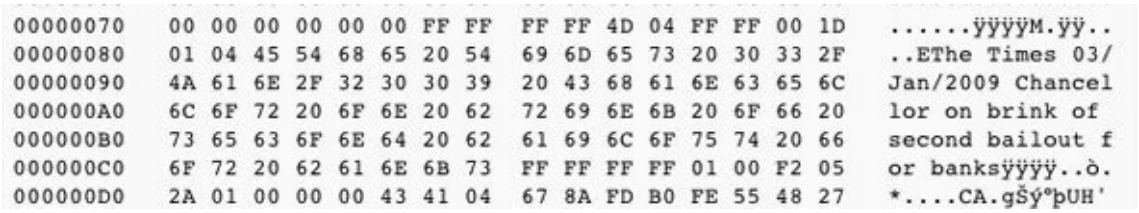
3. Bitcoin

Bitcoin je jednou z nejznámějších a nejstarších kryptoměn. Je jednou z mála kryptoměn, se kterou je možné platit za služby a zboží ve stále se rozšiřující síti obchodů. Ze zahraničních obchodů jde například o Newegg, Microsoft, Ovestock.com a další. V Čechách je asi největší firmou akceptující bitcoin Alza.cz, která také na vybraných pobočkách provozuje bitcoinové bankomaty od společnosti General Bytes. Další společností akceptující platby bitcoiny je například jihočeská společnost Wedos internet s.r.o. poskytující webhosting, server housing a další služby. Bitcoinové platby nejsou pouze výsadou elektronických obchodů, ale jsou to také restaurace a kavárny, které akceptují bitcoin. V Praze je více než 130 podniků akceptujících bitcoin [5], což je nejvíce z evropských metropolí.

3.1 Historie bitcoinu

První zmínka o bitcoinu je z 18. 8. 2008, kdy byla založena doména bitcoin.org [6]. V listopadu 2008 byla publikována práce „*Bitcoin: A Peer-to-Peer Electronic Cash Sys-*

tem“ [7]. Následně byl 3. 1. 2009 vydán software pro bitcoin ve formě opensource. Autorem výše uvedené práce byl Satoshi Nakamoto, bohužel se nejedná o autorovo pravé jméno, ale jen pseudonym. Podle spekulací za vývojem bitcoinu nestojí pouze jedna osoba, ale více jedinců. Téhož dne byl také vytěžen vůbec první blok, který byl vytěžen právě Nakamotem, měl hodnotu 50 BTC [8]. Jednalo se o tzv. „genesis block“ a bylo v něm uvedeno: „ Času 3. 1. 2009, kancléř na pokraji druhého záchranného balíčku pro banky“ [9]. Jednalo se o odkaz na kvantitativní uvolňování v Anglii a zároveň vzkaz, že je možná na čase zkusit něco jiného.



Obrázek 1: Genesis blok [10]

První vytěžený blok je neobchodovatelný, ze zdrojového kódu ale nevyplývá, proč tomu tak je.

Podle dostupných informací je největším držitelem bitcoinů právě zakladatel Nakomoto, který dle odhadů v počátcích vytěžil více než milion bitcoinů. Tato informace bohužel není ověřitelná, protože bitcoiny jsou uloženy v mnoha peněženkách a nikde není více než 50 BTC. Spekulace o množství bitcoinů vlastněných zakladatelem se opírá o rovnoměrné těžení jednoho zdroje – téhož zdroje, který vytěžil i úplně první blok.

Dalším velkým hráčem na poli s bitcoiny je americká FBI, která v současnosti podle veřejně přístupných informací drží kolem 144 000 BTC. Jedná se především o zabavené prostředky [11].

První uskutečněnou bitcoinovou transakcí byl 12. 1. 2009 převod bitcoinů od Nakamota Halu Finleyemu. Dalšími uživateli systému byli v této době Wei Dei, autor práce „b-money“ [1] a Nick Sazbo, autor konceptu „bitgold“[2].

Od roku 2010 je s bitcoinem spojováno jméno Gavin Andresen, jemuž bylo předáno do správy Bitcoin Core – úložiště, ve kterém je možné měnit parametry bitcion protokolu. Všechny závažnější změny v protokolu však musí být schváleny všemi vývojáři [12].

V září 2012 byla založena nezisková organizace s názvem Bitcoin Foundation [13], která zajišťuje konference na téma Bitcoin, zvedá povědomí o této kryptoměně, financuje vývojáře bitcoin protokolu, spravuje granty spojené s vývojem bitcoinu a další. V čele

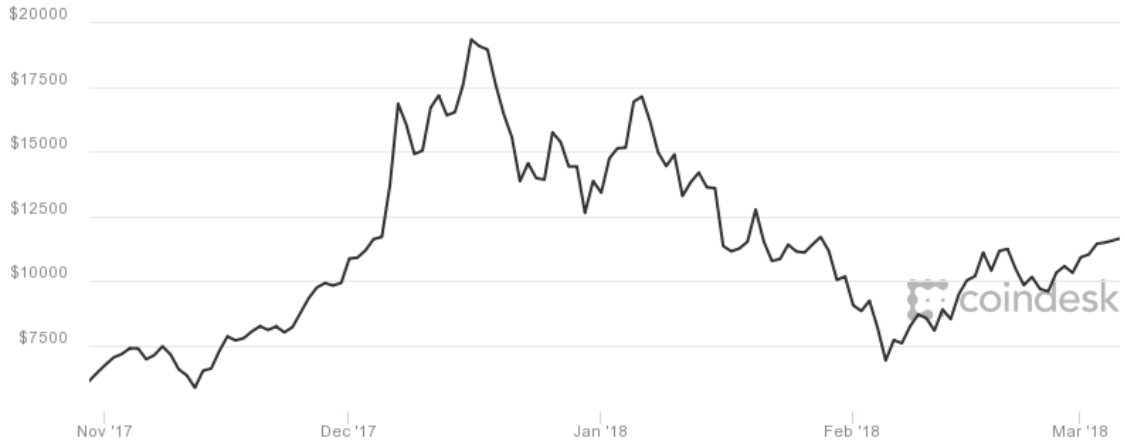
Bitcoin Foundation stanul právě Gavin Andresen spolu se správní radou. V roce 2014 odstoupil z pozice hlavního vývojáře Bitcoin Core a stal se hlavním vědcem v Bitcoin Foundation. Nyní je hlavním vývojářem a správcem Bitcoin Core Wladimir van der Laan, který je také nejaktivnějším přispěvatelem do kódu.

Na začátku roku 2017 byl také přidán znak bitcoinu ₿ do sady unicode 10.0, stalo se tak po neúspěšném pokusu z roku 2011, kdy byl znak zamítnut. Od letošního roku tedy najdeme znak pro bitcoin ve všech systémech obsahující unicode verze 10.0 – například Windows 10 Creators Update, macOS Sierra a další. Bitcoin má také zkratku jako standardní měny a to sice BTC. S tím také souvisí rozlišení systému od mince, kdy systém používá na začátku velké písmeno B, měna malé písmeno b a mince právě BTC.

3.2 Cenový vývoj

Kryptoměny jsou velmi volatilní. Cenový vývoj může vykazovat velmi rychlé změny, bitcoin není výjimkou. Od jeho založení do května roku 2010, kdy neměl téměř žádnou hodnotu, se cena pohybovala v setinách a tisícinách dolaru. V červnu roku 2010 zažil bitcoin první nárůst ceny o více než 900 % z 0,008 na 0,8 dolaru. Od února 2011 do dubna 2011 bitcoin tvořil paritu s dolarem, tzn. 1 BTC = 1 US Dolar. 8. července 2011 dosáhla cena na 31 dolarů za 1 BTC, po tomto růstu následoval v prosinci 2011 pád na 2 dolary. Od roku 2012 pozvolna rostl a cena za bitcoin v tomto období již neklesla pod 100 dolarů.

Největší výkyvy ceny zaznamenal bitcoin v posledních měsících roku 2017. Od ledna 2017 cena stoupala rychlým tempem. Od listopadu do 16. prosince 2017 vzrostla cena bitcoinu až na dosud nejvyšší hodnotu 19 185 dolarů za 1 BTC. Po tomto vrcholu následoval pád, který se zastavil 5. 2. 2018 těsně pod hranicí 7000 dolarů za 1 BTC. Z výše popsaného vývoje cen se nabízí otázka, co určuje cenu bitcoinu. Má bitcoin tak vysokou cenu proto, že je možné ho používat jako formu peněz? Má podobné charakteristiky jako fyzické peníze a to sice tyto: trvanlivost, přenositelnost, fungování, nedostatek, dělitelnost a rozpoznatelnost [14]. Cena bitcoinu je však podle mého názoru primárně určena nabídkou a poptávkou. Bitcoinů je omezené množství a s rostoucí poptávkou roste také jeho cena. Dalším faktorem v pohybech ceny je pravděpodobně to, že tisíc největších bitcoinových investorů na světě vlastní více než 40% všech bitcoinů na trhu [15] a tudíž je pro ně velmi snadné cenou za bitcoin manipulovat.



Obrázek 2: Graf cenového vývoje bitcoinu [16]

3.3 Princip fungování

Bitcoin je decentralizovanou kryptoměnou, jejíž fungování je založeno na veřejné účetní knize a na ověřování transakcí v ní zapsaných. Decentralizované řešení je takové, které nemá žádný centrální řídící prvek. Budeme-li uvažovat o tom, že bitcoin je měna, tak nejlepší analogií je klasický peněžní systém. Pokud provedeme jakoukoliv elektronickou peněžní transakci v klasické měně (koruny, dolary apod.), vždy naše transakce prochází centrálním uzlem, ve většině případů se jedná o banku. Tento centrální uzel má přehled o všech transakcích a také udržuje zůstatky na účtech. Tyto informace nejsou veřejně dostupné a koncoví uživatelé mají přehled pouze o svých transakcích. Bitcoin funguje přesně opačně – není zde žádný centrální prvek, přes který by se transakce zpracovávaly. Všichni uživatelé mají přístup do veřejné účetní knihy nazvané Blockchain, kde jsou zaznamenány všechny provedené transakce. Systém je koncipován tak, aby nemusela být vkládána důvěra ve třetí strany. To by ovšem nestačilo, je nutné samotné transakce ověřovat, aby nedošlo k dvojímu utrácení. Na to se používají tzv. těžaři a koncept zvaný Proof-of-Work, kterým se zabývám v samostatné kapitole.

3.3.1 Blockchain

Blockchain je v případě kryptoměn veřejně přístupná účetní kniha, do které se zapisují všechny transakce. Blockchain obsahuje bloky se záznamem o všech transakcích v rámci daného bloku. Transakce jsou skutečná data, která jsou ukládána v Blockchainu. Bloky jsou užívány pro ověření kdy a v jakém pořadí se transakce zapsaly jako součást Blockchain databáze. Transakce jsou vytvářeny uživateli platebního systému při každém pohybu včetně zaslání prostředků sám sobě. Bloky jsou vytvářeny a ověřovány uživateli

označovanými za těžaře (miners), kteří za pomoci hardwarového a softwarového vybavení vytvářejí a ověřují bloky. Těžaři za tuto práci dostávají zaplaceno v podobě čerstvě vytěžených bitcionů a části poplatků z provedených transakcí.
Struktura bloků v Blockchainu je následující:

- velikost bloku – 4 bytes,
- hlavička bloku – 80 bytes,
- čítač transakcí – 1- 9 bytes,
- transakce – proměnná velikost [17].

3.3.1.1 Velikost bloku

Současná velikost bloků je omezena na maximální hodnotu 1MB. V posledních několika letech je maximální velikost bloků velmi diskutována v souvislosti s rychlostí transakcí. Zvětšení bloků má výhodu v podobě možnosti uskutečnit více transakcí, ale nevýhodu v podobě větší paměťové náročnosti na uzlech. S rostoucím zájmem o bitcoin roste i velikost bloků. Do května 2012 byla velikost bloku do 40kb. Od té doby víceméně stabilně roste a v říjnu 2015 se přehoupla přes 50% maximální velikosti, tzn. 500kb. V roce 2017 se již několikrát velikost přiblížila maximální velikosti, kdy velikost bloků stabilně přesahuje 950kb [18].

3.3.1.2 Hlavička bloku

Hlavička bloku obsahuje tyto části:

1. verze,
2. hash předešlého bloku,
3. Merkle root,
4. časové razítko,
5. cíl pro obtížnost,
6. nonce. [19]

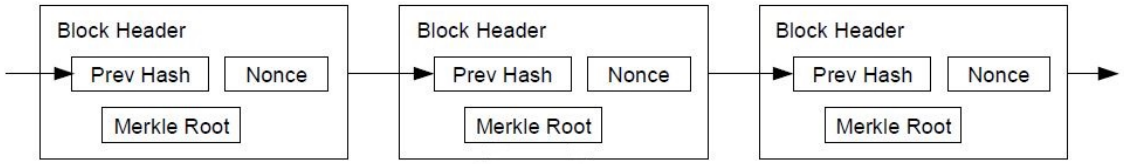
1. Verze

Verze se používá pro vyhledání změn v protokolu nebo softwaru. Aktuální verze je 4 z roku 2015. Verze 1 byla uvedena v roce 2009 při vzniku prvního (genesis) bloku. Verze 2 byla uvedena v roce 2012 s verzí jádra (bitcoin core) 0.7.0. Tato verze uvedla nová pravidla pro přijímání nových bloků a přestala přijímat nové bloky verze 1. Verze 3

v lednu 2015 byla uvedena současně s verzí jádra (bitcoin core) 0.10.0. V červenci začala tato verze požadovat kódování DER (Distinguished Encoding Rules). Aktuální verze z listopadu 2015 s verzí jádra 0.11.2 zavádí funkci OP_CHECKLOCKTIMEVERIFY, která by měla umožnit vrácení transakcí [20].

2. Hash předešlého bloku

Hash předešlého bloku je ukotven v každém bloku hlavně z důvodu ochrany proti manipulaci s transakcemi v bloku. Pokud bude potencionální útočník chtít manipulovat s jednou nebo více transakcemi, které jsou již v bloku zapsány, vyústí to ve změnu Merkle root, což změní hash celé hlavičky bloku. Aby pozměněný blok prošel, musel by útočník vynaložit velké množství prostředků na spočítání nové nonce pro daný blok a provést rehash pro danou hlavičku. To ovšem nestačí k tomu, aby se jeho blok dostal do sítě, jelikož každý další vytěžený blok po tomto upraveném, obsahuje hlavičku toho předchozího nezmanipulovaného. Z toho vyplývá, že nestačí provést rehash pouze jednoho bloku, ale všech následujících bloků [21]. Tohle je teoreticky uskutečnitelné, pokud by útočník měl alespoň 51% veškerého výkonu sítě.



Obrázek 3: Hlavička bloků [22]

3. Merkle root

Dalším prvkem hlavičky bloku je Merkle root, což je kořen stromového algoritmu Merkle tree. První práce na téma kryptograficky zabezpečeného řetězce bloků byla publikována v roce 1991 Stuartem Haberem a W. Scotem Stornettem s názvem „How to time-stamp a digital document“ v časopise o kryptologii [23]. V roce 1992 autoři v této práci pokračovali a spolu s Davem Bayerem vydali „Improving the Efficiency and Reliability of Digital Time-Stamping“. V této práci byl zveřejněn právě Merkle trees (patentován v roce 1979 Ralphem Merklem). Pomocí tohoto stromu je možné zřetězit hashe z více hashů postupně do jednoho konečného a tím výrazně ušetřit místo.

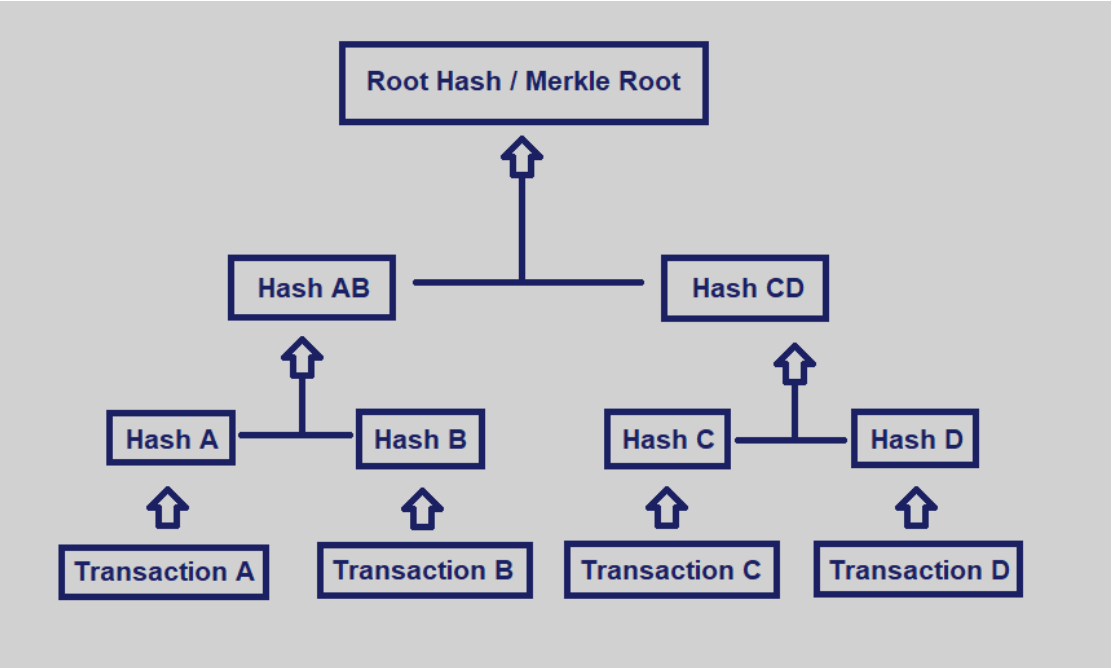
Merkle tree algoritmus tedy funguje na principu zřetězování hashů. Obsahuje 3 stavební prvky: listy, uzly (větve) a kořen (root hash). V listech je obsažena hash funkce přidružených dat k danému listu. Uzly se vytvářejí zřetězením hashe dvou sousedních

listů. V dalším kroku se vytvoří další vrstva uzlů zřetězením dvou potomků. Tento postup se opakuje, dokud není dosaženo vrcholu stromu a všechny uzly nejsou zřetězené do jednoho kořenového uzlu. Obvykle má Merkle tree rozvětvovací faktor roven 2. To znamená, že každý uzel má 2 potomky.

Tento strom je používán hlavně v peer-to-peer systémech, kde je potřebné ověřování dat. Protože jsou P2P sítě decentralizované, nacházejí se stejné informace obvykle na více místech. Z toho plyne, že pokud dojde ke změně, je potřeba data upravit na všech místech, kde se data vyskytují. Kontrolovat úplnost každého souboru, kdykoliv chce systém ověřit data, je velmi časově a výpočetně náročné. Z těchto důvodů je použití Merkleho stromu velmi výhodné. Omezíme množství dat odesílaných přes síť, místo celého souboru zasíláme pouze jeho hash a zjišťujeme, jestli se shoduje.

Protokol tedy funguje následovně:

1. počítač A zašle hash souboru počítači B;
2. počítač B zkontroluje hash proti kořenovému hashi v kořeni Merkleho stromu;
3. pokud se hashe shodují, algoritmus končí, pokud ne, pokračuje dál;
4. pokud se hash liší, počítač B zažádá o kořeny dvou podstromů této hashe;
5. počítač A vygeneruje požadované hashe a zašle je počítači B;
6. opakují se kroky 4 a 5, dokud není nalezen soubor, který se změnil. [24]



Obrázek 4: Merkle Tree [25]

Tímto způsobem je možné nalézt víc než jeden soubor, který se změnil. Z výše uvedeného tedy vyplývá, že tento algoritmus je efektivní pouze v případě, že počítač generuje hashe rychleji než by trvalo zaslání a porovnání celého souboru. Algoritmus není používán pouze v peer-to-peer sítích, ale například také v některých souborových systémech jako je ZFS, IPFS, Btrfs. V peer-to-peer sítích se využívá hlavně v blockchainu sítí kryptoměn jako je právě Bitcoin, Ethereum a další. Právě hash kořenu tohoto stromu se používá jako jedna ze součástí hlavičky bloku v Blockchainu [26].

4. Časové razítko

Časové razítko není vydáváno žádnou certifikační autoritou, jak je tomu běžně v případě tohoto termínu například u dokumentů. V hlavičce bloku je časové razítko určováno na základě přesně specifikovaných pravidel. Časové razítko je považováno za platné, pokud je větší než medián časových razítek předchozích 11 bloků a méně než nastavený čas v síti + dvě hodiny. Nastavený čas v síti je medián časových razítek vrácených od všech připojených uzlů. Z toho důvodu není čas v časových razítkách příliš přesný. Přesnost časového razítka bloku je v rozmezí jedné až dvou hodin.[27].

5. Cíl pro obtížnost

Úroveň obtížnosti kompenzuje výkyvy ve výkonu sítě, aby vytěžení nového bloku trvalo průměrně 10 minut. Z toho plyne, že s nárůstem počtu těžařů a výpočetního výkonu by se tento čas výrazně zkracoval, pokud by se neupravovala obtížnost a v opačném případě by se čas opět mohl výrazně prodlužovat. Prodloužení času potřebného k vytvoření nového bloku přímou měrou ovlivňuje počet transakcí za vteřinu, podrobněji v kapitole Transakce. Stejně jako v případě časového razítka i tyto úpravy se řídí přesně specifikovanými pravidly. Úprava obtížnosti se provádí každých 2015 bloků (dříve 2016) z důvodu tolerance odchylky byl jeden blok ubrán. V rámci jedné úpravy se obtížnost nesmí zvýšit o více než 300 % a snížit o více než 75 %.[28] Úprava obtížnosti se provádí podle níže uvedeného vzorce.

$$Nová\ obtížnost = \frac{(časové\ razitko\ 2015.\ bloku - časové\ razitko\ 1\ bloku)}{20160} * aktuální\ obtížnost$$

Ze vzorce vyplývá, že pokud vyjde hodnota zlomku větší než jedna, obtížnost se zvyšuje, pokud je naopak hodnota menší než jedna, obtížnost se snižuje. [29]

Dalším pojmem je pojem cíl (target). Velmi často jsou pojmy obtížnost a cíl zaměňovány. Ačkoliv jsou spolu svázány, neznamenají to samé. Cíl je 256-bitové číslo, které

je sdíleno všemi klienty. SHA-256 hash hlavičky bloku musí být nižší nebo roven současnému cíli, aby byl blok přijat do sítě. Čím nižší číslo cíle, tím obtížnější je nalézt správný cíl. Spíš než o matematicky stanovený problém to lze přirovnat k loterii. Každý generovaný hash vrátí hodnotu mezi 0 a 256 bitovým číslem. Pokud jsme spočítali hash pod cílovou hodnotou, vyhráváte. Pokud ne, upraví se nonce a výpočet se provádí znovu [30].

6. Nonce

Nonce je 32-bitové číslo, které je potřeba nastavit tak, aby výsledný hash začínal nulou. Nonce je tedy proměnná, která se přidává k ostatním součástem hlavičky bloku a jako jediná se mění. Právě za pomoci změny nonce se dostaneme pod nastavený target. Jako příklad nám poslouží fráze Hello world!, jejíž hash chceme spočítat tak, aby začínal 000. Vezmeme tedy frázi Hello world! a vytvoříme hash, který nezačíná nulou, přidáme k frázi nulu na Hello world!0 a znovu vytvoříme hash a takto pokračujeme, dokud fráze plus přidané číslo, naše nonce, neutvoří požadovaný hash s 000 na začátku. Z obrázku 5 vidíme, že požadovaná nonce je 4250, museli jsme spočítat tedy 4251 případů, než se nám podařilo dostat požadovaný hash. Tato hodnota se může jevit jako vysoká, ale i starší procesor jako je Intel Core 2 Duo E8400 (2008) zvládne vypočítat cca 100 hashí za vteřinu. Specializovaný hw jako AntMiner zvládne vypočítat 13,5 tera-hashí za vteřinu.

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Obrázek 5: Příklad použití nonce [31]

3.3.1.3 Transakce

Poslední částí, kterou Blockchain obsahuje, jsou transakce. Maximální počet transakcí uložených v bloku je omezen maximální velikostí bloku, která činí zatím pouze 1MB. Průměrná velikost jedné transakce je kolem 500B. Velikost se mění v řádech desítek bajtů, ale zatím nepřekročila více než 713B na jednu transakci [32]. Jeden blok může obsahovat až 1 999 transakcí. Pokud tuto hodnotu aplikujeme na pravidla pro vytěžení nového bloku, která jsou nastavená tak, aby byl nový blok vytěžen přibližně každých 10 minut, tak z toho zjistíme, že teoretické maximum jsou tři transakce za vteřinu (reálně

dvě). Při současném nárůstu zájmu je tato rychlost nedostatečná a obvykle trvá velmi dlouho, než transakce vůbec přijdou na řadu. Číslo zpracovaných transakcí je velmi nízké při porovnání s konvenčními platebními systémy. Například platební brána internetové služby PayPal je schopná zpracovat průměrně zhruba 193 transakcí za vteřinu – to je ve srovnání s bitcoinem mnohonásobně víc. Síť elektronických plateb a karet VISA v průměru zvládne odbavit 1 667 transakcí za vteřinu [33]. Samozřejmě toto porovnání není zcela přesné, protože se jedná o dvě rozdílné technologie, kdy VISA a PayPal jsou centralizované a kryptoměny nejsou, ale vzhledem k tomu, že bitcoin má ambice stát se plnohodnotným platebním systémem, měla by se rychlost výrazně zvýšit. Na téma transakční rychlosti sítě Bitcoin se vede již diskuze několik let, ale zatím nebylo rozhodnuto o způsobu, kterým se rychlost navýší.

U transakcí je nutné si uvědomit, že uživatel nemá ve své bitcoinové peněžence bitcoiny jako takové, ale pouze adresy, na kterých se nacházejí. Z těchto adres a za pomoci Blockchainu se dá vygenerovat, kolik bitcoinů daná osoba vlastní. V žádné peněžence není odkaz na místo uložení - například na pevném disku, který by nám ukázal a řekl: „tohle je bitcoin“, tak jak je tomu u tradičních peněz. Bitcoin je uložený v transakcích a je složený ze tří věcí: vstup transakce – bitcoinová adresa, odkud jsme bitcoin obdrželi; výstup transakce – bitcoinová adresa, kam jsme bitcoin odeslali – pokud je bitcoin v našem vlastnictví bude tato adresa pod naší kontrolou a množství odeslaných bitcoinů. Tímto způsobem zjistíme, kolik bitcoinů uživatel vlastní, protože Blockchain uchovává transakce od nultého bloku.

K uskutečnění transakce musíme mít adresu, na které se nacházejí bitcoiny uživatele a odpovídající soukromý klíč k této adrese. Bitcoinová adresa je složený řetězec alfanumerických znaků o délce 26 – 35 znaků a má podobnou funkci jako například emailová adresa. Soukromý klíč je opět sekvencí písmen a číslic o délce 256 bitů. Toto funguje jako bychom měli průhledný trezor, všichni vidí, co je uvnitř, ale pouze vlastník soukromého klíče ho může otevřít a nakládat s prostředky uvnitř.

Transakce probíhají následovně:

Otevřu si svoji „peněženku“ a řeknu, že chci zaplatit za službu např. 1 BTC.

Vyplním tedy adresu příjemce a odešlu.

Transakce se podepíše pomoci mého privátního klíče a je zaslána do sítě.

Následně je přidána do nového bloku, který je potřeba vytěžit.

Po vytěžení bloku je transakce potvrzena – příjemce vidí její potvrzení.

Transakce se nekombinují, takže v peněžence jsou uloženy různé sumy z předchozích transakcí. Pokud peněženka obsahuje adresu příchozí transakce za 1 BTC, tak se pouze tato adresa odstraní z peněženky a převede se do peněženky druhé strany. Pokud adresa obsahuje například 3 BTC a chci poslat pouze jeden bitcoin, situace se změní. Postup zůstane stejný, ale transakce bude obsahovat dvě výstupní adresy. Jedna adresa bude pro příjemce s částkou 1 BTC a druhá adresa se bude vracet do mojí peněženky s částkou 2 BTC. Touto transakcí se tedy vytvoří 2 nové transakční adresy. Je to dáno tím, že bitcoinové transakce nejsou dělitelné. Tudíž je nutné, aby stará transakce zanikla – místo ní je vygenerována nová. Je však možné zbytek bitcoinu zaslat opět na starou adresu.

Při každé transakci je třeba počkat na potvrzení od sítě. Při každé platbě je vytvořeno transakční id a podle něj si můžeme zkontrolovat, kolik potvrzení daná transakce má. U vyšších plateb bychom měli počkat na více než jedno potvrzení z důvodu možných útoků – viz kapitola Problémy a možné útoky. Pokud nedojde k potvrzení transakce do 72 hodin, je možné transakci znovu zaslat [34].

V ideálním případě by se první potvrzení se mělo uskutečnit maximálně do 10 minut. Jak je ale uvedeno výše, je v současné době reálná výkonost sítě pouze 2 transakce za sekundu a tudíž ověření platby může trvat i několik hodin. Důvodem je fakt, že se nejprve musí zpracovat transakce došlé před naší transakcí a musíme čekat, než se dostaneme do nového bloku. Po odeslání platby se obvykle dozvíme předpokládané zdržení o x bloků. Dalším faktorem v rychlosti potvrzení transakce jsou nastavené poplatky u naší transakce. Těžaři obvykle těží prioritně bloky s vyššími poplatky a tudíž s vyšším ziskem pro ně. Nyní je výše poplatku s nejkratším zpracováním a zároveň nejnižší cenou 200 satoshis za byte [35].

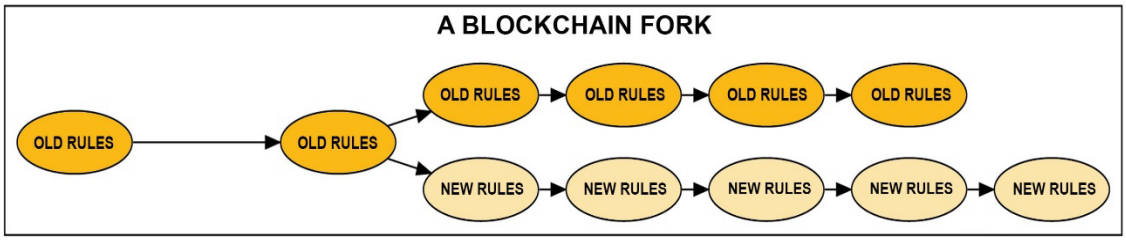
3.3.2 Fork v Blockchainu

Jedná se o rozdělení nebo také rozvětvení Blockchainu. K těmto rozdělením může docházet v případě, že dva těžaři vytěží blok ve stejný čas. V síti se tak objeví dva bloky stejného pořadového čísla. Aby nedošlo k trvalému rozdělení, je jeden blok sítí odmítnut a stane se z něj tzv. sirotek. Všechny další bloky za sirotkem se již budou hlásit jako nevalidní a bude se pokračovat pouze v hlavním řetězu.

K dalšímu rozvětvení dochází při změnách v síti. Protokol bitcoinu se stále vyvíjí, dochází novým k úpravám a změnám. Tyto změny ústí v nová pravidla. V těchto

situacích se rozlišují dva druhy rozdělení: soft fork a hard fork. V případě soft fork se jedná o drobná vylepšení, která mají přínos pro protokol, ale změna to není tak výrazná, aby to omezilo zpětnou kompatibilitu. Je tedy možné s bloky pracovat podle nového i starého protokolu. Tato změna může být aktivována těžaři (MASF), případně může být aktivována uživateli full nodů (UASF). Když je přidán soft fork, musejí mu porozumět jak uživatelé, tak těžaři. To se provede zasláním speciální transakce na staré klienty a těžaře, kteří potvrdí, že budou odmítat nové transakce podle starých pravidel. Aby tyto změny mohly platit, musí se na nich shodnout většina sítě. I v případě dohody a shody se může stát, že se Blockchain rozdělí na určitý počet bloků, než všichni začnou fyzicky dodržovat nová pravidla [36].

Naproti tomu hard fork je nová verze protokolu, která není zpětně kompatibilní s verzí stávající. Pokud část sítě s navrhovanými změnami nesouhlasí, může se odtrhnout a vytvořit hard fork. K odtrhnutí dojde zkopírováním stávajícího protokolu bitcoinu a naimplementováním vlastních pravidel. Toto je možné díky tomu, že kód bitcoinu je opensource a tedy veřejně dostupný. V protokolu je dále specifikováno číslo bloku, od kterého začne nový protokol platit. Tyto forky mohou být úspěšné a vydrží mnoho let po boku originální mince nebo můžou rychle ztratit podporu a zaniknout. Uživatelé na této situaci mohou potencionálně vydělat, jelikož se jedná o odštěpení ze stávajícího Blockchainu. Uživatel, který měl například 10 BTC, bude mít i nyní 10 jednotek podle nového protokolu, tedy zdvojnásobí počet mincí. Aby to pro uživatele mělo reálný přínos, musí se stát kryptoměna podle nového protokolu obchodovatelnou.



Obrázek 6: Blockchain fork [37]

V historii bitcoinu už k těmto hard forkům došlo několikrát:

Bitcoin XT – získal pozornost v roce 2015, zavedl zvýšení velikosti bloku z 1MB na 8MB, dosáhl velké podpory od více než 1000 uzlů, nicméně na začátku roku 2016 začala tato podpora klesat a na začátku roku 2017 se podpora snížila na cca 30 uzlů a stále klesá [38].

Bitcoin Classic – byl dalším forkem v pořadí, který přišel v únoru roku 2016 a opět přinesl zvětšení bloků. Tentokrát pouze na dvojnásobek tedy z 1MB na 2MB, nicméně i tento fork byl ukončen pro nedostatek podpory a vývojáři se přesunuli k Bitcoin Cash. [39]

Bitcoin Unlimited – není hard forkem v pravém slova smyslu, spíš se jedná o iniciativu, která se snaží udělat průzkum mezi uživateli, jestli stojí o změnu a navýšení velikosti bloků či nikoliv. V současné době se jedná pouze o klientský sw. Ten dovoluje uživatelům potvrzovat i bloky větší než je 1MB. Bohužel se také nedočkal velké podpory. [40]

V letošním roce došlo ke dvěma hard fork – v srpnu a říjnu na Bitcoin Cash a Bitcoin Gold.

Bitcoin Cash – je odtržením od Bitcoinu. Došlo k němu v srpnu roku 2017. Jako v předchozích případech se opět jednalo o velikost bloků a tím zrychlení transakcí. Bitcoin Cash zvedl velikost bloku z 1MB na 8MB stejně jako tomu bylo u Bitcoinu XT. Odstranil určité části z transakce jako takové, aby se i samotné transakce zmenšily a vešlo se jich do bloků ještě více. Tvůrci Bitcoin Cash doufají, že se jim podaří razantně zvýšit počet transakcí za sekundu na úroveň ostatních platebních služeb, jako je například PayPal. Je otázkou, zda bude tato nová kryptoměna dlouhodobě podporována a uchytí se, nebo se bude opakovat podobný scénář jako s BitCoin Classic, který byl ukončen a vývojáři přešli k nové měně [41].

Bitcoin Gold – je nejnovějším odtržením od Bitcoinu, ke kterému došlo v říjnu 2017. Bitcoin Gold transformuje krypto-algoritmus Bitcoinu SHA256 na Equihash. Velikost a ani rychlost těžení bloků se neliší, tzn. jeden blok každých cca 10 minut. Rozdíly jsou v obtížnosti, která se upravuje po každém bloku, Největším rozdílem je právě krypto-algoritmus, který nevyužívá acis pole, ale grafické karty. Hlavním impulsem bylo narovnání prostředí těžby, kdy u současného Bitcoinu je těžba možná pouze na specializovaných asic polích, které zvýšily obtížnost svojí výkonností nad možnosti běžných CPU i GPU a tak se vytvořil monopol pro firmy vyrábějící tato asic pole. Mohou proto držet celou výpočetní sít jako rukojmí [42].

Jestli budou mít nově odtržené mince větší úspěch se ukáže až postupem času. Základním předpokladem pro úspěch je tržní kapitalizace přes 1 miliardu dolarů a obchodovatelnost na burze. Tyto podmínky Bitcoin Cash i Gold již splňují.

3.3.3 Proof of Work

Proof of Work znamená ve volném překladu důkaz o vykonané práci. Používá se v systémech vyžadujících ověření. Obecně jsou systémy pracující s metodou proof-of-work, dále jen PoW, odolné proti běžným útokům typu DDoS (Distributed Denial of Services), spamu a dalším. Tato odolnost je dána tím, že pokud chceme něco od systému, musíme vykonat určitou práci, za kterou dostaneme odměnu – například přístup do daného systému. Úkol musí být dostatečně složitý, ale únosný na straně žadatele a zároveň jednoduše ověřitelný na straně provozovatele. Hlavním znakem je tedy asymetričnost. PoW je založen obvykle na výpočtu, který se vypočítá na procesoru nebo grafické kartě bez zásahu uživatele. Na rozdíl od modelu CAPTCHA, který je vyhotovený tak, aby ho člověk snadno a rychle vyřešil, u PoW není vyžadován žádný zásah od uživatele, vše obstarává výpočetní výkon stroje.

V případě kryptoměny bitcoin je tento systém použit na odhalování případného manipulování se sítí pomocí hashe. Bitcoin používá SHA-256 hash, každý blok má jedinečnou hash a i sebemenší úprava dat znamená změnu hashe. Práci vykonávají těžaři a data ověřují uzly sítě. Aby byla uznána odvedená práce, musí být požadovaný hash menší než target (viz kapitola Cíl pro obtížnost). Toho docílí těžaři přidáním tzv. nonce (viz kapitola Nonce). PoW tedy dělá velmi obtížné jakékoliv manipulace s bloky, protože by bylo potřeba „přetěžit“ kromě zmanipulovaného bloku také všechny následující bloky. Toho lze dosáhnout pouze v případě velkého výpočetního výkonu, více se tomu věnuji v kapitole Problémy a možné útoky.

Vzhledem k možným útokům na PoW, vznikla myšlenka na nový princip a tím je Proof-of-Stake (důkaz o vkladu), dále jen PoS. PoS je další možností ověřování transakcí v blocích. Hlavní změna je právě v systému ověřování, kdy se nemusí provádět žádné výpočty jako v případě PoW. U PoS musí uživatel prokázat vlastnictví určitého množství dané kryptoměny. Uživatel pro ověření bloku je zvolen pseudo-náhodnou cestou a to sice na základě jeho tzv. zdraví, která je definováno podle vkladu (stake). V tomto případě se nehovoří o těžařích, ale o kovářích (forgers). U tohoto ověřování je vhodné použít takovou měnu, která vydala všechny mince na začátku a má konečný počet mincí nebo původní vydání mincí zajistí pomocí PoW a poté přejde na PoS. „Kováři“ nedostávají odměnu v podobě mincí, ale dostanou zaplaceno z poplatků za transakce. Ověření bloků probíhá tak, že vybraný kovář dá do zástavy svoje mince (vklad), které by měly zajistit

čestné ověření transakcí. Pokud se odhalí ověření podvodných transakcí, kovář o svoje mince přichází a je vyloučen z dalšího ověřování transakcí.

U PoS jsou v zásadě používány dvě metody výběru uživatelů, kteří budou ověřovat transakce:

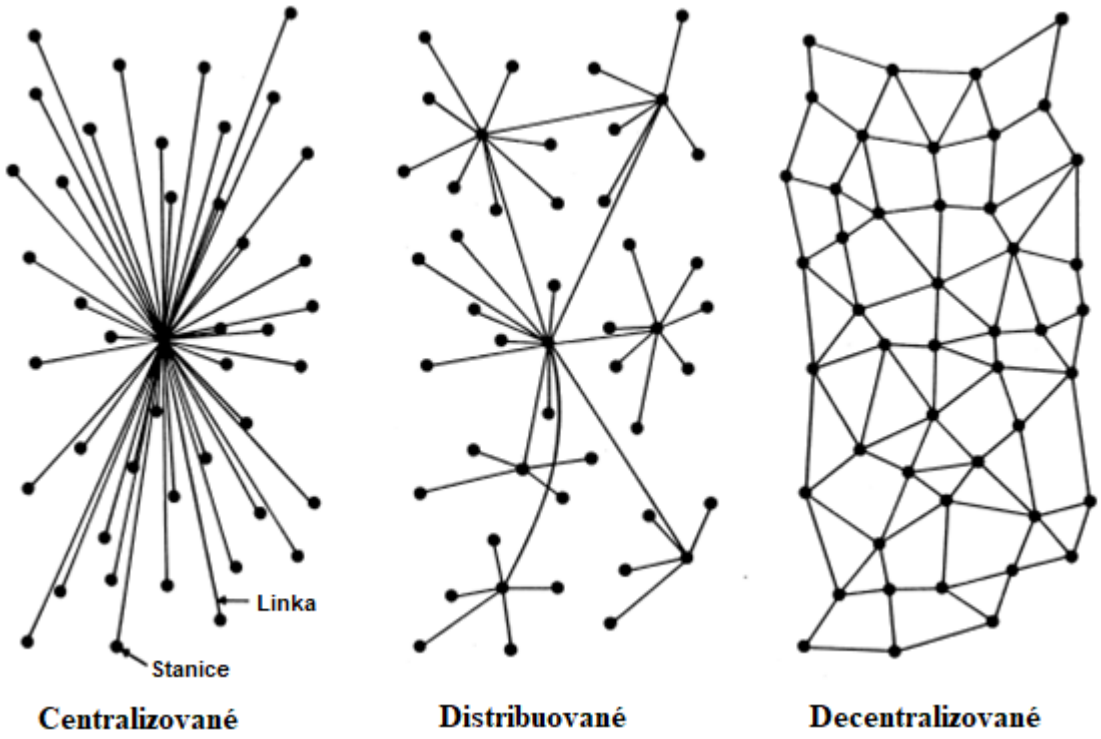
1. Náhodný výběr bloků – v tomto případě algoritmus hledá kombinaci uživatele s nejnižším hashem a výší jeho vkladu. Jelikož velikost vkladu je veřejná informace, může podle toho uzel předpovědět uživatele, který potvrdí další blok.
2. Na základě stáří mincí – tento algoritmus vyhodnocuje velikost vkladu a stáří držených mincí. Aby byl uživatel zvažován, musí držet mince minimálně po dobu 30 dní. Pokud uživatel ověří blok, je věk jeho mincí resetován zpět na nulu a musí čekat opět alespoň 30 dní. Tento uživatel je přiřazen k vytvoření dalšího bloku během maximálně 90 dní, aby se předešlo ovládnutí ověřování transakcí uživateli s velkým a velmi starým vkladem.

Celkově je tento princip více energeticky šetrný, protože není potřeba vysokého výpočetního výkonu k ověřování transakcí. Aktuálně tento princip používají kryptoměny: BlackCoin, Lisk, Nxt a Peercoin. Ethereum prověřuje možnosti přechodu, a i u Bitcoinu začíná diskuze na toto téma [43].

3.4 Decentralizace Bitcoinu

Bitcoin byl založen na myšlence decentralizované měny, která nebude ovlivňována žádným hlavním bodem, jako je tomu v případě fyzických peněz, které ovlivňují centrální banky. Nejprve je důležité si uvědomit, co vlastně znamená, pokud je systém decentralizovaný a jaké jsou další možnosti.

Rozlišujeme tři základní architektury systémů: centralizovaný, distribuovaný a decentralizovaný.



Obrázek 7: Architektura systémů [44]

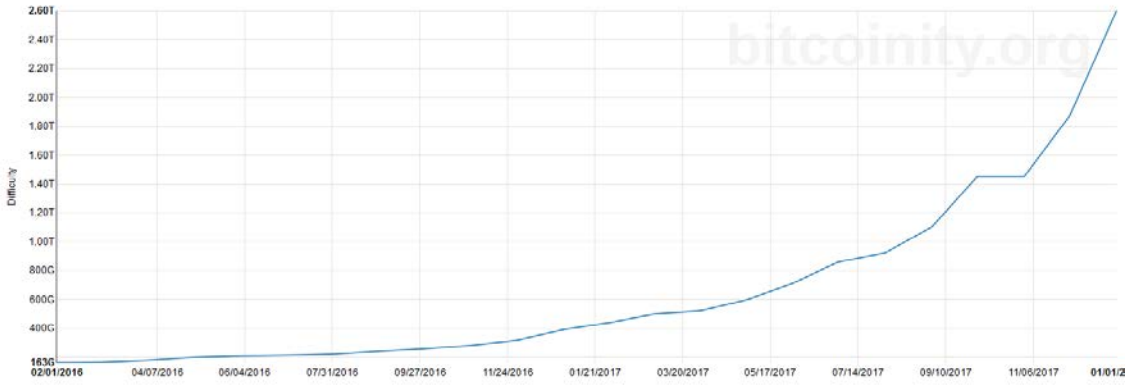
Centralizovaná síť je taková, která obsahuje jeden centrální prvek, který odesílá data na koncové stanice. Tento model je velmi jednoduchý na implementaci. Lze velmi snadno upravovat parametry sítě, poskytované služby a další, ale také jsou zde značné nedostatky. Prvním, asi nejzásadnějším nedostatkem je právě centrální řídící uzel. Pokud tento uzel přestane pracovat, znamená to výpadek pro celou síť. V současné době je tento problém zabezpečen záložním uzlem nebo uzly, které se aktivují v případě výpadku hlavního uzlu, ale to může nějakou dobu trvat. Další nevýhodou je omezenost a unifikace přístupu. Přistupující uživatelé musejí využívat stejných procesů k přístupu k hlavnímu uzlu a tato skutečnost může některým uživatelům zabránit v přístupu. Z toho vyplývá poslední nevýhoda a tím je zabezpečení. U centralizovaného systému máme jeden přesně daný bod, na který je možné zacílit v případě útoku. Obvyklým útokem na tyto centrální uzly je útok typu DDoS, který daný uzel přetíží množstvím požadavků nebo počtem uživatelů snažících se připojit ve stejný okamžik a obvykle vyústí v zablokování centrálního uzlu a služby, kterou poskytuje [45].

Druhou možností je distribuovaná síť. Tato síť nespoléhá pouze na jeden centrální uzel, ale využívá více uzlů. V distribuovaných sítích, jak již název napovídá, jsou data a výpočetní úkoly distribuovány mezi jednotlivé uzly. Tento systém má značné výhody, ale i jisté nevýhody. Díky rozdělení práce mezi jednotlivé uzly jsou uzly mnohem méně zatěžované, než je tomu u sítě centralizované. Je možné mnohem lépe síť optimalizovat a lépe rozložit zátěž. Tak je docíleno rychlejšího vyřizování požadavků. Tuto síť je také možné velmi dobře škálovat, protože je rozprostřena mezi větší množství uzlů. V případě nízké zátěže lze uzly odpojit a šetřit energii. V případě nárůstu zátěže je uzel opět zapnut a sníží tak zatížení ostatních uzlů. Další nespornou výhodou je, že u distribuovaných systémů nestačí pro výpadek služby přetížit pouze jeden uzel. V případě výpadku uzlu jeho práci převezmou ostatní uzly, které navýší svůj výkon, aby vykompenzovaly vypnutý uzel. Bohužel z toho také vyplývá, že tuto síť je možné zablokovat, pokud dojde k výpadku u více uzlů, než je síť schopná kompenzovat. Síť pak začne kolabovat jako domino. Nevýhodou takovéto sítě je nutnost synchronizace, protože data jsou rozprostřena na více uzlech. Každý uzel vykonává určitou část práce. Proto je důležité, aby bylo jasné, co každý uzel vykonává a kam má dokončená data předat dál. Pokud se provede špatná synchronizace nebo uzel nedokončí a neodešle svá unikátní zpracovávaná data dalšímu uzlu, který na ně čeká, může to vyústit v opakování požadavku nebo v nejhorším případě v nedostupnost služby. [46]

Třetí možností jsou decentralizované sítě. Tato forma sítě je přesným opakem centralizovaného řešení. Síť neobsahuje žádný centrální prvek, který by řídil komunikaci a ke kterému by se všichni uživatelé připojovali. Data jsou v tomto případě rozprostřena přes celou síť a uživatelé si je předávají mezi sebou obvykle v zašifrované formě. Šifrování v tomto scénáři zajišťuje důvěru v síti. Na rozdíl od centralizovaného řešení, uživatel přesně neví, kudy jeho data jdou. Tato skutečnost by bez šifrování byla velmi problematická, protože každý uzel by si mohl přečíst zasílaná data. Samozřejmě ve světě internetu není ani u centralizované sítě navazováno spojení point to point, ale obvykle data procházejí přes několik poskytovatelů (poskytovatel internetu a jeho servery) a proto se používá i u centralizovaného přístupu šifrování. Nespornou výhodou decentralizovaných sítí je narůstající propustnost sítě s každým dalším připojeným uživatelem, na rozdíl od centralizované sítě, kde každý připojený uživatel znamená snížení výkonu. Pokud v síti vypadne jeden nebo více uzlů, obvykle to nemá žádný dopad na výkon dané sítě, zasílaná

data se pošlou pouze jinou cestou. U decentralizovaných sítí je tedy velmi obtížné vysledovat původce dat, protože data prochází přes velké množství uzlů a jsou v zašifrované podobě. Tato skutečnost vedla také k myšlence decentralizovaného internetu, který by odboural sledování provozu za účelem shromažďování dat, poplatky za poskytování obsahu a další. Nicméně jako každé řešení i toto má jisté nevýhody. Hlavní nevýhodou je ochota jednotlivých uživatelů poskytovat svoje zařízení jako průchozí bod, to může vyústit ve velmi proměnnou kvalitu připojení a dostupnost služeb. Dalším problémem je, že vzhledem k absenci centrální kontrolní autority se musíme spoléhat na dodržování pravidel ostatními uživateli. Poslední nevýhodou je náročnost na implementaci a řízení sítě. S narůstajícím počtem uzlů je stále náročnější zajišťovat komunikaci mezi uzly a je potřeba vytvářet řídící uzly, které lépe rozprostřou komunikaci [47].

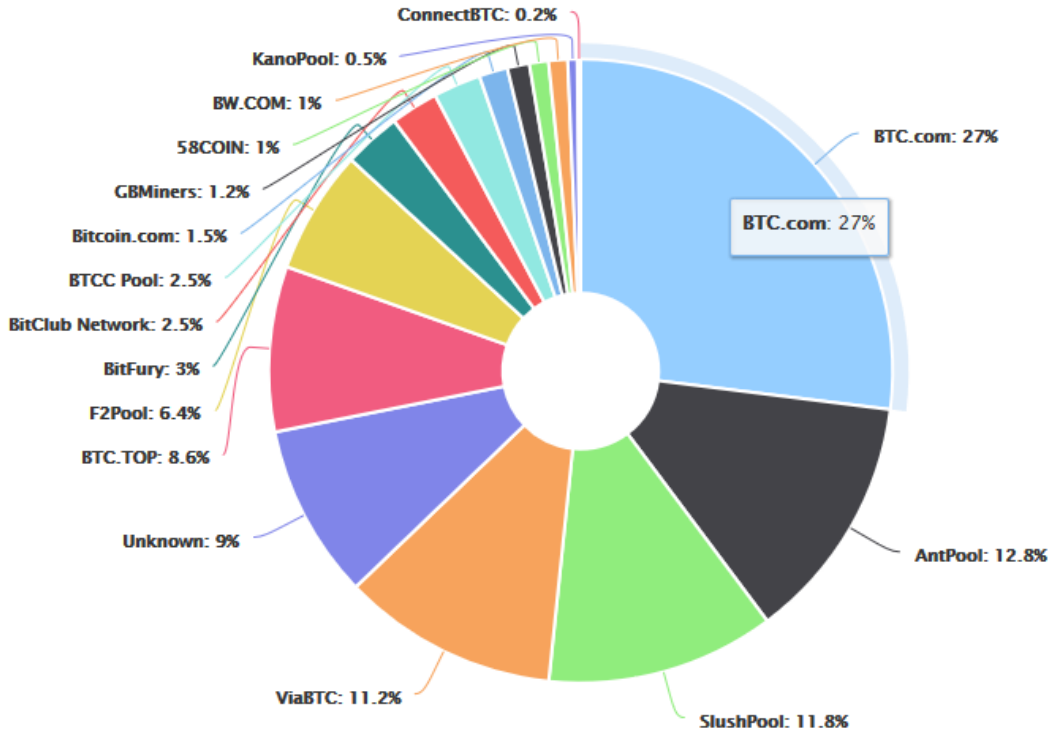
Bitcoin byl založen na stejném principu a jedná se o jednu z mála plně funkčních decentralizovaných sítí. Základní kamenem pro fungování je právě veřejná kniha transakcí, tedy Blockchain, kde každá transakce je ověřována těžaři a je tak velmi obtížné s transakcemi manipulovat. Nicméně s vzrůstající oblibou této kryptoměny jak ze strany uživatelů, tak ze strany těžařů, se začala situace měnit. S narůstající hodnotou bitcoinu se stalo těžení lukrativnější a začalo těžit více lidí, což by bylo v zásadě přínosné.



Obrázek 8: Graf obtížnosti v síti Bitcoin leden 2016 - leden 2018 [48]

Se vzrůstajícím výpočetním výkonem ovšem začala narůstat obtížnost a standardní počítače nebo serverové jednotky přestávaly mít dostatečný výkon. To mělo za následek nástup specializovaných zařízení tzv. ASIC minerů. Zařízení jsou speciálně konstruovaná pouze k jednomu účelu, a to v tomto případě, k počítání SHA-256 hashí. Zavedení těchto zařízení mělo za následek velký nárůst obtížnosti, viz obrázek 8. S takovou úrovní náročností již není těžení pro jednotlivce lukrativní. Těžení se začalo tedy soustřeďovat do

tzv. mining pools.Situace začala být velmi nepřehledná. Pokud si vezmeme graf rozdělení současných mining pools (výpočetní výkon se stále mění a graf je tak pouze orientační), zjistíme, že na první pohled je vše v pořádku, jelikož žádné z těžebních uskupení nemá více než 51% výkonu a pro ovládnutí sítě bychom potřebovali ovládnout alespoň tři největší těžební uskupení. Sice to není pouze jedno uskupení, ale již se velmi blížíme centralizaci. V případě férové decentralizace by mělo 100 % výkonu být produkováno alespoň stovkou těžařů.



Obrázek 9: Graf rozdělení těžebních poolů [49]

Hlavní problém ovšem nastává, pokud se zaměříme na geografické umístění těchto těžebních uskupení. Na první pohled se může zdát, že to není relevantní, pokud se jedná o nezávislé subjekty. Ovšem to by platilo, pokud bychom žili v zemích, kde nejsou žádné orgány, které mohou ovlivňovat provoz těchto uskupení. V současné době je dominantní zemí v těžbě Čína, která generuje více než 71% současného hashratu. Z toho plyne, že v Číně se reálně nachází 71% výpočetního výkonu a to může ohrozit princip, na kterém je Bitcoin založen a to sice Proof-of-Work. Z této situace se pokouší dostat Bitcoin Gold

změnou algoritmu, ale pravděpodobně to nebude dostatečné a bude potřebná změna principu z Proof-of-Work na Proof-of-Stake, který se nyní snaží prosadit například kryptoměna Etherum. [50]

3.5 Problémy a možné útoky

V této kapitole se zaměříme na možnosti ovlivnění Bitcoinu a to především transakcí uložených v Blockchainu. Seznámíme se zde se základními zdokumentovanými útoky na síť Bitcoin.

3.5.1 Útok 51%

Jedním z nejznámějších útoků na Bitcoin je tak zvaný útok 51% (51% attack). Pro úspěšné provedení tohoto útoku je potřeba ovládnout, jak název napovídá, více než 50% výpočetního výkonu sítě neboli hashratu (počet vypočtených hashů za vteřinu). Myšlenkou stojící za tímto útokem je, že uskupení této výpočetní síly může blokovat potvrzení nových transakcí a také může ovlivňovat i transakce již uskutečněné. Tak by útočníci mohli svoje bitcoiny utratit vícekrát. Tato situace se nazývá dvojí utrácení (double-spending). S největší pravděpodobností by nebylo v moci útočníků vytvářet nové mince nebo upravovat transakce většího stáří.

Pokud ovládneme více jak 50% výpočetního výkonu, neznamená to automaticky úspěch a možnost libovolně ovlivňovat Bitcoin. Nicméně s takovým výpočetním výkonem se šance na úspěch velmi zvyšuje. Pokud nedosáhneme přes 50% výpočetního výkonu, neznamená to, že tento typ útoku není možné vykonat, pouze to znamená velmi malou šanci na úspěch. Další faktorem, který je nutné si uvědomit, je fakt, že s ovládnutím nadpolovičního výkonu nijak nezvýšíme fyzické množství vlastněných mincí. Dojde pouze navýšení o odměny za těžbu bloků. Transakce je možné upravovat i ty uskutečněné, ale v rámci jednotek bloků do minulosti. Není možné manipulovat libovolně staré bloky, na to není tento výkon dostatečný. Vzhledem ke složení bloků by bylo nutné znovu vytěžit všechny následující bloky (viz předchozí kapitoly) [51].

Čeho tedy můžeme tímto útokem reálně docílit a jaké potenciální škody lze napáchat? Útokem lze ovlivňovat nové transakce dvojím způsobem. Prvním je zamezení ostatním těžařům v těžení. Je zde vyšší pravděpodobnost, že útočník bude úspěšný právě z důvodu ovládnutí nadpolovičního výpočetního výkonu a vytvořením monopolu pro sebe. Tak je možné zvyšovat množství svých bitcoinů za odměny z těžení (aktuálně 12,5 BTC za

blok). Tato možnost nepřináší teoreticky riziko pro síť. Riziko by však vzniklo, kdyby ostatní těžaři s těžením skončili a uskupení s 51 % výkonu by se stalo uskupením se 100% výkonu. Tímto způsobem by byla zrušena jakákoliv decentralizace. Nicméně na sbírání odměn za bloky ostatním není potřeba 51% výkonu, to lze uskutečnit i s menším výpočetním výkonem a nazýváme to selfish mining (více v další kapitole).

Druhou možností je ovlivňování transakcí formou jejich „zrušení“ a vytvořením dvojího utrácení. Uveďme si příklad: zaplatím za službu například v restauraci (transakce v bloku 2), restaurace si počká na ověření jedním blokem (blok 3). Protože se jedná o malou částku, službu považuje za zaplacenou. Útočník danou transakci vymaže z bloku 2 a znovu blok 2 a 3 vytěží. V případě, že ovládá nadpoloviční výkon a obtížnost se neupravuje po každém bloku, tak se mu to s velkou pravděpodobností povede úspěšně, obdržel službu za 0 BTC a svoje „utracené“ bitcoiny může utratit znovu. Bezpečnost z kryptografické strany není porušena, ale porušila by se důvěra ostatních uživatelů. A je to právě důvěra uživatelů, která je jedním z faktorů určujícím cenu bitcoinu. Takový útok by byl velkým problémem pro celou síť. Došlo by pravděpodobně k obrovskému pádu ceny a odlivu těžařů. Tomuto útoku nelze zabránit, protože neexistuje žádná kontrolní autorita. [52]

V současné době taková situace může nastat právě sdružováním těžařů do poolů a také porušením geografické decentralizace. Pokud uvažujeme, že 71 % všech těžařů se nachází na území Číny a Čína není plně demokratickou zemí, může být potencionálně budoucnost Bitcoinu v rukách čínské vlády [53].

3.5.2 Selfish mining

Selfish mining nemá takový dopad jako útok 51 %, protože primárně neslouží k upravování transakcí a dvojímu utrácení. Jedná se spíše o okrajovou možnost, než reálně proveditelný útok, je totiž relativně snadno detekovatelný. Tento útok se zaměřuje na poctivé těžaře a „krade“ jim odměny za vytěžené bloky. Je k němu zapotřebí minimálně 25% výpočetního výkonu. Pracuje na principu zatajování bloků.

Bitcoin protokol předpokládá čestnost těžařů a věří, že těžař zveřejní blok hned, jakmile ho nalezne. Útočník si ale objevené bloky nechává pro sebe. Pro názornost předpokládejme že Blockchain končí blokem 3 a hledá se navazující blok 4. Čestný těžař hned po nalezení bloku 4 blok připojí na konec Blockchainu a své úsilí přesune na hledání bloku 5 a takto to pokračuje dál, pokud se do hry nevloží náš útočník. Ten, pokud vytěží

blok 4, uchová si ho ve svém privátním Blockchainu a nezveřejní ho. Jeho prostředky se přesunou na hledání bloku 5, ale prostředky ostatních jsou stále zaměřeny na blok 4. Protože nový blok nemá jen jedno řešení, mohou čestní těžaři nalézt také blok 4, ale v tuto chvíli už může mít útočník i blok 5. Jakmile tyto dva bloky uveřejní, je blok čestných těžařů přesunut na vedlejší kolej a Blockchain navazuje na blok útočníka, který dostane odměnu za dva bloky.

Jaké jsou důsledky pro síť? Útočníci budou mít víc zisků než čestní těžaři a to povede k růstu tohoto uskupení. Většina těžařů samozřejmě potřebuje, aby se jim jejich investice vrátily. Růst může způsobit dominanci uskupení a překonání 51 % výpočetního výkonu. Takové uskupení pak může manipulovat s bloky [54].

3.5.3 Time Jacking

Time jacking je dalším z možných útoků na síť Bitcoin. Teoreticky se jedná o vylepšení útoku 51%. Lze ho použít pro dvojí utrácení. Tento typ útoku se zaměřuje na manipulaci s časovým razítkem. Celá síť má síťový čas, který jednotliví členové udržují. Každý nový uživatel sítě dostává při připojení časové razítko od svých sousedů, průměrem těchto časových razítek dostaneme síťový čas. Pokud se některý uzel liší o více než 70 minut, je z tohoto výpočtu vynechán. Z toho tedy plyne, že pokud útočník připojí kolem nového uživatele dostatek jiných uživatelů s nepřesným časem, může tomuto uživateli zrychlovat nebo zpomalovat čas. Pokud by měl útočník dostatek síly, může zpomalovat čas v jedné části sítě a ve zbytku čas může naopak zrychlit. Jelikož jsou uzly s rozdílem času více než 70 minut z výpočtu vynechány, může útočník vytvořit rozdíl až 140 minut.

Síťový čas je také důležitý při ověřování nových bloků. Časový rozdíl nového bloku proti síťovému času může být pouze 120 minut. Pokud je tento rozdíl větší, je daný blok uzlem odmítnut jako neplatný. To také platí, pokud je časové razítko starší než posledních 11 bloků. Toto pravidlo je zavedeno z důvodu tolerance časové nepřesnosti.

Útok se dá použít pro odtržení uzlu ze sítě nebo také pro dvojí utrácení, oboje spolu úzce souvisí. Útočník může odříznout uzel se sítě tak, že mu podstrčí „otrávený“ blok, který může mít časové razítko posunuté až o 190 minut dopředu. Jelikož se na daném uzlu zpomalil čas, tak tento uzel vyhodnotí blok jako neplatný, protože jeho časové razítko se liší z pohledu uzlu o 260 minut. Zbytek sítě ho však přijme, protože pro něj je ještě v toleranci do 120 minut v jejich zrychleném síťovém čase. Takto útočník může

daný uzel zablokovat na velmi dlouhou dobu, protože každý další blok bude tímto uzlem zahozen – vzhledem k tomu, že obsahuje hash předešlého neplatného bloku. Daný uzel by musel manuálně kompletně resetovat svůj čas, aby se vymanil. Tento typ útoku tedy vytváří forky od hlavního Blockchainu, které jsou později odříznuté.

V souvislosti s izolací uzlu od současného Blockchainu lze útok využít také k dvojímu utrácení. Na rozdíl od útoku 51% lze dvojí utrácení aplikovat pouze na uzel, který útočník dal do izolace. Výrazně klesá požadavek na výkon útočníkova uskupení, stačí mu pouze 10% výkonu sítě, aby mohl útok provést. Útočník pro daný uzel v izolaci generuje falešné bloky a je schopen vytvořit potvrzení o šesti blocích za několik dní. Je 10% pravděpodobnost, že se mu to podaří již za šest hodin. Útočník tedy nakoupil od uživatele spoléhajícího se na uzel v izolaci a dostal svých šest potvrzení. Zaslal objednané zboží útočníkovi, který izolovaný uzel vrátí do sítě. Hlavní Blockchain převezme kontrolu a takto vytvořené bloky budou zrušeny. Útok je možné aplikovat také na těžaře, kteří budou vlastně těžit neplatné bloky nebo mohou být použiti na pomoc k vytvoření potvrzovacích bloků pro útočníka a urychlení útoku.

Z výše uvedených informací vyplývá, že pokud by byli útočníci dostatečně sofistikovaní, stačilo by jim pouze kontrolovat čas v síti a síť rozdělovat dle svých potřeb na dvojí utrácení. K uzlu v izolaci by se přidal dostatek těžařů, kteří by těžili a potvrzovali jeho falešné bloky. Tato těžba by pro těžaře probíhala zadarmo, ale tuto skutečnost by odhalili až ve chvíli, kdy by kontrolu převzal hlavní Blockchain a zrušil takto vytvořený fork. [55]

Útoky uvedené v této kapitole jsou vedené pouze proti síti Bitcoin, nejedná se o útoky na koncové uživatele. Nejedná se primárně o porušení kryptografie nebo bezpečnosti sítě Bitcoin jako takové. Medializované útoky na uživatele využívající některý druh podvodu (phishing, zpronevěra burzou a další) nejsou pro tuto práci relevantní a nejsou zde proto uvedeny.

3.6 Další populární kryptoměny

Bitcoin byl první funkční kryptoměnou. V posledních letech jsou však populární i jiné kryptoměny. V této kapitole se zaměříme na přímé konkurenty Bitcoinu a rozdíly v jejich fungování. Bylo vybráno pět kryptoměn, které mají aktuálně (únor 2018) nejvyšší tržní hodnotu. Tržní hodnota Bitcoinu nyní přesahuje 180 miliard dolarů. Před prosincovým pádem v roce 2017 dosahovala dokonce přes 250 miliard dolarů [56].

3.6.1 Ethereum

Ethereum, stejně jako Bitcoin, využívá decentralizovanou síť a blockchain, ale na rozdíl od Bitcoinu se nejedná pouze o systém k přístupu a převodům kryptoměny. Další podobností s Bitcoinem je systém ověřování pomocí těžení bloků a tedy i použití algoritmu PoW (proof-of-work). V současné době síť Ethereum zkoumá možnost přejít z PoW na PoS (proof-of-stake). Prvním výrazným rozdílem oproti Bitcoinu je rychlost těžení bloků, která je u této sítě snížena z 10 minut na 12 vteřin. Toto zrychlení velmi zvyšuje celkovou propustnost sítě a tím i počet transakcí za vteřinu. Kryptoměnou je v tomto případě ether, který slouží jako „palivo“ sítě. Stejně jako u bitcoinu se ether používá k zaplacení těžebního výkonu těžařům. U této sítě však nebyla velká část vytěžena prvotními těžaři, ale nabídnuta v předprodeji, což vlastně zaplatilo vývoj celé sítě. V současné době se odhaduje, že polovina etheru bude vytěžena nejdříve v průběhu roku 2020.

Na rozdíl od Bitcoinu tato síť není pouze platebním systémem, ale je vytvořena tak, aby podporovala i jiné služby, které potřebují ověřování – tzv. chytré kontrakty. Ethereum je tady v podstatě platforma pro virtualizaci decentralizovaných aplikací. Do sítě Etherea lze vytvářet a přidávat vlastní aplikace za použití poskytnutých softwarových nástrojů, například rozšíření pro prohlížeč Google Chrome. Tyto softwarové nástroje dělají blockchainové aplikace více dostupnými. Tato dostupnost může znamenat ale i problémy, protože chytré kontrakty jsou pouze tak dobré, jako osoba, která je vytvořila. Síť Ethereum pouze poskytuje výpočetní výkon a chyby v kódu nekontroluje – jsou za ně zodpovědní vývojáře aplikace. Kryptoměna ether se používá na placení výpočetního výkonu těžařů a je tedy důležité poskytnout dostatek „paliva“ pro vykonání výpočtu. Pokud nastavíme příliš nízkou hladinu, „palivo“ v průběhu úkolu dojde – těžaři už ho spotřebovali za poskytnutý výkon. Ether se tedy stejně jako u bitcoinu vytváří těžením a je odměnou za vytěžené bloky. Ether je obchodovatelný a je používán i na placení poplatků v síti za zpracování chytrých kontaktů. Současná tržní hodnota dle Coin market cap je 94 miliard dolarů [57].

3.6.2 Ripple

Ripple je název pro kryptoměnu, ale zároveň také pro platební síť provádějící finanční transakce. Současná tržní hodnota je 22,99 miliardy dolarů. Ripple je známější

spíše jako platební síť, než jako kryptoměna. Jedná se také o open source řešení využívající peer to peer decentralizovanou síť. Přes tuto platformu je možný bezproblémový převod peněz v jakékoliv podobě, ať už jsou to standardní měny nebo konkurenční kryptoměny. Kryptoměna ripple je velmi odlišná od bitcoinu. V rámci rozlišení měna používá zkratku XRP, síť je Ripple. Nevyužívá se zde těžení, ale měna byla vydána v objemu sto milionů XRP. Toto číslo je konečné a nebude se měnit. Dalším rozdílem je, že přes 61% všech XRP vlastní jejich vydavatel firma Ripple Labs Inc. Firma kryptoměnu postupně uvolňuje mezi uživatele, obchodníky a další, aby zvýšila zájem a rozšířila kryptoměnu a platební systém. Toto řešení je mnohem méně energeticky náročné, než v případě kryptoměn používajících proof-of-work, ale i tak se jedná o plně decentralizovanou měnu bez nutnosti důvěřovat třetím stranám.

Hlavní myšlenkou této kryptoměny a její platební sítě je zrychlit a výrazně zlevnit všechny platby. Současné standardní bankovní převody trvají řádově desítky hodin při vysokých transakčních poplatcích. V případě sítě Ripple je možné uskutečnit i zahraniční platby v řádu vteřin s velmi nízkými poplatky. Poplatky jsou počítány z objemu transakce. Ripple pracuje na principu IOU (I owe you). Do blockchainu se nezapisují pouze transakce, ale účty uživatelů, zůstatky a kdo, komu dluží. Aby se snížilo riziko, jsou v síti tzv. brány (gateway), které přebírají požadavky na platby. Řekněme, že pan František chce zaslat peníze panu Josefovi. Pan František předá zasílaný obnos a heslo svému agentovi A, ten zavolá agentovi B na druhé straně a řekne mu, aby uvolnil požadovaný obnos tomu, kdo bude znát správné heslo. Pan Josef přijde ke svému agentovi, řekne mu heslo a obdrží částku od pana Františka. V tuto chvíli agent A dluží agentovi B zasílaný obnos. Tento obnos si mezi sebou buď vyrovnají, nebo se dohodnou, že ho srovnají, až půjde obrácená transakce. Základní podmínkou fungování je důvěra. Zákazníci musí důvěřovat agentům a ti musí věřit sobě navzájem. Může nastat i situace, že agent A nedůvěřuje agentovi B, ale oba mohou důvěřovat agentovi C, platba se tedy uskuteční přes agenta C. V síti se hledá vždy nejkratší možný řetězec agentů, kteří si důvěřují. Agenti jsou v tomto příkladu právě výše zmíněné gateway. Poslední možností je, že se nenajde řetězec mezi agenty A a B, kterým zároveň důvěřují oba, pak nastupuje právě XRP, která slouží jako poslední možnost a použije se v případě, že pan František chce zaslat například zlato, ale agent protistrany nevěří agentovi pana Františka, že mu zlato dodá. Objem zlata se tedy přepočte na hodnotu v XRP a ty se zašlou agentovi pana Josefa. Kryptoměna XRP slouží

také jako bezpečnostní prvek v platebním systému Ripple a díky ní bude v budoucnu možné přes tuto síť poslat cokoliv, co má vyčíslitelnou hodnotu. XRP je samozřejmě také samostatně obchodovatelná a je možné ji nakupovat a prodávat za aktuální tržní hodnotu pomocí burz jako je například BitStamp [58].

3.6.3 Bitcoin Cash

Jak již bylo uvedeno v kapitole Fork v Blockchainu, Bitcoin cash je pouze hardforkem Bitcoinu. Současná tržní hodnota je 16,2 miliardy dolarů. Jedinou změnou oproti Bitcoinu je zavedení větší velikosti bloků pro zvýšení počtu transakcí za vteřinu.

3.6.4 Litecoin

Litecoin byl uveden do provozu v říjnu 2011 a jedná se z velké části o kopii Bitcoinu, která má aktuální tržní hodnotu 12,6 miliardy dolarů. Stejně jako Bitcoin využívá těžení k ověřování transakcí a pracuje tedy na principu Proof-of-Work. Hlavní rozdíly jsou v použitém algoritmu a rychlosti těžení. Litecion nepoužívá SHA256, ale tzv. scrypt. Scrypt algoritmus přetváří SHA256 do více sériové podoby. Na rozdíl od Bitcoinu není možné těžit paralelně, protože potřebujeme část A, abychom mohli spočítat část B. U tohoto algoritmu není limitujícím faktorem výpočetní výkon, ale operační paměť, proto se tento algoritmus také nazývá problém náročný na paměť. Myšlenka byla taková, že obyčejní lidé budou moci problém vyřešit pomocí běžné paměti a nemusí si kupovat specializované ASICs. Použití tohoto algoritmu mělo umožňovat dostupné a demokratické těžení, jak jen to je možné. Společnosti Zeus a Flower Technology však vytvořily specializované ASIC pole i pro algoritmus scrypt, což bohužel původní myšlenku značně narušilo.

Dalším rozdílem oproti Bitcoinu je nastavený čas potřebný na vytěžení jednoho bloku, který je zde snížen z 10 minut na 2,5 minuty. Výrazně se tak zkrátí čas potvrzení transakce, kdy za stejnou dobu jednoho potvrzení u Bitcoinu (10 minut), máme čtyři potvrzení v případě Litecoinu. Další výhodou je rychlejší odměňování těžařů a lepší rozložení odměn. Zrychlení má i nevýhody. Protože je mezi bloky tak málo času, je velmi pravděpodobné, že bude docházet k vytváření tzv. osiřelých bloků, které jsou velkou zátěží pro blockchain. Každý vytěžený blok, který není přidán do blockchainu, je také velkou ztrátou energie [59].

3.7 Vlastnictví bitcoinu

V této kapitole se zaměřím na metody, kterými lze kryptoměnu bitcoin získat, jakým způsobem je možné ji mít uloženou a zda ji lze získat a používat anonymně.

3.7.1 Bitcoinová peněženka

Před samotným získáním bitcoinu je nutný první krok – založení tzv. bitcoinové peněženky, abychom měli mince kam zaslat a uložit. Zaměříme se pouze na obecné principy, na jejichž základě peněženky fungují. V dalších kapitolách bude vybráno několik peněženek a popsány jejich výhody a nevýhody. Také popíši možnosti forenzního zkoumání.

Co je tedy bitcoinová peněženka? Jedná se o program k práci s bitcoiny. Často je peněženka označována jako místo, kde máme uložené bitcoiny, ale to není technicky správně. Bitcoiny nejsou nikde fyzicky skladovány, protože se nejedná o fyzickou měnu. V peněžence se tedy nenacházejí samotné bitcoiny, ale pouze adresy, na kterých jsou uloženy. Další položkou, kterou peněženka musí obsahovat, je privátní klíč pro přístup k těmto adresám.

V současné době jsou používány čtyři druhy peněženek v závislosti na platformě: pro osobní počítače, pro mobilní zařízení, webové a hardwarové.

1. Peněženky pro osobní počítače jsou určeny pro systémy Windows, Mac i Linux, jedná se o programy instalované na desktopovém prostředí. Tento druh peněženky je vhodný pro placení online, případně ke kontrole historie transakcí. Většinou jsou nevhodné pro použití v kamenných podnicích, kde jsou přijímány bitcoiny.
2. Mobilní peněženky mají obvykle stejné funkce jako peněženky pro osobní počítače, ale navíc nabízí lepší mobilitu. Platit je možné odkudkoliv. Mobilní peněženky také nabízejí platbu za pomoci technologie QR kodů nebo NFC. Tento typ peněženky je tedy velmi vhodný pro placení v kamenných podnicích.
3. Webové peněženky mají obvykle omezenější funkce než mobilní peněženky (nepodporují NFC), ale na rozdíl od obou výše jmenovaných nejsou vázané na žádnou platformu a jsou použitelné na skoro každém operačním systému nebo webovém prohlížeči. Největší nevýhodou je, že privátní klíč je skladován online a tudíž je nutné velmi dobře si rozmyslet, jakou peněženku, od kterého poskytovatele použijeme.

4. Hardwarové peněženky jsou obdobou čipové karty v internetovém bankovnictví. Soukromý klíč, pokud není používán, je uchováván mimo počítač, a tak je zvýšeno zabezpečení. Tyto peněženky zatím nemají velké zastoupení, protože uživatel potřebuje software a hardware, aby mohl uskutečňovat transakce. Hardwarové peněženky dosahují obvykle nejvyššího stupně zabezpečení. Je velmi obtížné odchytnout soukromý klíč. Mezistupněm hardwarové peněženky může být tzv. papírová peněženka. I když se to na první pohled může zdát zvláštní, je možné obsah peněženky převést i do papírové formy, některá softwarová řešení toto umožňují. Protože peněženky neobsahují bitcoiny jako takové, ale pouze jejich adresy, je možné použití papírové formy, kdy si jednoduše dané adresy vytiskneme na papír. Vytisknout je možné také soukromý klíč. Tato metoda je v elektronickém světě nejbezpečnější, ale je nejméně uživatelsky přívětivá. Pokud papíry ztratíme nebo je někdo odcizí, neexistuje žádná možnost obnovy bitcoinů. Vlastnictví určuje pouze znalost adres a soukromého klíče.

Z výše uvedených informací jasně plyne, že je vždy velmi důležité vybrat vhodný typ peněženky a důvěryhodného tvůrce. Dále je nutné zvolit si dostatečně bezpečné heslo, abychom bitcoiny zabezpečili [60].

3.7.2 Získání bitcoinu

Vzhledem ke značnému rozšíření bitcoinů je i mnoho možností, jak bitcoiny získat. Popíšeme si zde metody jejich získání, jeho obtížnost a přístupnost běžným uživatelům. Budeme se zabývat i potřebným vybavením. Zaměříme se na to, jestli lze bitcoin získat anonymně a pokud ano, jaký postup je nutné dodržet.

V současné době je možné bitcoiny získat nákupem nebo těžením. Nejprve popíšu současné možnosti těžení a zamyslím se nad tím, jestli je těžba vzhledem k nárůstu obtížnosti ještě vůbec možná. Pak prostuduji a popíši možnosti nákupu.

3.7.2.1 Těžení

Jak bylo uvedeno v přechozích kapitolách, těžení se používá k ověření bloků v Blockchainu a tedy i ověření transakcí obsažených v bloku. Těžení je nastaveno tak, aby se blok vytvořil cca každých 10 minut. Toho je dosaženo úpravami obtížnosti. Za vytěžení každého bloku náleží odměna tomu, kdo jako první vypočítal hash pod targetem.

Výše této odměny se postupem času mění, protože bitcoinů bude pouze omezené množství. Výše odměny klesá každých 210 000 bloků na polovinu. Odměna v roce 2009 byla za jeden blok 50 BTC. V letošním roce je odměna již pouze 12,5 BTC za jeden vytěžený blok. Tato částka jsou pouze nově vytěžené mince, těžaři ještě mohou dostávat poplatky z transakcí.

Nyní se zaměřím na to, jestli je ještě touto cestou možné získat bitcoiny i pokud jsme běžným uživatelem, který má prostory a chtěl by zkusit těžbu. Je nutné si uvědomit, že díky nárůstu obtížnosti již není možné těžit na klasickém domácím počítači. Ani high endové počítače nedosahují potřebného výkonu na samostatnou těžbu. Pokud nechceme investovat do pořízení nového hardwaru, je možné se připojit do těžebních uskupení nazývaných pooly. Po připojení do těchto poolů je možné poskytnout výkon svého pc k těžení. Pokud se poolu, ve kterém je těžař připojen, podaří vytěžit blok, dostane část odměny podle procenta výkonu, kterým do poolu přispěl. Budeme-li využívat výkonnější multimediální stroj, který je složený z procesoru Ryzen 7 1700 a má i grafickou kartu AMD RX 580, je možné dosáhnout až 270H/s pro procesor. Grafická karta s úpravou biosu dává podstatně lepších 27 MH/s. Z toho plyne, že těžení na procesorech již dávno nedává smysl (alespoň v případě Bitcoinu). Ještě v roce 2010 by tento hardware stačil na 10 % výkonu celé sítě. V roce 2018 je to pouhých 1,2 x 10^{-9} výkonu sítě [61]. Touto cestou tedy již není reálné bitcoiny získat. Situaci způsobil vznik specializovaného hardwaru, který byl vyvinut pouze na výpočet SHA256 hashe. Tato zařízení se jmenují ASIC miners – to je zkratka pro jednoúčelový integrovaný obvod. Nástup těchto zařízení zapříčinil enormní navýšení obtížnosti a snížení dostupnosti těžení pro běžné uživatele. Přes vysoký výpočetní výkon těchto zařízení (až 13,5 TH/s) je odhadovaný výnos pouze 0,36 BTC za měsíc [62]. Těžením je i dnes možné bitcoiny získat, ale je k tomu potřebná značná investice. Těžení je anonymní a je tedy možné touto cestou získat bitcoiny anonymně.

3.7.2.2 Nákup

V této části práce se zaměřím na možnosti nákupu bitcoinu a v jakých měnách jsou bitcoiny dostupné. Možnost anonymního získání mincí popíšu pouze v teoretické rovině.

Aktuálně největším inzertním serverem, přes který je možné bitcoiny zakoupit, je LocalBitcoins.com. Na serveru je možné nakupovat převodem, kartou i hotově od lidí, kteří vlastní bitcoiny. U některých prodejců je nutný ke koupi doklad totožnosti, jiní

prodejci nic nepožadují. Je tedy teoreticky možné anonymně nakoupit bitcoin. Nejprve je třeba zabezpečit naše připojení například pomocí sítě TOR, aby byla skryta naše ip adresa. Poté si vytvoříme účet na LocalBitcoin, abychom mohli kontaktovat vybraného prodejce. Zde se samozřejmě zaregistrujeme pomocí falešných osobních údajů, falešného emailu a telefonního čísla na přeplacené kartě. Na internetu jsou dokonce generátory falešných jmen (fakenamegenerator.com) spolu s poštovními adresami, tyto stránky podporují i Českou Republiku. Po zaregistrování si můžeme vybrat prodejce. Vybereme si takového, který dovoluje platbu v hotovosti, nevyžaduje doklad totožnosti a je možné se sejít na veřejném místě. Pak již zbývá poslední krok – přijít na dohodnutou schůzku a zaplatit za bitcoiny. V tomto kroku je možné samozřejmě někoho pověřit předáním peněz pro zajištění větší anonymity. Touto formou je tedy možné zakoupit bitcoiny zcela anonymně [63].

Za bitcoiny můžeme zaplatit téměř jakoukoliv měnou včetně české koruny. Další možností pořízení bitcoinů je jejich zakoupení ve specializovaných bankomatech. Existují bankomaty, které nevyžadují ověření a dokonce u některých není nutné mít vlastní peněženku – bitcoiny jsou z bankomatu vytištěny v podobě papírové peněženky [64]. V České Republice jsou možnosti anonymního nákupu u bitcoinového bankomatu omezeny na 1000 € (cca 25 000,- Kč). Nad tento limit by měli požadovat ověření i prodejci například ze serveru LocalBitcoins.com, ale je na jejich uvážení, jestli podstoupí riziko plynoucí z porušení zákona. Toto omezení vešlo v platnost od 1. 1. 2017, kdy sumu upravuje zákon 368/2016 Sb. Tento zákon mění zákon č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu a další související zákony [65].

3.7.3 Anonymita transakcí v Bitcoin síti

Je bitcoin opravdu anonymní kryptoměnou a lze v době dnešního internetu provádět transakce anonymně? Anonymita byla jednou ze stavebních myšlenek celého systému i navzdory tomu, že všechny transakce jsou uloženy ve veřejné účetní knize (Blockchainu). V Blockchainu jsou ale uloženy pouze elektronické adresy, ze kterých jsou dané transakce uskutečněné. Adresy jsou v tomto případě tvořeny alfa numerickou sekvencí dlouhou 26 – 36 znaků. Adresa vypadá například takto:1BoatSLRHtKNngkdXEeobR76b53LETtpy [66]. V Blockchainu nejsou k adresám přiřazeny žádné personální informace. Je zde ale určité riziko, že adresa může být vysledována zpět k majiteli a tím

bude odhalena i celá jeho transakční historie. Z toho důvodu je bitcoin často označován jako pseudonymní. Nyní se tedy podíváme na to, jak jednoduché nebo obtížné je toto spojení vytvořit.

V současnosti je stále více dat zaznamenáváno zcela bez našeho vědomí nebo se dle nových směrnic na webových stránkách objevují upozornění na sledovaná data. Většina uživatelů bezmyšlenkovitě tato upozornění potvrdí, protože obvykle zakrývají část webu, který si prohlížejí. Jedná se převážně o webové trackery a cookies. To jsou kusy kódu účelně umístěné na webové stránce za účelem získávání a zasílání dat třetím stranám, kterými jsou Google, Facebook a další. Na základě těchto dat jsou poskytovány cílené reklamy podle námi navštívených webů. Některé weby dokonce mohou zasílat i data, která uživatele přímo identifikují - jméno, adresu, email. Běžný internet tedy opravdu není anonymní. Samozřejmě je možné používat anonymizační nástroje jako například síť ToR, ale ty nezabrání webovým stránkám ukládat informace, které jim zadáte například při nákupu v eshopu.

Existuje několik možností, jak spojit uživatele s adresou bitcoinu. První a zároveň nejjednodušší z nich je špatné zabezpečení elektronického obchodu, které vyústí v nevědomé zaslání, kdy mimo osobních údajů odešleme i bitcoinové adresy.

Dalším způsobem je dohledání transakce a spojení bitcoinové adresy zpět k uživateli. Pokud víme, kdy a za jakou částku se transakce uskutečnila, můžeme v Blockchainu dohledat tuto transakci a spojit bitcoinovou adresu zpět k uživateli. Tento způsob je obvykle více náročný, protože je zde celá řada proměnných. Většina obchodů obchoduje v národní měně a částky přepočítává svým kurzem na bitcoin. Další proměnnou je přesný čas uskutečnění. Pokud bereme v úvahu, že trakery většinou zasílají informace o košíku, může se čas uskutečnění objednávky lišit od času provedení transakce a nalezení transakce v Blockchainu se tak stává obtížnějším. Poslední proměnnou mohou být dodatečné poplatky, jako je například doprava. Všechny tyto faktory ztěžují propojení údajů, ale i tak je úspěšnost těchto propojení kolem 60% [67]. Jakmile dojde z výše uvedených důvodů k propojení bitcoinové adresy se jménem uživatele, ztrácí jakoukoliv anonymitu a všechny předchozí i budoucí transakce budou díky veřejné dostupnosti snadno dohledatelné.

Samozřejmě existují metody, jak více zabezpečit a skrýt své provedené transakce. Některé jsou placené a je potřeba důvěra ve třetí stranu, další mohou být součástí bitcoinové peněženky.

Jednou z nejpopulárnějších technik je slučování transakcí tzv. CoinJoin. Tato služba slučuje uživatele, kteří plánují podobnou platbu a sdružuje je. Namixuje jejich bitcoiny. Tuto službu nabízí například BITMIXER.IO. Jedná o placenou službu a anonymita je zachována pouze tak dlouho, dokud stránka informace o transakcích neposkytne. Transakce má tedy více vstupů a výstupů a identifikace se stává těžší. Ovšem ani tato metoda nezajistí bitcoinovým transakcím stoprocentní anonymitu. Stále je možné s větším úsilím platbu vysledovat.

Na podobném principu také pracuje JoinMarket. V tomto případě se nejedná o software ani službu, kde je potřeba důvěřovat třetí straně. Transakce jsou slučovány u tzv. tvůrců, kteří posbírají více transakcí a za poplatek je sloučí do jedné. Ze sloučené jedné adresy jsou finance zaslány na požadovaná místa. O tuto službu není v současnosti takový zájem, protože pro uživatele není úplně jednoduché ji zprovoznit.

Další možností je použití anonymizace na internetu pomocí sítě ToR nebo bez záznamové VPN služby. Tyto dvě metody skryjí identitu uživatele na internetu tím, že maskují skutečnou IP adresu. Pak je složitější uskutečnit propojení vytvořených transakcí. Tato metoda funguje pouze za předpokladu, že webová stránka nezasílá údaje z objednávky a bitcoinovou adresu. V takovém případě by bylo toto řešení neúčinné.

Pro zajištění anonymizace je možné také vytvářet nové adresy pro každou platbu spolu s novými adresami pro příchozí bitcoiny. Toto řešení bývá již implementováno v některých bitcoinových peněženkách. Používání stejné adresy může dát potencionálnímu útočníkovi přesný přehled, kolik financí v peněžence máte. Peněženky obvykle umožňují generovat libovolné množství adres. Je možné pro každou transakci vytvořit novou adresu a pro žádné dvě transakce nepoužít stejnou adresu. To zajistí, že sledování finančních prostředků se stane více obtížným.

Poslední možností je výměna bitcoinu za fyzické peníze například přes LocalBitcoins. Stačí se zaregistrovat pod falešným jménem i emailem a pro domluvu schůzky použít předplacený telefon. Této metodě jsem se podrobněji věnoval v předchozí kapitole: Získání bitcoinu – Nákup [68].

Situace s pseudonymitou není příznivá pro uživatele doufající v anonymní platby. Pokud se podíváme optikou bezpečnostních složek, při současných možnostech anonymizace plateb může být odhalení propojení transakcí s trestnou činností obtížné, při špatném zabezpečení ze strany uživatele však není nemožné.

3.8 Legislativa a Bitcoin

3.8.1 Česká Republika

V aktuální verzi legislativy není žádný zákon, který by jakkoliv definoval názvosloví virtuální měna a případně se zabýval konkrétními měnami. Dle vyjádření ČNB se u bitcoinů a obecně virtuálních měn nejedná o bezhotovostní peněžní prostředky ani elektronické peníze. Dle § 4 zákona 284/2009 sb. o platebním styku se nejedná ani o peněžní prostředky definované v § 2, odst. 1 písm. c. Nakládání s bitcoiny nepředstavuje žádnou platební službu dle § 3 ani bezhotovostní obchod s cizí měnou dle § 2, odst.1 písm. e). Bitcoin a všechny operace s ním tedy nepodléhají žádným nařízením zákona o platebním styku. Dalším zákonem, který by mohl měnu regulovat je zákon č. 277/2013 Sb., o směnárenské činnosti. Ten by se vztahoval na směnu bitcoinu za běžné měny, nejsou ale naplněny podmínky tohoto zákona. Bitcoin i přes svůj název virtuální měna, podle platných zákonů výše uvedených, měnou není – v zákoně je výslovně uvedena směna na určitou měnu. Bitcoin také nenaplňuje § 3 zákona č. 256/2004 Sb. o podnikání na kapitálovém trhu, ve znění pozdějších předpisů, protože bitcoin není komoditou ani cenným papírem. Z toho tedy jasně plyne, že obchodování, směna, prodej a nákup nejsou v případě virtuálních měn nijak regulované Českou národní bankou a k jejich obchodování není vyžadováno žádné povolení od ČNB [69].

Bitcoin je v současné podobě považován za nehmotnou věc dle § 496 odst. 2 zákona č. 89/2012 Sb. občanského zákoníku. Z toho plyne, že v případě krádeže je celá věc řešena podle § 205 zákona č. 40/2009 Sb. trestního zákoníku. Zákonem omezujícím nepřímo virtuální měny je zákon 368/2016 Sb., kterým se mění zákon č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Tento zákon upravuje omezení nákupu nebo prodeje virtuálních měn v hotovosti na výši 1000 € (cca 25 000,- Kč) bez nutnosti legitimace [70].

Na bitcoiny a ostatní virtuální měny se mohou vztahovat také daňové zákony a to jmenovitě zákon o dani z příjmů. Daň z příjmů se na virtuální měny vztahuje, ale pouze

v případě, že od zákazníků obdržím platbu za poskytnuté služby nebo zboží ve formě bitcoinu, místo tradiční měny. Na vlastnictví virtuálních měn ani na zisky z obchodování s nimi se daně nevztahují, jelikož se jedná pouze o nehmotnou věc a příjem z obchodování tak nelze zařadit do žádné kategorie příjmů dle zákona o daních z příjmů.

V tomto odstavci rozebereme potenciální protiprávní jednání v souvislosti s kryptoměnami. Trestnou činnost v rámci kryptoměn můžeme rozdělit na trestné činy proti majetku a hospodářskou kriminalitu. Jak bylo popsáno v předchozích kapitolách, například bitcoiny jako takové není možné odcizit, ale je možné odcizit adresy a potřebné klíče k nim. Ve světě již bylo zaznamenáno několik krádeží a ani Česká Republika není výjimkou. Jak jsme si již řekli, v případě krádeže se celá záležitost bude řešit jako krádež nehmotné věci. V dalších postupech se názory mohou lišit. První důležitou otázkou je, jestli odcizení hesla nebo soukromého klíče je možné brát jako přípravu trestného činu nebo nikoliv. Obvykle se rozlišují dva typy krádeže a to sice krádež zvenčí a krádež zevnitř.

U krádeže zvenku neboli zcizení potřebných údajů je problematické určit přípravu k trestnému činu, protože oběť má obvykle do poslední chvíle kontrolu nad svojí peněženkou a trestný čin je naplněn až ve chvíli, kdy jsou prostředky převedeny. Čin je tedy spáchán až ve chvíli, kdy poškozený o prostředky fyzicky přijde.

Krádeží zevnitř je situace, kdy máme soukromý klíč uložen například na flash disku nebo vytištěný na papíru. Zde je možné určit přípravu trestného činu již ve chvíli, kdy nám bude toto medium odcizeno. V případě, že nemáme záložní medium, ztrácíme jakýkoliv přístup ke své peněžence. V síti totiž neexistuje žádná centrální autorita, která by mohla změnit heslo nebo zablokovat certifikát. V tomto případě se obtížně určuje, kdy je trestný čin naplněn, protože bez přístupu k peněžence nemáme možnost kontrolovat zůstatek, to je možné je pouze v případě, že bychom měli záložní kopii uloženou na dalším mediu nebo druhou vytištěnou kopii.

Závažnou trestnou činností spojenou s bitcoiny je hospodářská kriminalita. Jak jsme si řekli v předchozí části na bitcoin se v České Republice vztahuje daň z příjmu a v případě nákupu bitcoinu za hotové tyto nákupy dokonce nepřímo podléhají EET. EET nepodléhá bitcoin jako takový, ale hotovost přijatá na jeho nákup. Problém nastává u plateb, kdy platíme přímo obchodníkovi v bitcoinu. Je velmi obtížné kontrolovat objem přijatých transakcí, protože obchodník může vlastnit neomezený počet adres a jednotlivé platby

párovat s náhodnými adresami, aby případná kontrola obtížně dokazovala eventuální daňové úniky. Je to podobné, jako by obchodník část příjmů ze své činnosti zasílal na zahraniční účet registrovaný na jiné jméno. U kryptoměn je tato skutečnost mnohem snáze proveditelná z počítače a takřka bez nákladů. Touto cestou mohou vznikat značné daňové úniky. [71]

Další trestnou činností spojenou s kryptoměnami může být legalizace výnosů z trestné činnosti a financování terorismu. Tuto skutečnost se snaží řešit zákon 368/2016 Sb., ale obdobně jako u daňových úniků se porušení zákona bude v praxi velmi těžko dokazovat. Pachateli také velmi pomáhá velká volatilita měny. Z těchto důvodů jsou již virtuální měny v některých zemích postaveny mimo zákon. Některé země dovolují kryptoměny těžit a vlastnit, ale nelegální je s nimi platit a také obchodovat.

3.8.2 Ostatní země

Jaké země tedy přímo regulují virtuální měny a jakým způsobem?

Austrálie začala požadovat registraci všech směnáren na virtuální měny u své finanční správy a v případě nákupu a prodeje jsou tyto směnárny povinné evidovat své zákazníky na základě průkazu totožnosti. Podobně se zachovala Kanada s Japonskem, kteří virtuální kryptoměny začlenili do své legislativy jako měnu. Vztahují se tedy na ně stejná pravidla jako na běžně používané měny, včetně všech daňových zátěží, zákona o praní peněz a legitimaci zákazníků. Evropská unie se k otázce virtuálních měn zatím staví velmi opatrně a žádné regulace v současnosti nechystá. To se ovšem nelíbí Evropské centrální bance, která by byla pro zavedení přísnější kontrol, hlavně v případě legalizace výnosů z trestné činnosti.

Virtuální měny jsou plně zakázané v některých zemích – například: Bangladéš, Bolívie, Ekvádor, Kyrgyzstán, Maroko a další. Jednou z těchto zemí je i Nepál, kde již bylo zatčeno několik lidí za obchodování s virtuálními měnami [72]. V některých zemích je možné kryptoměnu vlastnit, ale nelze s ní obchodovat – například v Indii [73].

Samostatnou kapitolou jsou světové velmoci – Rusko, Čína a Spojené státy.

V Rusku byl podán ministrem financí návrh zákona regulující virtuální měny již v prosinci 2017, kdy se strhla rozsáhlá debata na toto téma. Po této debatě byly nakonec virtuální měny plně legalizovány a začleněny do legislativy. V nově podaném zákoně jsou definovány všechny části virtuální kryptoměny v následujícím znění: Kryptoměna "typ digitálního finančního aktiva vytvořeného a účtovaného v distribuovaném registru

digitálních transakcí účastníky tohoto registru v souladu s pravidly udržování registru digitálních transakcí". Samotná mince je definován jako "typ digitálního finančního aktiva, který je vydán právnickou osobou nebo jednotlivým podnikatelem (dále jen emitent) za účelem získání financování a je zaznamenán v rejstříku digitálních záznamů." Těžení je "podnikatelská činnost zaměřená na vytvoření kryptoměny a / nebo validace za účelem získání odměny ve formě kryptoměny." Veškerá těžební činnost je legálně platná [74]. Rusko je tedy jednou z prvních zemí, která má kryptoměny definované v zákoně a vytvořilo zákon přímo se jich týkající.

V případě Číny je situace zatím stále nejasná. Podle oficiálního stanoviska nebyly uvedeny v platnost zákony na omezení bitcoinu a to ani vládou, ani Čínskou národní bankou. Musíme si ovšem uvědomit, že Čína není plně demokratickou zemí a tudíž ne vše je podpořeno zákony. V posledních měsících roku 2017 a v prvních měsících toho současného se Čínská vláda ve spolupráci s Čínskou centrální bankou snaží omezovat obchodování s kryptoměnami v zemi. Podle dostupných informací byl prováděn nátlak na místní směnárny a burzy, aby zastavily obchodování v kryptoměnách a tím nepřímo snížily motivaci k těžení, která je energeticky náročná. Těžaři obvykle využívali k těžení odlehlá místa s nadbytkem elektrické energie a dávali část zisků i tamním činitelům ve prospěch stabilních dodávek energie za zlevněnou cenu. Vláda má také v plánu blokovat stránky a aplikace nabízející obchodování s kryptoměnami. Zatím není obchodování plně zastaveno, ale je možné pouze přes zahraniční burzy, což je o mnoho pomalejší. Tento postoj Číny ke kryptoměnám je zapříčiněn hlavně obavou o ztrátu kontroly na tamním trhu. Čína není zásadně proti kryptoměnám jako takovým, protože čínská vláda si buduje také svoji kryptoměnu. Tato kryptoměna se od ostatních velmi liší, protože by byla pod plnou kontrolou Čínské centrální banky. Oznámení regulací ze strany vlády mělo za následek rychlý pokles ceny za bitcoin a přesídlení těžebních poolů do jiných zemí. Dochází tak ke ztrátě financování odlehlejších oblastí ze zisků těžařů. Také většina společností provozující burzy, směnárny, peněženky z Číny odchází jinam [75].

Poslední velmocí jsou Spojené státy americké. V USA je situace obtížnější o komplikovaný právní systém. Ve Spojených státech se zákony dělí na federální a zákony, které tvoří jednotlivé státy. Federální zákony jsou samozřejmě nadřazené zákonům jednotlivých států. Spojené státy v současnosti přes četné iniciativy, které skončily nezdarem, nemají federální zákon na přímou regulaci kryptoměn. Stejně jako v České republice

je na kryptoměny uvalena daň z příjmu, což je jediná federální iniciativa. To však neznamená, že v USA regulace nejsou. Jsou řešeny na úrovni jednotlivých států a postoje se v dané problematice velmi liší. Ve třiceti třech státech z celkových padesáti momentálně na kryptoměny nepanuje žádný názor a bitcoin není omezen a ani není připravována žádná legislativa v tomto ohledu. Zbývající státy se dělí v zásadě na tři skupiny: podporující, zakazující a jednající o omezení nebo zákazu.

Kryptoměny podporuje zatím pět států: Texas, Kansas, Montana, Tennessee a New Hampshire. V těchto státech není potřeba žádné speciální licence pro prodej kryptoměn a je přislíbeno tamní správou, že se ani žádná omezení v tomto směru nechystají. Opačný postoj má šest států: Connecticut, Georgia, Havaj, Nové Mexiko, New York a stát Washington (ne DC). Tyto státy jsou v názoru na kryptoměny téměř jednotné. Společným znakem těchto států je zákon jednotných peněžních služeb nebo jeho variace. To v praxi znamená, že bitcoin a jeho transakce jsou považovány za peněžní služby a tyto služby není možné poskytovat bez potřebné licence.

Další regulace se již v jednotlivých státech mohou lišit. Connecticut požaduje jistinu ve výši stanovené bankovním komisařem, který výši posuzuje individuálně. Georgia zase opravňuje ministerstvo bankovnictví a financí přijmout další předpisy a pravidla pro osoby zapojené do transakcí. Na Havaji je používání bitcoinu jako platidla nelegální, tzn. není umožněno nakupovat zboží a služby bez výměny na dolary. V New Yorku je vydání licence zpoplatněno a stejně jako v případě Connecticutu je i zde skládána finanční záruka. Zbylé dva státy požadují pouze licenci, není potřeba platit žádné poplatky. Do poslední skupiny spadá zbývajících šest států: Kalifornie, Florida, Severní Karolína, Pensylvánie, Jižní Karolína a Wisconsin. Tyto státy se primárně inspirují předchozími skupinami států a připravují vlastní regulace s podobnými principy. Většina připravované legislativy chce zahrnout potřebu licencí, přísnější regulace a finanční záruky určované bankami [76].

4. Forenzní analýza

V případě forenzního zkoumání výpočetní techniky se rozlišuje, jestli se dostaneme k živému systému, tzn. dané zařízení je odemčené a v zapnutém stavu nebo se k nám dostane například pouze pevný disk pro zkoumání. V prvním případě máme větší možnosti

ze systému získat více informací, protože systém může být šifrovaný a po odpojení bez správného hesla nebude možné dané zařízení zkoumat.

V následujících kapitolách se budu zabývat možnostmi zkoumání živých systémů, protože potřebný privátní klíč v bitcoin peněžence může být snáze extrahovatelný ze zapnutého systému.

Důležitým faktorem při reálném zkoumání je také vedení pečlivé dokumentace, protože v systému by nemělo docházet k nevratným změnám, pokud k tomu nemáme svolení. K těmto změnám může dojít velice snadno – například spuštěním nového programu a smazáním části operační paměti obsahující důležité informace. Při offline zkoumání je vždy doporučeno vytvořit bitovou kopii zkoumaného media, aby bylo původní medium použitelné pro případné opakované vytvoření bitové kopie a opětovného zkoumání a nedošlo k nevratným změnám. Při vytváření této kopie je velmi důležité vytvořit tuto kopii včetně volného místa. Právě ve volném prostoru mohou být smazaná data a bude tak možná jejich obnova, protože například pevné disky data fyzicky nemažou, ale pouze jim dají příznak pro přepsání a k fyzickému smazání dojde až přepisem novými daty.

Samostatnou kapitolu ve forenzním zkoumání tvoří mobilní zařízení. U těchto zařízení může být zkoumání obtížnější z důvodu velké rozmanitosti. U osobních počítačů je většinou hardwarové vybavení shodné včetně úložiště dat a liší se pouze operačním systémem. U mobilních zařízení se můžeme setkat s velkým množstvím různého hardwaru, stupňů zabezpečení a verzí operačního systému. I když na trhu jsou momentálně pouze dva široce rozšířené systémy a to: Google Android a Apple iOS. Tyto systémy bývají často hodně upravována samotnými výrobci zařízení, ale i výrobci operačního systému – v případě systémových záplat. Největších změn doznal v tomto směru právě Android, který jako původně otevřená platforma se s posledními aktualizacemi začal velmi rychle uzavírat pro zvýšení bezpečnosti, ale díky jeho otevřenému zdrojovému kódu lze zařízení se systémem Android stále zkoumat snadněji než jejich konkurenční protějšek s Apple iOS.

V následujících kapitolách se budu věnovat forenzní analýze a zajištění kryptoměn na zabavené výpočetní technice. Ke zkoumání není možné použít výpočetní techniku přímo z reálných případů, ale případné možnosti budou otestovány a popsány na fyzických zařízeních v kontrolovaném prostředí. Zaměřím se na možnosti zkoumání krypto-

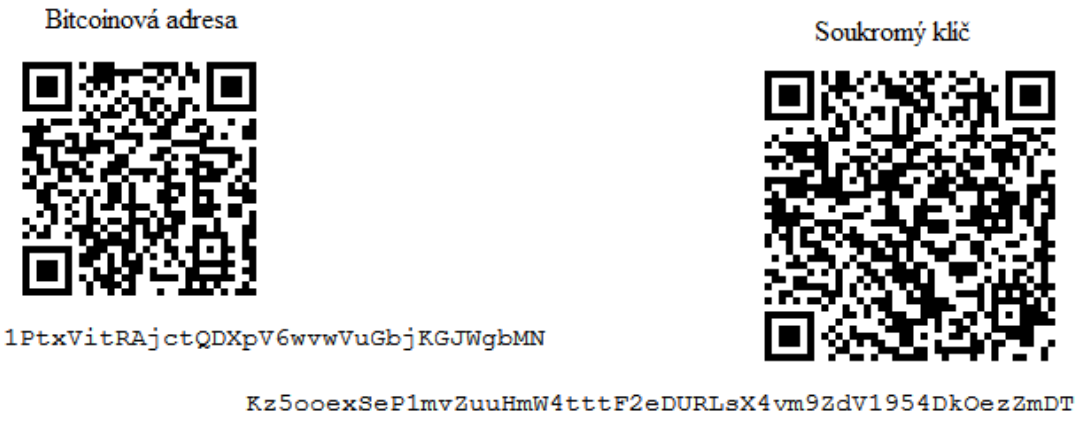
měn, na dostupné nástroje a kroky, které je nutné učinit, aby bylo možné nalezené kryptoměny zabavit nebo alespoň zabránit jejich dalšímu užívání. Z důvodu velkého množství možností se zaměřím pouze na malou část dostupných eventualit pro ukládání kryptoměn. Hlavní roli budou plnit peněženky pro ukládání kryptoměny Bitcoin, protože bez peněženky není provádění transakcí možné. Peněženkou se v případě kryptoměn může rozumět i papír, kde máme vypsané jednotlivé adresy s naší kryptoměnou a potřebný soukromý klíč. Rozeberu zde detailně funkci několika vybraných peněženek, jejich výhody, nevýhody a případné slabiny, které budou využitelné v rámci forenzního zkoumání a následného zabavení nebo případného znemožnění nakládání s kryptoměnou.

Mnemonic phrase

Před tím než se budu zabývat konkrétními peněženkami, je důležité uvést, že některé z peněženek používají tzv. frázi pro obnovení (seed, mnemonic phrase). Jedná se o sekvenci slov generovaných peněženkou při její prvotní konfiguraci, která slouží k obnovení klíče a účtu/adres. Obvykle je tato sekvence 12, 18 nebo 24 vygenerovaných slov. Slova jsou generována z množiny 2048 slov v osmi různých jazycích: anglicky, japonsky, korejsky, španělsky, čínsky (tradičně i zjednodušeně), francouzsky a italsky [77]. Peněženka musí podporovat protokol BIP39, aby bylo možné frází peněženku obnovit. Tyto protokoly obsahují pravidla, která umí vygenerovaná slova přetvořit zpět na potřebné údaje k peněžence. Toto obnovení není vázané na konkrétní peněženku, ale lze ho obvykle aplikovat na libovolnou peněženku, která podporuje výše uvedené protokoly. Frázi si můžeme kamkoliv poznamenat nebo pro větší bezpečnost zapamatovat [78].

4.1 Papírová peněženka

Nejjednodušším způsobem uložení bitcoinů nebo i jiných kryptoměn je použití papírové peněženky. Tato peněženka nepoužívá žádný software. Jak plyne z názvu, jedná se pouze o kus papíru, kde máme vytištěný soukromý klíč a k němu korespondující adresu. V základní podobě nejsou tyto údaje nijak šifrované a v případě nálezu tohoto papíru, je situace srovnatelná s nálezem hotovosti. Kdo má papír v držení, drží i obsaženou kryptoměnu a může s ní bez omezení nakládat. Papírová peněženka může vypadat jako příklad na obrázku 10. Mohou se objevovat různé variace dle konkrétní peněženky nebo webu, který papírovou peněženku vygeneroval. Další příklady papírové peněženky jsou součástí přílohy 1.



Obrázek 10: Příklad papírové peněženky [84]

I papírové peněženky však mohou využívat zabezpečení. Privátní klíč může být kódovaný (base64, WIF, hexadecimální tvar) nebo šifrovaný. Pro šifrování privátního klíče, slouží protokol BIP38. Tento protokol slouží k zašifrování soukromého klíče pomocí hesla zvoleného uživatelem. Zda je privátní klíč šifrovaný či nikoliv lze poznat na první pohled. Šifrované soukromé klíče začínají vždy 6P, toto je pevně stanovené protokolem [85]. Na to, jestli možné dešifrovat zašifrovaný privátní klíč papírové peněženky bez znalosti hesla se zaměřím v kapitole Dešifrování peněženky. Pokud heslo známe, dešifrování je možné za použití sw peněženky, která podporuje tento protokol.

Druhou formou zabezpečení papírové peněženky je rozdělení peněženky na několik částí a pro obnovení peněženky je potřebný určitý počet částí (například dvě ze tří částí), ukázka je součástí přílohy 1.

Do skupiny papírových peněženek lze také zařadit frázi pro obnovení peněženky (Mnemonic phrase), která je generována hardwarovými nebo softwarovými peněženkami, které podporují daný protokol.

4.2 Webová peněženka

Webové peněženky jsou dostupné přes klasické webové rozhraní. Uvedu zde některé zástupce a zmapuji, jaká data se dostávají do počítače, zda lze exportovat například soukromý klíč k peněžence a další. Webové peněženky spoléhají na servery třetích stran, kde jsou uloženy naše údaje. Na rozdíl od běžných bank nejsou servery vázány žádnými předpisy ani pravidly. V případě webových peněženek důvěřujeme správci webových stránek, který se vlastně stává správcem našich financí. Tato skutečnost by byla využitelná v případě nalezení webové stránky například v historii prohlížeče při zkoumání. Bohužel ak-

tuálně není v České Republice žádný poskytovatel webové peněženky a přeshraniční výměna informací v případě trestního řízení bývá velmi obtížná. Z toho důvodu se zaměříme pouze na data, která lze získat z počítače a na možnosti jejich využití.

4.2.1 Coinapult

Jedná se o základní webovou peněženku s minimalistickou funkčností. Z této peněženky nelze nic ukládat do počítače, všechny transakce se odehrávají přes web. Není možné uložit do počítače zálohu privátního klíče, jelikož tato volba není v peněžence k dispozici. Naše finance jsou tedy plně pod správou webu. Přístup je zabezpečen pomocí jména (emailové adresy) a hesla, stejně jako například přístup do emailu. Je zde možnost dodatečného zabezpečení pomocí dvoufázového ověřování. Toto ověření vyžaduje klienta TOTP (Time-based-One-time Password), jímž je například aplikace Google Autheticator. Jelikož se jedná o složitější postup, je možné usuzovat, že uživatel toto ověření nebude využívat a bude nám stačit zajistit pouze jeho jméno a heslo. Tyto informace lze potenciálně nalézt v počítači v historii prohlížeče v sekci uložených hesel. Protože se jedná o webovou stránku s centrální správou, je možné také k přístupu využít možnost resetování hesla. Tato metoda bude fungovat, pokud jsou na zkoumané technice uloženy přístupové údaje do emailu. Poslední možností na převod fondů z této peněženky je jejich převedení pomocí sms zprávy. Tento převod předpokládá přiřazené telefonní číslo k naší webové peněžence. Je tedy vhodné u zabavení techniky podrobně prozkoumat i sms zprávy. Tento typ převodu nevyžaduje žádné ověření, pouze aby číslo, ze kterého je sms poslána, bylo spárované s příslušnou peněženkou. Čísla, na které se příkazy zasílají a možné sms příkazy jsou součástí přílohy 2.

4.2.2 BitGo

Jedná se o další webovou peněženku. Tato peněženka na rozdíl od předešlé vyžaduje použití dvoufázového ověření již pro první přihlášení. Po provedení ověření za pomoci Google Autheticator je uživatel vyzván k uložení a vytištění tzv. KeyCard, která obsahuje všechny potřebné údaje. Podoba KeyCard je součástí přílohy 2. Pomocí KeyCard je možné obnovit privátní klíč, adresu peněženky a další. Ačkoliv je tato karta vyvedena v textové podobě, jsou údaje šifrované a k jejich dekódování je nutné znát heslo. Heslo se může lišit pro peněženku a pro přihlášení. Samotná peněženka požaduje vždy při přihlášení zadat jméno, heslo a kód z mobilní aplikace pro druhou fázi ověření.

Je možné nastavit, aby danému počítači bylo důvěřováno 30 dní, po tuto dobu není vyžadováno ověření druhou fází, stačí nám tedy zajistit jméno a heslo jako v případě předešlé peněženky. Peněženka nabízí možnost obnovení hesla, která ovšem v získání dat z peněženky nepomůže, protože po změně hesla je opět vyžadován kód a pro obnovu přes KeyCard bude platit staré heslo. Tato peněženka je velmi dobře zabezpečena. Jedinou možností je kombinace nalezení hesla v zabavené technice spolu s KeyCard, jiným způsobem se nelze k prostředkům této peněženky dostat.

4.2.3 Blockchain

Jedná se o poslední zkoumanou webovou peněženku. U této peněženky je několik rozdílů oproti předchozím. Prvním rozdílem je, že se nepřihlašujeme jménem, ale za pomoci ID peněženky, které je v tomto tvaru: d864e9e2-6a77-4c5c-a30c-0c537237a8af a standardně heslem. Ve výchozím stavu není nastaveno dvoufázové ověření jako aktivní, lze ho ovšem relativně snadno aktivovat, protože tato peněženka umožňuje ověření přes Google Autheticator jako v předchozích případech. Umožňuje také ověření přes mobilní telefon pomocí sms, stačí v nastavení tedy zadat pouze telefonní číslo. Dalším rozdílem je podpora fráze pro obnovení (Mnemonic phrase). Tato fráze má standardních dvanáct slov. Za pomoci této fráze lze opět obnovit celou peněženku bez znalosti ID a hesla. Při obnovení bude vytvořena kompletně nová peněženka a finance se do ní pouze převedou. Při ztrátě hesla není možnost obnovení pouze hesla, ale za pomoci dané fráze je možné obnovit celou peněženku. Obnovit zasláním na email lze pouze ID peněženky. Opět jako u předchozích případů, lze potencionálně najít uložené ID a heslo v počítači nebo obnovovací frázi na papíře, bez nalezení příslušných údajů však nelze s financemi nijak manipulovat.

Vybrané příklady nejsou všemi dostupnými webovými peněženkami na trhu, ale reprezentují skupinu s nejjednodušším přístupem až po nejkomplexnější. Webové peněženky využívají velmi podobné principy, lze tedy předpokládat, že i ostatní webové peněženky budou využívat principy nebo kombinaci principů výše uvedených peněženek. Při forenzním zkoumání j třeba vždy důkladně prohledat webovou historii včetně uložených údajů a kromě toho hledat stejně jako v případě papírových peněženek i papírové informace (obnovovací frázi, KeyCard a jiné).

4.3 Hardwarové peněženky

Hardwarové peněženky jsou zařízení k uchování adres a privátního klíče. Jedná se o offline zařízení chráněné pinem. Hardwarové peněženky představují obdobu čipových karet u běžného bankovnictví. Výrobci u těchto zařízení tvrdí, že je jejich zabezpečení na takové úrovni, že je lze používat i na napadeném systému. Tyto peněženky na rozdíl od softwarových nejsou zdarma, vzhledem k tomu, že se jedná o fyzický hardware. Ceny se pohybují okolo 100 dolarů. Pokud vlastníme větší množství bitcoinů, je taková cena peněženky zanedbatelná výměnou za mnohem vyšší bezpečnost. Zaměřím se na tři konkrétní peněženky na trhu, popíšu jejich funkčnost, zabezpečení a rozdíly. Na konci této kapitoly shrnu, jaké jsou možnosti v případě nálezu tohoto druhu peněženky, jestli zabavením dojde k zamezení přístupu k bitcoinům nebo k jejich zadržení.

4.3.1 Leger Nano S

Jedná se o jednu z hardwarových peněženek. Tato peněženka kromě bitcoinu podporuje i jiné kryptoměny: Litecoin, Ethereum a další. Do peněženky se kryptoměna zasílá přes aplikaci vytvořenou pro Google Chrome s názvem Ledger Wallet plus název kryptoměny. Aplikace funguje jako standardní peněženka, jen s tím rozdílem, že vše je uloženo na hardwarovém zařízení. S tímto zařízením je možné používat i mobilní a desktopové peněženky, například: Electrum, Mycelium, Greenbits a další. Na obrázku 11 je jasně vidět nenápadnost tohoto zařízení, které vypadá ve vypnutém stavu jako standardní flashdisk. Při zajišťování by tak mohlo dojít ke snadnému přehlédnutí. Tato peněženka používá několik druhů ochrany, aby zabezpečila privátní klíč uložený na zařízení. Z toho plyne, že pokud máme toto zařízení fyzicky v ruce, neznamená to automaticky i vlastnictví uložené kryptoměny. Základním zabezpečením je pin kód, který si uživatel nastaví při prvotní konfiguraci. Tento pin kód je minimálně čtyři čísla a maximálně osm čísel dlouhý. Prvotní pin kód se nastavuje přímo na zařízení pomocí tlačítek. Po zadání čtyř čísel je zahlášeno, že délka pinu je splněna. Pro zadání delšího pinu je potřeba další krok, můžeme tak usuzovat pravděpodobné užívání čtyřmístného pinu. Pin je potřebný k přístupu k uložené kryptoměně a nelze ho hádat hrubou silou, protože po třech špatných zadáních se celé zařízení resetuje do továrního nastavení, což znamená ztrátu celého obsahu. Tento postup je velmi dobrý z bezpečnostního hlediska, ale není úplně uživatelsky přátelský. Z toho důvodu je možné si při prvotní inicializaci nastavit záchranu v podobě

fráze pro obnovení (viz mnemonic phrase). Zařízení vygeneruje dvacet čtyři slov, které je nutné si zapsat nebo zapamatovat. V balení je přiložena karta viz druhá část obrázku 11. Při zajištění tohoto zařízení je velmi důležité hledat také tuto kartu, která umožňuje obnovení zařízení a přístup k financím. Pokud nalezneme pouze kartu s frází pro obnovení bez zařízení, přístup nám to umožní také, protože jak bylo popsáno v příslušné kapitole, je tato fráze kompatibilní napříč peněženkami, které podporují potřebné protokoly [79].

Obrázek 11: HW peněženka Ledger Nano S a fráze pro obnovu [80]

4.3.2 TREZOR

Další hardwarovou peněženkou je TREZOR. Jedná se principiálně o totožné zařízení jako je Leger Nano S. Obě tato zařízení používají ochranu pinem a možnost obnovení za pomoci nastavené fráze. Stejně jako předchozí zařízení se i toto po zadání špatného pinu resetuje a smaže veškerá data. Rozdílem oproti Leger Nano S je méně podporovaných kryptoměn, jiný vizuální design. Dalším rozdílem je práce se zařízením. Zařízení je koncipováno tak, aby jeho použití bylo bezpečné i na napadeném systému. Při zadávání pinu pomocí aplikace v počítači se na obrazovce zobrazí číselná klávesnice s otazníky místo čísel a příslušné rozložení se zobrazí na displeji zařízení. Tímto způsobem není zanechána v počítači žádná stopa. [81]

Obrázek 12: HW peněženka TREZOR [82]

4.3.3 KeepKey

Poslední hardwarovou peněženkou je keepkey. Funkcionalita této peněženky je naprosto shodná s oběma dříve jmenovanými. Je vlastně upravenou kopií peněženky TREZOR, vznikla odtržením části vývojářů. Rozdílem je pouze design a větší displej na přední straně.

Obrázek 13: HW peněženka keepkey [83]

Z výše uvedených informací vyplývá, že pro zabavení prostředků v těchto peněženkách je vždy nezbytně nutné také hledat pin nebo frázi pro obnovení, jinak jsou tyto peněženky pouze kusem nepoužitelného hardwaru. Pin je potřeba zadat při každé transakci a tudíž není možné nalézt „odemčenou“ hardwarovou peněženku. Jak bylo uvedeno v odstavci Mnemonic phrase, fráze se skládá u hardwarových peněženek z 12, 18 nebo 24 slov. Slova mohou být v těch jazycích: anglicky, japonsky, korejsky, španělsky, čínsky (tradičně i zjednodušeně), francouzsky a italsky. Vygenerovaný text vypadá například v angličtině takto: „huge web glimpse mixed winter sad oval alert inquiry giant joke chaos“. Čeština není v současné době podporována. Je tedy velmi nepravděpodobné, že by byla fráze nalezena v češtině. Muselo by se jednat o překlad vytvořený jako určité zabezpečení, ale pro uživatele by vzniklo riziko špatného překladu zpět a nemožnosti obnovení peněženky. V mediích se nedávno objevily články o špatném zabezpečení hardwarových peněženek a odcizení uložené kryptoměny. Tyto zprávy se ukázali jako nepotvrzené a jednalo se pouze o podvod na uživatele, který s fyzickým zabezpečením zařízení neměl nic společného. Uživatel měl v balení kartu s frází pro obnovení, která byla již předvyplněná a zařízení nakonfigurované na její zadání. Útočník tedy znal frázi pro obnovení uživatele a z podstaty funkčnosti této fráze se snadno dostal k prostředkům uživatele.

4.4 Peněženky pro počítače

Předposledním druhem zkoumaných peněženek jsou peněženky určené pro počítače. Uvedu opět několik zástupců peněženek a možnosti získávání dat z těchto peněženek. Postupy zde popsané se budou primárně týkat peněženek instalovaných na operačním systému Windows. Ke zkoumání peněženek byly na základě doporučení vedoucího práce použity tyto softwarové nástroje: Belkasoft Evidence Center Ultimate ve verzi 9.0 build 2500, Magnet Axiom Process ve verzi 1.2.6.8944 a Magnet Internet Evidence Finder ve verzi 6.12.6.9998, které mají nativní podporu pro vyhledávání přítomnosti kryptoměn. Jak se dozvíme v dalších kapitolách, jsou jejich možnosti omezené. Při zkoumání se ukázalo, že oba produkty společnosti Magnet mají v případě bitcoinových peněženek shodné detekční schopnosti a v dalších částech je proto již nebudu rozdělovat.

V této kapitole popíšu, co lze jednotlivými programy na zkoumaném počítači odhalit, co je možné odhalit ruční analýzou a jaký je další postup přístupu k finančním prostředkům ve formě kryptoměny bitcoin u jednotlivých peněženek. Softwarové nástroje na případné dešifrovaní hesla k peněžence a podporované možnosti u vybraných peněženek budou uvedeny v kapitole Dešifrování peněženky.

4.4.1 Bitcoin Core

První peněženkou je jedna z nejzákladnějších peněženek – Bitcoin Core 0.16.0. Název není pouze náhodný. Peněženka je vyvíjena přímo vývojáři Bitcoin Core a jedná se o jednu z nejbezpečnějších peněženek. Má vždy implementovány aktuální bezpečnostní změny na síti Bitcoin. Jedná se o peněženku pracující s plným uzlem, to znamená, že se nám na počítač stáhne celá kopie aktuálního Blockchainu, který se při každém spuštění peněženky doplňuje. Toto řešení je náročné na prostor v našem počítači, aktuální Blockchain přesahuje 175 GB a stále se rozrůstá. Další nevýhodou této peněženky je určitá uživatelská nepřívětivost, kdy není možné všechny operace ovládat přes grafické rozhraní, ale je potřeba některé operace provádět přes příkazový řádek peněženky. Jedním z příkazů je odemčení peněženky. Výhodou pro zkoumání může být fakt, že tato peněženka není implicitně šifrována. Šifrování si musí uživatel zapnout sám. Po zapnutí šifrování je nutné při každé manipulaci s uloženou kryptoměnou peněženku odemknout. Po vypršení nastaveného limitu při odemykání se opět uzamkne. Další výhodou je, že použité softwarové nástroje pro zkoumání plně podporují soubory

peněženky. Pojďme se tedy zaměřit na to, co je možné za pomoci jednotlivých softwarů u této peněženky zjistit.

Software od společnosti Belkasoft neměl problém s nalezení souboru peněženky. Bohužel z peněženky vyextrahoval velké množství bitcoinových adres. K jednotlivým adresám jsou vypsané i jejich privátní klíče – pokud není peněženka šifrovaná, v opačném případě jsou vypsané pouze šifrované podoby klíčů. Jak se ukázalo následným zkoumáním, ani jedna z nalezených adres není aktivní adresou, na které držíme bitcoiny.

Konkurenční software od společnosti Magnet je na tom lépe z pohledu nalezených adres. Nalezeny jsou pouze aktivní adresy používané peněženkou, ale na rozdíl od Belkasoftu nejsou zobrazeny privátní klíče k nalezeným adresám. Bohužel tedy nelze zkombinovat nalezené aktivní adresy softwarem Magnet s privátními klíči nalezenými pomocí konkurenčního softwaru firmy Belkasoft.

Obě softwarová řešení dokáží zjistit, kde jsou důležité soubory a zálohy peněženky uloženy a díky tomu se soubory můžeme dále pracovat. Soubory je možné importovat do nově nainstalované peněženky a zjistit, jestli jsou šifrované či nikoliv. To to lze poznat snadno v grafickém rozhraní peněženky. Pokud je v pravém spodním rohu tento symbol: 🔒, je peněženka šifrovaná a není možné získat přístup k privátnímu klíči. Pokud tam výše uvedený symbol není, je peněženka nešifrovaná a privátní klíč lze získat pomocí příkazu *dumpprivkey a* adresy, pro kterou chceme daný klíč zobrazit. Pokud je peněženka šifrovaná, je potřeba použít jeden z dešifrovacích nástrojů uvedených v kapitole Dešifrování peněženky. Adresy obsažené v peněžence jsou přístupné v obou případech a to v sekci Přijmi. Zda jsou na nalezených adresách nějaké finanční prostředky, je viditelné přímo v peněžence. V případě nalezených adres si to lze ověřit na adrese Blockchain.info.

Kopií peněženky Bitcoin Core je peněženka Bitcoin Knots spravovaná pouze jedním člověkem. Jedná se o totožnou peněženku pouze s drobnými vylepšeními nebo rychlejší implementací změn, jinak z hlediska analýzy je totožná.

4.4.2 Bitcoin Armory

Bitcoin Armory 0.96 je dalším testovaným zástupcem peněženek pro systém Windows. Vyžaduje ke své funkčnosti plně aktualizovanou peněženku Bitcoin Core, protože využívá její plný Blockchain uzel. Stejně jako u Bitcoin Core ani zde není nutné šifrování a můžeme objevit otevřenou peněženku. Šifrování je samozřejmě podporované.

Jestli je peněženka šifrovaná či nikoliv, se dozvíme na základní obrazovce programu, kde v položce Security je vidět, zda je šifrováno (Encrypted) či nikoliv. Stejně jako u Bitcoin Core jsou v případě šifrování dostupné všechny adresy a to i v případě importu z jiného počítače do čisté peněženky. Tato peněženka na rozdíl od Bitcoin Core má více funkcí a je uživatelsky více přívětivá. Není potřeba používat žádné příkazy v konzoli, vše lze ovládat přes grafické rozhraní. Peněženka také podporuje zálohu do papírové podoby včetně vyexportovaných soukromých klíčů (ukázka je součástí přílohy 3), které jsou i po odemčení kódované pomocí base58, kterou ale lze velmi jednoduše dekódovat.

Nyní se zaměřím na automatickou detekci Bitcoin Armory vybranými forenzními nástroji.

Software společnosti Belkasoft byl v hledání peněženky úspěšný. Co se detekovaných adres týká, opět došlo i k detekci neaktivních adres, nicméně jsou uvedeny i aktivní adresy včetně privátního klíče, pokud je peněženka v nešifrované formě. Máme tedy vše potřebné pro zabavení finančních prostředků. V případě zašifrované peněženky software nalezl umístění souborů peněženky pro další dešifrování. Zároveň úspěšně rozlišil primární a záložní peněženku.

Bohužel konkurenční software společnosti Magnet nebyl schopný tuto peněženku jakkoliv detekovat. Detekce by musela být provedena nepřímo například pomocí nalezených ikon peněženky a na základě tohoto nálezu vyhledat soubory peněženky ručně. Soubory se nacházejí ve výchozím stavu v adresáři C:\Users\username\ AppData \Roaming\Armory.

Hlavní soubor peněženky je pojmenovaný armory_nazevpeněženky.wallet.

Podoba názvu je generována automaticky a uživatel si může volit pouze název peněženky. Ze zkoumání ostatních souborů v úložišti peněženky vyplynulo, že nejjednodušším způsobem zjištění podrobností, je vytvořit čistou instalaci peněženky a soubory ze zkoumaného systému nakopírovat. Stačí nakopírovat pouze soubor peněženky.

Výše uvedené informace platí o pokročilém módu peněženky. Peněženka ještě obsahuje expertní mód. Ten dělá zkoumání a případné zabavení prostředků obtížnějším díky možnosti vytvoření Multi-Signature Lockbox a fragmented backup. První funkce sice neznemožní přístup k adresám a výši zůstatku na těchto adresách, ale velmi komplikuje zabavení takových prostředků. Lockbox umožňuje sdílené nakládání s prostředky, kde si

můžeme zvolit, kolik podpisů potřebujeme k odeslání platby. Pokud tedy zabavíme peněženku s Lockboxem, kde je vyžadován minimálně jeden další podpis, nemůžeme bez tohoto podpisu pokračovat. Lockbox lze detekovat podle prefixu Lockbox a přípony *.lockbox.def.
Celý název souboru může vypadat například takto: Lockbox_KUvMwrGi_.lockbox.def.

Druhá funkce je pokročilejší metoda zálohování do papírové peněženky. Fragmented backup funguje obdobně jako Lockbox, ale není potřeba více podpisů, ale více částí zálohy. Nestačí nám tedy nalézt pouze jeden „papír“ s údaji, ale je třeba nalézt předem zvolený počet z celkového počtu. Jak vypadá fragmented backup, je vyobrazeno v příloze 3. Tuto formu zálohy lze vyexportovat také do oddělených souborů. Soubory lze detekovat podle přípony *.frag. Obsah souboru je totožný s podobou papírové verze, pouze neobsahuje grafiku. Soubory lze otevírat v poznámkovém bloku a neobsahují šifrování.

4.4.3 mSigna

Další zkoumanou peněženkou byla peněženka mSigna 0.10.6 od společnosti Ciphrex. Peněženka může využívat opět Bitcoin Core nebo se může připojovat na IP adresu plného uzlu mimo počítač a tím šetřit místo. Stejně jako v případě obou předchozích peněženek je i zde možné po otevření peněženky zobrazit adresy, kde se mohou nacházet bitcoiny. Stejně tak je vidět i zůstatek sečtený z našich adres. Peněženka používá pro uchování klíčů tak zvaný keychain. Ten není ve výchozím stavu šifrovaný a obsahuje všechny důležité klíče – jak privátní, tak i frázi pro obnovení peněženky, kterou lze vyexportovat. Jedná se o frázi pro obnovení o maximální délce dvaceti čtyř slov. Keychain lze uzamknout, ale pokud nenastavíme šifrovací heslo, lze ho opět v peněžence odemknout. Pokud ovšem nastavíme šifrovací heslo, není možný přístup k danému keychainu a peněženky je potřeba dešifrovat. Možnosti dešifrování jsou uvedeny v kapitole Dešifrování peněženky. Frázi pro obnovení je možné vytisknout do papírové podoby. Peněženka nemá specifickou stránku jako v případě Armory, proto nebude příklad součástí přílohy. Jedná se o řetězec 24 anglických slov.

Při použití obou softwarů pro zkoumání bohužel nedošlo k odhalení peněženky ani jedním z nich. Přítomnost peněženky lze zjistit pouze nepřímým způsobem například podle ikon programu. Peněženka bohužel také nemá výchozí umístění jako v případě předchozích peněženek, ale uživatel si při založení nové peněženky určuje, kam daný soubor chce uložit. Poznávacím znamením souboru peněženky je přípona *.vault. Další

exportované soubory mohou mít příponu *.priv a *.pub – jedná se o vyexportovaný privátní a veřejný klíč. Tyto klíče je možné importovat do nově vytvořené peněženky bez potřeby znalosti jakéhokoliv předchozího hesla, protože klíče se exportují po odemčení peněženky. Stejně jako klíče je i v nově nainstalované peněžence potřeba otevřít soubor peněženky nalezený při zkoumání, pro snadné zjištění zůstatku a zda je peněženka šifrovaná.

4.4.4 Bither

Předposlední peněženkou, na kterou se zaměřím je Bither 1.4.5. Nevyžaduje plný uzel nainstalovaný na počítači. Hlavní funkcí, kterou tato peněženka přidává, je zobrazení počtu bitcoinů a jejich aktuální cena v jedné z podporovaných měn. Tato funkcionalita je hlavním důvodem, proč ji někteří uživatelé používají. Je to jedna z mála funkcí, které peněženku odlišují od ostatních. Z funkčního hlediska se jedná o velmi jednoduchou peněženku, takže si ji popíši jen ve zkratce.

Peněženka vyžaduje vždy při vytvoření zadání hesla. Heslo je potřeba zadávat při každé manipulaci s peněženkou. Není požadované při otevření peněženky, kdy lze zobrazit zůstatek a veřejnou adresu peněženky. Pro manipulaci s prostředky v peněžence je tedy potřeba zjistit heslo – zjištění hesla se věnuji v kapitole Dešifrování peněženky. Peněženka také využívá fráze pro obnovení. Ta je opět exportována ve formě QR kódu nebo v čisté textové podobě a je složena z dvanácti slov.

Vybrané softwarové nástroje tuto peněženku nebyly schopny automaticky detekovat a je tedy potřeba peněženku hledat ručně na základě předem známých parametrů. Soubory peněženky se opět nachází ve výchozím nastavení v umístění C:\Users\username\App Data\Roaming\Bither. Peněženka si uchovává adresy a klíče v databázových souborech na výše uvedené cestě s názvy bither.db a address.db. Názvy těchto souborů jsou dané peněženkou a uživatel nemá možnost názvy volit. Soubor je možné otevřít jakýmkoliv nástrojem na prohlížení databázových souborů, ale soubor address.db je vždy šifrovaný. Názvy souborů peněženky jsou zavádějící, protože soubor obsahující adresy je bither.db a soubor obsahující privátní klíče je address.db. Adresy šifrované nejsou a zůstatek lze tak snadno ověřit importem do čisté peněženky nebo pomocí webu Blockchain.info. Import se provede nakopírováním souborů peněženky do stejného adresáře nově vytvořené peněženky.

4.4.5 Electrum

Poslední peněženkou je Electrum 3.1.0. Je mezi uživateli velmi oblíbená. Jedná se o jednoduchou peněženku, která nevyžaduje plný uzel, používá servery Electrum. Peněženka se neinstaluje a díky použití fráze pro obnovení ji lze při znalosti dané fráze obnovit kdekoliv. Peněženka při vytváření nabízí několik stupňů zabezpečení. Prvním je standardní zabezpečení, kde použijeme pouze heslo a je vygenerována fráze pro obnovení. Druhou možností je dvoustupňové ověřování, které využívá Google Autheticator. Tato služba ale není zdarma, platí se procenta za určitý objem transakcí. Pokud známe frázi pro obnovení peněženky, je zabezpečení neúčinné, protože po obnovení peněženky lze toto ověřování vypnout bez vlastnění potřebného kódu z Google Authetica-tor. Posledním typem zabezpečení, který tato peněženka podporuje, je multi-signiture wallet. Stejně jako v případě Bitcoin Armory to znamená, že pro odeslání nebo zabavení fondů je potřeba určitý počet schválení, kde minimum u této peněženky jsou dva lidé. V tomto případě je nález fráze pro obnovení jednoho z uživatelů použitelný pouze na zjištění zůstatku a adres v peněžence.

Bohužel ani tato peněženka není detekovatelná žádným ze zkoušených softwarových nástrojů. Stejně jako v ostatních případech si i tato peněženka vytváří implicitně soubory v umístění C:\Users\username\AppData\Roaming\Electrum. V podsložce wallets se nacházejí všechny peněženky. Soubory peněženky se mohou ale nacházet i kdekoliv mimo toto umístění – při spuštění peněženky lze pouze vybrat jiné umístění. Bohužel soubory nemají žádnou specifickou příponu, ale jedná se o standardní file. Detekce této peněženky je tedy obtížnější i o to, že se peněženka neinstaluje, ale pouze spouští, takže se v počítači nenacházejí ani fragmenty tipu ikony a podobně. Vyhledání je možné hledáním slova electrum. Pokud detekujeme tuto peněženku ve zkoumané technice, je možné se do jejích dat dostat pouze za pomoci dvanáctislovné fráze pro obnovení. Možnost importování souboru peněženky do čistě nainstalované peněženky zde nelze aplikovat, protože soubor po otevření vyžaduje heslo. Není možné se dostat ani k zůstatku a případným adresám. Možnosti zjištění hesla se budeme i u této peněženky věnovat v kapitole Dešifrování peněženky.

4.5 Mobilní peněženky

Posledním druhem zkoumaných peněženek jsou peněženky určené pro mobilní zařízení. Vybral jsem peněženky pro systém Android, vzhledem k tomu, že se jedná o nejrozšířenější mobilní systém se 75 % podílem na trhu [86]. Popíšu několik vybraných zástupců peněženek, které jsou určeny pouze pro mobilní telefony. Budou zde uvedeny i dvě multiplatformní peněženky a jejich rozdíly proti počítačové verzi. Zaměřím se také na potenciální slabiny peněženek. Provedu fyzickou analýzu zařízení a popíšu znaky, podle kterých můžeme usuzovat na přítomnost mobilní peněženky. Dále zjistím, jaká data lze z této peněženky získat. Fyzická analýza byla zvolena z důvodu, že nemodifikuje data, na rozdíl od logické analýzy při zapnutém zařízení. Fyzická analýza byla provedena na telefonech Honor 7 s Androidem verze 6.0 a Samsung Galaxy S Duos s Androidem verze 4.0.4. U obou telefonů byla vytvořena fyzická kopie telefonu. V případě Honoru byl použit UFED 4PC od společnosti Cellebrite. U Samsungu byl použit program XRY. V Samsungu bylo možné vyzkoušet pouze peněženky MyCelium a Bitcoin Wallet, ostatní zkoumané peněženky nepodporují takto starou verzi androidu. Telefony nepoužívaly v době zkoumání žádnou formu šifrování. Honor používal pouze zámek obrazovky, který ovšem umí software UFED u vybraných modelů obejít. Mimo nástrojů UFED a XRY byly použité i stejné nástroje jako v případě peněženek pro počítače. Možnost použití nalezených souborů v případě potřeby dešifrovat nebo nalézt heslo (pin) peněženky bude uvedena v kapitole Dešifrování peněženky.

4.5.1 MyCelium

První vybranou peněženkou je MyCelium 2.9.11.7. Tato peněženka je vyhledávaná pro velké množství nabízených funkcí. Mezi hlavní funkce patří podpora práce s hardwarovými a papírovými peněženkami. Při založení peněženky je požadováno nastavení šestimístného pinu a zároveň je vytvořena záloha v podobě dvanácti slovné fráze pro obnovení. Zadání pinu je požadováno při každé operaci. Nemusí se zadávat při otevření peněženky a prohlížení zůstatku. Privátní klíče není možné samostatně exportovat, ale pouze jako součást zálohy peněženky pomocí fráze pro obnovení.

Pro zkoumání této peněženky byly vytvořeny fyzické kopie obou zařízení pomocí softwarů UFED a XRY. Byly vyzkoušeny softwary pro detekci bitcoinů jako v případě peněženek pro počítače. Bohužel automatická detekce softwarem Belkasoft a Magnet

nebyla u této peněženky úspěšná a bylo proto nutné provést ruční analýzu. Ta byla provedena za pomoci vyhledávání názvu peněženky ve všech čtyřech softwarových řešeních. Při vyhledávání ve fyzické kopii vykazovaly všechny čtyři nástroje shodné výsledky.

Bylo zjištěno, že stejně jako v případě některých peněženek pro počítač, má i tato peněženka určenou cestu, kam se soubory peněženky ukládají. Soubory důležité pro zkoumání jsou uloženy v adresáři /root/data/com.mycelium.wallet, který obsahuje několik podsložek. Cesta se může u různých zařízení drobně lišit. V kopii z telefonu Samsung je cesta: /data/data/com.mycelium.wallet, ale název aplikace com.mycelium.wallet je všude shodný. Na základě podrobnějšího zkoumání jsem objevil soubor, který obsahuje pin k peněžence v nešifrované podobě. Tento soubor je uložen v /root/data/com.mycelium.wallet/shared_prefs/settings.xml. Po otevření souboru je pin zobrazen v položce string name="PIN" viz obrázek 14.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<map>
    <boolean value="false" name="KeyManagementLocked"/>
    <string name="PinResettable">1</string>
    <int value="0" name="failedPinCount"/>
    <string name="PIN">283917</string>
    <string name="selectedAccount">44a4feb8-4eed-8ba5-2bf7-26fac7127726</string>
    <string name="tor_mode">ONLY_HTTPS</string>
  - <set name="selectedFiatCurrencies">
        <string>USD</string>
    </set>
</map>
```

Obrázek 14 Soubor s pinem MyCelium

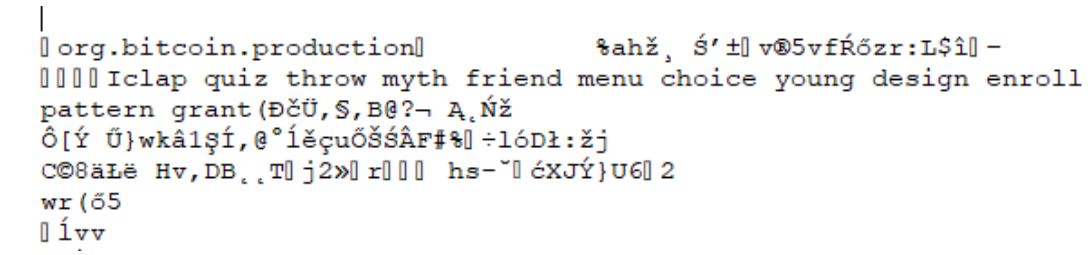
S pomocí pinu máme plný přístup k peněžence, včetně možnosti převodu financí a zjištění obnovovací fráze. Použití pinu na zařízení bude znamenat změnu dat v telefonu. Adresy a privátní klíče se v úložišti telefonu nepodařilo nalézt.

4.5.2 Bitcoin Wallet

Další zvolenou peněženkou je Bitcoin Wallet 6.16. Jedná se o velmi jednoduchou peněženku, která nabízí navíc pouze načtení papírové peněženky. Tato peněženka není ve výchozím stavu chráněna pinem, ale šifrování samozřejmě podporuje. Z peněženky lze vyexportovat zálohu, která je vždy šifrovaná. Soubor zálohy se jmenuje například bitcoin-wallet-backup-2018-03-31. Možnosti dešifrování tohoto souboru si popíšeme v kapitole Dešifrování peněženky.

Stejně jako v případě peněženky MyCelium bylo zkoumání prováděno z fyzické kopie obou zařízení. Automatická detekce softwarem společnosti Belkasoft byla úspěšná. Byly nalezeny všechny adresy obsažené v peněžence včetně privátních klíčů. Nalezené privátní klíče jsou v šifrované nebo nešifrované podobě, podle toho, jestli je peněženka zabezpečena pinem. Adresy byly detekovány všechny včetně neaktivních. V detekovaném souboru jsou obsaženy i aktivní adresy. Zůstatky na získaných adresách je možné zkontrolovat na adrese Blockchain.info. Konkurenční software společnosti Magnet nebyl v hledání úspěšný.

Na základě poznatků získaných při zkoumání předchozí peněženky byla provedena také ruční analýza, při které byly procházeny soubory uložené v mobilním telefonu. Úložiště této peněženky má lokaci /root/data/de.schildbach.wallet/files. V tomto úložišti nás konkrétně zajímá soubor „wallet-protobuf“. Pokud není peněženka chráněna pinem, je v tomto souboru možné nalézt frázi pro obnovení peněženky. To poznáme po otevření souboru ve WordPadu – začátek musí vypadat jako na obrázku 15. V opačném případě je peněženka chráněná pinem. Zda je možné soubor dešifrovat si uvedeme v kapitole Dešifrování peněženky.



Obrázek 15 Soubor wallet-protobuf

4.5.3 Greenbits

GreenBits 2.03 používá různé možnosti zabezpečení. Ve vychozím stavu není uzamčená. Prvním zabezpečením, které je možné nastavit, je šestimístný pin. Pokud je peněženka zabezpečena pinem, pin nelze hádat hrubou silou, protože po třech špatných pokusech je peněženka vymazána a musí být použita fráze pro obnovení. K uložení této fráze jsme vyzváni v prvním kroku při vytváření nové peněženky. Fráze lze uložit ve formě obrázku, který je součástí přílohy 4.

Dalším výchozím zabezpečením je automatické uzamknutí peněženky po pěti minutách nečinnosti. Pokud bychom se dostali k zapnutému zařízení, je nepravděpodobné, že peněženka bude odemčená a navíc bychom se dopustili manipulace s daty telefonu.

Mimo těchto základních zabezpečení je možné nastavit také dvoufázové ověřování. Lze použít několik možností: email, Google Autheticator, SMS, telefonní hovor. Můžeme také používat jedno i více možností dvoufázového ověřování najednou.

Pro zkoumání byla opět použita fyzická kopie zařízení, ale v tomto případě pouze telefonu Honor. Verze Androidu druhého telefonu není podporovaná. Ani jeden z použitých softwarových nástrojů nebyl schopný peněženku automaticky detekovat. Opět jsem tak musel provést ruční analýzu.

Ruční analýza byla provedena lokalizací hlavního úložiště peněženky, za použití cesty: /root/data/com.greenaddress.greenbits_android_wallet. Složka obsahuje několik podsložek, po detailnějším prohledávání jsem objevil soubor s názvem pin.xml, ale jak se ukázalo (na rozdíl od peněženky MyCelium), je pin zde šifrovaný. Dalším zajímavým souborem může být com.greenaddress.greenbits_android_wallet _preferences.xml, kde zjistíme, jestli peněženka využívá dvoufázové ověřování. Po analýze ostatních nalezených souborů se ukázalo, že peněženka využívá velmi dobré šifrování všech údajů. Nemá pouze jeden soubor, který by se dal použít pro dešifrování jako v případě peněženek pro počítače a některých mobilních peněženek. Jedinou možností k zabavení prostředků z této peněženky je nalezení fráze pro obnovení vyobrazené v příloze 4.

4.5.4 Electrum

Předposledním vybraným zástupcem mobilních peněženek je peněženka Electrum 3.1.2. Jedná se o peněženku vytvořenou stejnými tvůrci jako v případě její počítačové varianty, nabízí ale méně funkcí. Je vždy zabezpečena pinem. Požaduje nastavení pinu při prvotním vytvoření hned po zapsání fráze pro obnovení, kterou lze opět uložit ve formě obrázku, který je součástí přílohy 4. Pin je v tomto případě standardně šestimístný. Pin je teoreticky možné zkoušet na zařízení, protože zde není omezen počet chybných zadání. Z peněženky nelze exportovat zálohy ani klíče, vše je obsaženo ve frázi pro obnovení.

U této peněženky, stejně jako v případě GreenBits, byla použita z důvodu nekompatibility s verzí Android u Samsungu, fyzická kopie pouze telefonu Honor. Stejné byly výsledky analýzy pomocí používaného software. Ani jeden použitý software nebyl schopen peněženku automaticky detekovat. Analýza musela být opět provedena ručně.

Prvním krokem bylo nalezení úložiště peněženky jako v předchozích případech. Úložiště peněženky se nachází v adresáři /root/data/org.electrum.electrum/files/. Tento adresář na rozdíl od předchozích peněženek obsahuje velké množství souborů, ale i tak se podařilo lokalizovat soubor peněženky. Soubory peněženek se nachází v adresáři /root/data /org.electrum.electrum/files/data/wallets. Obsah souboru peněženky není na rozdíl proti počítačové verzi celý šifrovaný. V nešifrované podobě jsou zde vypsané všechny adresy obsažené v peněžence. V šifrované podobě lze nalézt fráze pro obnovení a privátní klíč. I u této peněženky je vhodné v první řadě hledat frázi pro obnovení. Na možnosti dešifrování se opět podíváme v kapitole Dešifrování peněženky.

4.5.5 Bither

Posledním vybraným zástupcem mobilních peněženek je peněženka Bither 1.8.2. Jako v případě peněženky Electrum se jedná o kopii peněženky stejného názvu pro počítače. Stejně jako v případě počítačové verze se jedná o jednoduchou peněženku, která pro otevření nevyžaduje heslo. Heslo je vyžadováno pouze při provádění transakcí nebo některých úprav v peněžence. Peněženka také nabízí automatický přepočet hodnoty bitcoinu na vybrané měny.

Peněženka byla nainstalována pouze na zařízení Honor, ze stejného důvodu jako předchozí dvě peněženky. Automatické zkoumání za pomoci softwarových nástrojů nebylo úspěšné, ani jeden nebyl opět schopen soubory peněženky automaticky detekovat. Byla tak nutná ruční analýza fyzické kopie.

Jako v předchozích případech bylo třeba lokalizovat úložiště peněženky. Soubory peněženky se nacházejí v adresáři: /Root/data/net.bither/databases/. V tomto úložišti se nacházejí totožné soubory jako v případě peněženky pro počítače – address.db a bitherj.db. Soubor address.db je šifrovaný (na možnosti dešifrování se zaměříme v kapitole Dešifrování peněženky). Soubor bitherj.db je možné otevřít jakýmkoliv databázovým nástrojem a obsahuje všechny adresy pro uchovávání bitcoinů. Obsaženy jsou všechny adresy včetně neaktivních. Před samotným započetím dešifrování je vhodné stejně jako v předchozích případech zjistit, jestli jsou adresy aktivní a obsahují bitcoiny.

Z provedeného zkoumání vybraných zástupců vyplývá, že někteří tvůrci mobilních peněženek více spoléhají na zabezpečení mobilního zařízení než na zabezpečení vlastního softwaru. Prověřování by samozřejmě nebylo úspěšné bez použití specializovaných nástrojů (UFED a XRY) pro vytvoření fyzické kopie ze zkoumaných zařízení. K souborům

uváděným u jednotlivých peněženek je přístup pouze za pomoci těchto nástrojů, nebo pokud by byl zkoumaný telefon takzvaně „rootnutý“ a uživatel telefonu by měl plná administrátorská práva.

4.6 Dešifrování peněženky

V této kapitole se zaměříme na možnosti dešifrování zkoumaných peněženek a možnosti nalezení hesel a pinů k těmto peněženkám. V případě zapomenutého hesla nebo potřeby obnovit heslo pro zabavení nalezené kryptoměny máme několik možností. Můžeme heslo zkoušet zjistit pomocí procesoru nebo grafické karty. V takovém případě jsou grafické karty mnohem výkonnější než procesory, ale ne všechny peněženky dešifrování na grafické kartě podporují. Výpočetní výkon pro dešifrování bitcoin peněženky byl testován ve dvou programech pro dešifrování: btcrecover a HashCat. Druhý jmenovaný je optimalizovaný primárně pro použití pouze s grafickou kartou. V níže uvedené tabulce je uveden výkon testovaného hardwaru v jednotlivých programech. Jak již bylo zmíněno, HashCat je určen pouze pro grafické karty, proto je u procesorů uvedeno N/A. Uvedené hodnoty jsou hashe za vteřinu. Programy počítají hashe a porovnávají je s hashí peněženky. Z níže uvedené tabulky jasně plyne, že pokud to lze, je vhodné použít pro dešifrování grafické karty. Obě softwarová řešení podporují více grafických karet zároveň.

Tabulka 1 Testovaný hardware

Hardware	**btcrecover**	**HashCat**
Ryzen 7 1700 8C/16T	20 h/s	N/A
AMD Radeon RX580 8GB	1170 h/s	2073 h/s
Intel Xeon Hyper-V 32T	62 h/s	N/A

Dalším faktorem ovlivňujícím hledání (prolomení) hesla je použitá metoda. V zásadě máme na výběr ze dvou metod, kdy reálně v úvahu připadá pouze jedna. První metodou je tzv. hrubá síla, odhadované časy jsou uvedené v tabulce 2. V příkladové tabulce jsou uvedené časy pro heslo o délce 8 znaků, kde se mohou znaky opakovat. Jedná se o nejhorší možné případy. Dle statistické pravděpodobnosti lze heslo v průměru nalézt v cca polovině možností. Pro výpočet času bude brán výkonu procesoru Intel v btcrecover a grafické karty v programu HashCat pro peněženku Bitcoin Core.

Vzorec pro výpočet možností vypadá takto:

$$\check{c}as = \frac{(počet\ znaků\ vstupní\ abecedy)^{délku\ hesla}}{výpočetní\ výkon\ zařízení}$$

Tabulka 2 Dešifrování hrubou silou

Vstupní abeceda	Poč. znaků	Kombinace	Čas CPU	Čas GPU
Pouze čísla	10	100000000	18,6 dne	13,3 hod
Pouze malá písmena	26	2,08827E+11	106 let	3,2 roku
Velká a malá písmena	52	5,34597E+13	27 341 let	817 let
Čísla, malá a velká písmena	62	2,1834E+14	111 670 let	3 339 let
Řádek výše + speciální znaky	80	1,67772E+15	858 068 let	25 663 let

Z tabulky 2 jasně vyplývá, že hrubou sílu můžeme použít pouze v případě obrovského výpočetního výkonu nebo pokud je heslo velmi krátké, v opačném případě za použití standardního počítače není dešifrování možné provést.

Druhou metodou je dešifrování za použití slovníku nejčastějších hesel. Tyto slovníky jsou značně rozsáhlé a obsahují velké množství kombinací. Množství hesel obsažené ve slovnících je však mnohonásobně nižší v porovnání s hrubou silou. Pokud vezmeme slovník obsahující deset milionů hesel a pro dešifrování použijeme grafickou kartu, bude nám prolomení na zkoušené grafické kartě trvat cca jednu hodinu a dvacet minut. Existují i slovníky obsahující kombinace s českými slovy, ovšem při použití opravdu dlouhého a náhodně poskládaného hesla je pravděpodobnost úspěchu malá.

Předtím než podrobněji popíšu softwarová řešení pro dešifrování peněženek, uvedeme si možnosti dešifrování papírové peněženky. V kapitole Papírová peněženka jsme si uvedli, že lze u této peněženky používat šifrování promocí protokolu BIP38. Jak se ukázalo, dešifrování bez znalosti nezašifrovaného privátního klíče není možné. Pokud použijeme pro dešifrování špatné heslo, privátní klíč se sice dešifruje, ale nemáme možnost potvrdit, jestli se jedná o správný klíč.

4.6.1 Btcrecover

Jedná se o program napsaný v jazyce Python, který slouží k obnově zapomenutého hesla. Primárním účelem tohoto programu je obnova hesla, pokud známe alespoň část hesla nebo jsme při jeho zadávání udělali překlep. V případě zkoumání neznámého zařízení není možné použít hrubou sílu, jak jsme si uvedli výše. Příklady budou uváděny pro slovníkový vstup. Součástí přílohy 5 je návod na instalaci potřebného softwaru pro chod samotného programu a pokročilejší nastavení pro dešifrování. Pro spuštění samotného programu po nainstalování potřebného softwaru je potřeba otevřít příkazový řádek jako správce, za pomoci příkazu cd je nutné se dostat do složky, kde máme btcrecover umístění

– pro zjednodušení budeme předpokládat C:\btc-recover. Po nastavení správné složky je příkaz pro spuštění:

```
C:\Python27\python btcrecover.py --help
```

Tento příkaz nám vypíše všechny možné příkazy programu, které lze použít. Předpona C:\Python27\python je nutná – pokud není tato lokace uvedena v systémových proměnných. Dále budu uvádět příklady bez předpony. Pro samotné spuštění práce programu je potřeba zadat více parametrů. Aby program mohl začít dešifrování, je třeba si připravit soubor peněženky a list hesel, které budeme zkoušet, například stažený slovník nejčastějších hesel. Příkaz tedy bude:

```
btcrecover.py --passwordlist pass.txt --wallet bcp.dat
```

Tento příkaz začne zkoušet hesla ke zkoumané peněžence bcp.dat, kterou jsme si zvolili přepínačem --wallet + cesta k peněžence a seznam hesel pass.txt přepínačem --passwordlist. V tomto konkrétním případě jsou oba soubory ve složce btc-recover, není to podmínkou, lze zadat libovolnou cestu. Příkaz začne zkoušet hesla za pomoci našeho procesoru. Jak jsem již uvedl, dešifrování grafickou kartou je mnohem rychlejší, ukážeme si potřebné příkazy. Přepínač pro dešifrování hesla na grafické kartě je --enable-gpu, celý příkaz bude:

```
btcrecover.py --passwordlist pass.txt --wallet bcp.dat --enable-gpu
```

Takto aktivujeme hledání hesla pomocí grafické karty, jedná se o úplně základní nastavení. Jak optimalizovat nastavení a získat maximální rychlost dešifrování je uvedeno v příloze 5. Tento program má slabší optimalizaci pro grafické karty a na grafické kartě je možné dešifrovat pouze peněženky Bitcoin Core/Knots a Armory.

Tímto softwarem byla testována funkčnost dešifrování pomocí procesoru u všech zkoumaných peněženek pro počítače: Bitcoin Core, Armory, mSigna, Bither a Electrum. Všechny peněženky se povedlo úspěšně dešifrovat za pomoci omezené vstupní abecedy a za využití pouze základních příkazů zde uvedených. U peněženky Bither je nutné použít soubor address.db jako vstupní soubor peněženky pro dešifrování. Poslední funkčností softwaru je možnost dešifrovat frázi pro obnovení, ale to předpokládá, že známe většinu fráze, celou frázi nelze dešifrovat. Příkaz je součástí přílohy 5.

Možnosti dešifrování mobilních peněženek byly testovány na těchto peněženkách: Bitcoin Wallet, Electrum a Bither.

U Bitcoin Wallet jsou dvě možnosti dešifrování –možnost dešifrovat heslo zálohy nebo pin peněženky. Zjištění hesla pro zálohu se provede standardními příkazy jako v případě peněženek pro počítače. Jako vstupní soubor peněženky použijeme soubor se zálohou. Druhou možností je nalezení pinu peněženky. Pin lze získat přímo ze souboru peněženky. Pokud není soubor k dispozici, je možné pin získat i ze souboru zálohy. Příkaz pro získání pinu z obou souborů je shodný, pouze s tím rozdílem, že u souboru zálohy musíme znát dešifrovací heslo.

Příkaz pro získání pinu je následující:

```
btcrecover.py --tokenlist token.txt --wallet wallet-protobuf --android-pin --min-token 6 --max-token 6
```

V tomto případě můžeme použít hrubou sílu, protože víme, že se jedná o pin složený pouze z čísel o délce přesně šest znaků (jedná se o cca 1 000 000 možností). Délku pinu nám zde omezují přepínače min a max-token. Přepínač --adroid-pin specifikuje, že hledáme pin. Tento příkaz funguje pouze pro Bitcoin Wallet, ostatní peněženky nepodporuje. Po nalezení pinu je potřeba dešifrovat soubor peněženky, to provedeme dalším nástrojem uvedeným v příloze 5, pomocí kterého získáme frázi pro obnovení.

Druhou zkoušenou peněženkou byla Electrum, bohužel se ukázalo, že soubor této peněženky není podporován jako v případě její počítačové verze (nepodporovaná verze).

Poslední zkoušenou peněženkou byla Bither, která používá stejné principy jako její počítačová verze, nalezení hesla je tedy bez problému proveditelné za použití příkazů pro počítačové peněženky.

4.6.2 HashCat

Druhým softwarem pro dešifrování peněženky je HashCat 4.1.0. Je primárně optimalizovaný pro dešifrování na grafické kartě. Jeho hlavní výhodou je téměř dvojnásobný výpočetní výkon proti btcrecover. Hlavní nevýhodou je neschopnost pracovat přímo se souborem peněženky a také je, jako v případě btcrecover, omezen počet peněženek podporovaných přes grafickou kartu. Pro dešifrování hesla je nutné nejdříve vytvořit hash dané peněženky za pomoci dalšího programu, který je uveden v příloze 5, spolu s instalačními pokyny, stejně jako v případě btcrecover. Program se spouští opět přes příkazový řádek, který musíme spustit jako správce. Dalším shodným prvkem je nutnost namapovat příkazový řádek do složky, kde máme HashCat umístěný.

Začneme příkazem, který nám vypíše všechny možnosti programu a tím je:

```
hashcat64.exe --help
```

Z výpisu je jasné, že program má velmi široký záběr v dešifrování a podporuje mnoho šifer. Zaměříme na příkaz, který využijeme k nalezení hesla pro zkoumanou bitcoinovou peněženku.

Příkaz bude vypadat tedy takto:

```
hashcat64.exe -m 11300 -O btc.txt pass.txt --force
```

Příkazem programu sdělíme, že chceme dešifrovat bitcoinovou peněženku. Přepínačem --m vybereme jednu z podporovaných peněženek: 11300 Bitcoin Core/Knots, 16600 Electrum. Soubor btc.txt obsahuje vytvořenou hash naší peněženky a pass.txt je soubor s hesly. Přepínač --force, zabezpečuje ignorování chyb při spuštění. Nejčastějším varováním je špatný ovladač grafické karty. Pokud by byl ovladač opravdu vadný, nemusí dojít ke korektnímu dešifrování i v případě, že heslo se nachází ve slovníku hesel. Další užitečné příkazy a optimalizace jsou uvedeny v příloze 5. V současné době jsou podporované pouze výše uvedené peněženky. Mobilní peněženky v tomto programu nejsou podporované.

4.6.3 Bitcoin Password

Posledním softwarem pro dešifrování je Bitcoin Password od společnosti Thegrideon. Software je dalším testovaným dešifrovacím nástrojem, který se ukázal velmi omezený v rychlosti i možnostech. Výhodou programu je grafické rozhraní pro méně zkušené uživatele. Nevýhodou je podpora peněženek pouze ve formátu *.dat (primárně Bitcoin Core/Knots). Při testování také nebylo ani zdaleka dosaženo výrobcem udávaného výpočetního výkonu (poštu hesel za vteřinu). Jednalo se o trial verzi, která je dle výrobce omezena pouze dobou dešifrování, nikoliv rychlostí. Tento software je navíc proti oběma výše uvedeným placený (btcrecover licence GNU a HashCat jsou opensource).

5. Závěr

Cílem mé práce bylo prozkoumat možnosti analýzy současných kryptoměn se zaměřením na bitcoin.

V první polovině práce byla popsána historie kryptoměn, teoretické principy fungování, stavební bloky, možnosti získání kryptoměny bitcoin a legislativa týkající se kryptoměn.

V druhé polovině práce byly prozkoumány možnosti ukládání kryptoměny bitcoin, nalezení a zabavení kryptoměn na zařízeních. Protože se kryptoměna bitcoin uchovává v bitcoinových peněženkách, byla zaměřena hlavní pozornost právě na vybrané zástupce peněženek. Zkoumány byly všechny druhy dostupných bitcoinových peněženek. Výzkum byl proveden u papírových, webových, hardwarových a softwarových peněženek. U softwarových peněženek byly použity ke zkoumání peněženky pro počítače – konkrétně pro operační systém Windows a mobilní pro operační systém Android. U webových a softwarových peněženek nebylo možné prozkoumat všechny dostupné peněženky z důvodu velkého množství dostupných peněženek. Existuje také značné množství manuálů pro vytvoření vlastní peněženky s minimem znalostí. Takové peněženky nebyly předmětem zkoumání, protože se jedná o kopie využívající stejné principy, jako prozkoumané peněženky pouze na nižší úrovni. Vybral jsem tedy takové peněženky, které nejlépe reprezentují danou skupinu a byly uvedeny jako doporučené na hlavní webové stránce Bitcoinu: bitcoin.org.

Po výběru peněženek byly vybrány vhodné softwarové nástroje pro automatizované zkoumání výpočetní techniky. Z dostupných nástrojů byly použity Belkasoft Evidence Center Ultimate, Magnet Axiom Process, Magnet Internet Evidence Finder. Jednal jsem o zapůjčení softwaru i se společnostmi EnCase, Eliptic a CypherTrace. Bohužel ani jedna z těchto společností nebyla ochotná poskytnout bezplatně svůj software k vyzkoušení. Dále byly použity softwarové nástroje od společností Cellebrite UFED 4 PC a XRY pro vytvoření bitových kopií mobilních telefonů.

Softwary pro vytvoření kopií telefonů neměly s tímto úkolem u vybraných telefonů žádný problém a mohlo být přistoupeno k analýze pořízených dat. Úspěšnost vytvoření fyzické kopie telefonu se může lišit podle verzí systému, ale i podle jednotlivých modelů daného výrobce. Samotnou kapitolou jsou telefony s operačním systémem Apple iOS, které jsou velmi dobře zabezpečené a zkoumání tak je možné pouze u starších zařízení.

Po otestování softwarových nástrojů na vybraných peněženkách se ukázala výrobci slibovaná automatická detekce bitcoinů velmi omezenou. Software od společnosti Belkasoft detekuje korektně pouze peněženku Armory a mobilní peněženku Bitcoin Wallet. U Bitcoin Core/Knots detekuje adresy i privátní klíče, ale seznam nalezených adres neobsahoval aktivní adresy používané peněženkou. Obě softwarová řešení od společnosti Magnet měly totožné detekční schopnosti v případě kryptoměny bitcoin. Oba softwary

byly schopné detekovat pouze peněženku Bitcoin Core. Na rozdíl od softwaru společnosti Belkasoft byla detekce korektní a zobrazeny byly pouze aktivní adresy. U ostatních peněženek, jak pro počítač, tak pro mobilní telefony, bylo nutné provést analýzu umístění souborů a možnosti odhalení adres ručně.

Po ruční analýze souborů peněženek bylo zjištěno, že soubory peněženek jsou šifrované. Některé peněženky nešifrují ve výchozím stavu, jiné šifrování používají vždy. Bylo tedy nutné se zaměřit na možnosti dešifrování. K dešifrování byly použity dva nástroje btcrecover a hashcat, které jsou schopné nalézt heslo do peněženky při správném nastavení. Testování těchto dešifrovacích nástrojů odhalilo omezení výkonosti. Z toho důvodu byl navrhnut postup slovníkového dešifrování, místo použití hrubé síly, i když jsou podporované obě možnosti. Další pro analýzu výhodnou vlastností peněženek jsou odkryté veřejné adresy. Je tak možné zjistit, jestli se na adresách obsažených v peněženkách nacházejí bitcoiny a jestli je tedy dešifrování vůbec potřebné a finančně rentabilní.

Výsledkem této práce je ucelený souhrn informací o možnostech zkoumání bitcoinových peněženek. Na vybraných peněženkách jsou popsány vhodné postupy, možnosti zajištění nalezené kryptoměny a rozdílné přístupy ke zkoumání jednotlivých peněženek. Pro rozdílnost peněženek se možnosti zkoumání odlišují a to, co je možné u jedné peněženky, nemusí být proveditelné u jiné, protože peněženky sice používají stejné principy, ale mohou tyto principy implementovat velmi rozdílnými směry.

6. Literatura

1 DAI, Wei. B-money [online]. [cit. 2018-03-07]. Dostupné z: http://www.weidai.com/bmoney.txt

2 PECK, Morgen E. Bitcoin: The Cryptoanarchists' Answer to Cash. Spectrum.ieee [online]. 2012 [cit. 2018-03-07]. Dostupné z: https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0

3 BLACK, Adam. Hashcash - A Denial of Service Counter-Measure. Hash Cash [online]. 2002 [cit. 2018-03-07]. Dostupné z: http://www.hashcash.org/papers/hashcash.pdf

4 VON AHN, Luis. ReCAPTCHA: Human-Based Character Recognition via Web Security Measures. Science [online]. [cit. 2018-03-08]. Dostupné z: http://www.cs.cmu.edu/~biglou/reCAPTCHA_Science.pdf

5 CoinMap [online]. [cit. 2018-03-28]. Dostupné z: http://www.coinmap.org/#/map/49.71915220/14.79858398/9

6 ICANN WHOIS. ICANN [online]. [cit. 2018-03-28]. Dostupné z: https://whois.icann.org/en/lookup?name=bitcoin.org

7 NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. 2009, 9 [cit. 2018-03-28]. Dostupné z: https://bitcoin.org/bitcoin.pdf

8 Blockchain [online]. [cit. 2018-03-28]. Dostupné z: https://Blockchain.info/block-index/14849

9 DAVIS, Joshua. The Crypto-Currency. The New Yorker [online]. 2011 [cit. 2018-03-28]. Dostupné z: https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

10 REDMAN, Jamie. Bitcoin's Quirky Genesis Block Turns Eight Years Old Today. Bitcoin.com [online]. 2017 [cit. 2018-03-28]. Dostupné z: https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/

11 MCMILLAN, Robert. WHO OWNS THE WORLD'S BIGGEST BITCOIN WALLET? THE FBI. Wired [online]. 2013 [cit. 2018-03-28]. Dostupné z: https://www.wired.com/2013/12/fbi-wallet/

12 GERVAIS, Arthur, Ghassan O. KARAME, Srdjan CAPKUN a Vedran CAPKUN. Is Bitcoin a Decentralized Currency?. ETH Zurich [online]. 2014 [cit. 2018-03-28]. Dostupné z: http://www.syssec.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/publications/pub2014/spmagazine_gervais.pdf

13 Bitcoin Foundation [online]. [cit. 2018-03-28]. Dostupné z: https://bitcoinfoundation.org/about/

14 WOLLA, Scott. Functions of Money - The Economic Lowdown [online]. [cit. 2018-03-28]. Dostupné z: https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-9-functions-of-money

15 KHARIF, Olga. The Bitcoin Whales: 1,000 People Who Own 40 Percent of the Market [online]. 2017 [cit. 2018-03-28]. Dostupné z: https://www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market

16 Bitcoin (USD) Price. CoinDesk [online]. [cit. 2018-03-28]. Dostupné z: https://www.coindesk.com/price/

17 Block. Bitcoin Wiki [online]. [cit. 2018-03-28]. Dostupné z: https://en.bitcoin.it/wiki/Block

18 Transaction and block size. TradeBlock [online]. [cit. 2018-03-28]. Dostupné z: https://tradeblock.com/bitcoin/historical/1w-f-tsize_per_avg-01101

19 NARANG, Narendra N. Uncover Blockchain Opportunities [online]. [cit. 2018-03-28]. Dostupné z: https://online.ptc.org/assets/uploads/papers/ptc18/WS_RedHat_Narang_Narendra.pdf

20 Block Headers. Bitcoin [online]. [cit. 2018-03-28]. Dostupné z: https://bitcoin.org/en/developer-reference#block-headers

21 PACIA, Chris. Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics. *Escape Velocity* [online]. [cit. 2018-04-06]. Dostupné z: https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/

22 PACIA, Chris. *Hash-Chain* [online]. [cit. 2018-04-06]. Dostupné z: https://chrispacia.files.wordpress.com/2013/09/hash-chain.jpg

23 *Journal of cryptology*. Springer, 1991, **1991**(3). ISSN 0933-2790.

24 CHUMBLEY, Alex, Karleigh MOORE a Jimin KHIM. Merkle Tree. *Brilliant* [online]. [cit. 2018-04-06]. Dostupné z: https://brilliant.org/wiki/merkle-tree/

25 SHAAN, Ray. Merkle Trees. *HACKERNOON* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://hackernoon.com/merkle-trees-181cb4bc30b4

26 CLIFTON, Marc. Understanding Merkle Trees - Why use them, who uses them, and how to use them. *Code Project* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://www.codeproject.com/Articles/1176140/Understanding-Merkle-Trees-Why-use-them-who-uses-t

27 Block timestamp. *Bitcoin Wiki* [online]. 2016 [cit. 2018-04-06]. Dostupné z: https://en.bitcoin.it/wiki/Block_timestamp

28 MATĚJ, Pavel. *Problémy virtuální měny bitcoin*. Praha, 2015. Bakalářská práce. Vysoká škola ekonomická v Praze.

29 WALKER, Greg. Difficulty. *Learn me a bitcoin* [online]. 2015 [cit. 2018-04-06]. Dostupné z: http://learnmeabitcoin.com/guide/difficulty

30 Target. *Bitcoin Wiki* [online]. 2016 [cit. 2018-04-06]. Dostupné z: https://en.bitcoin.it/wiki/Target

31 Proof of Work. *Bitcoin Wiki* [online]. 2016 [cit. 2018-04-06]. Dostupné z: https://en.bitcoin.it/wiki/Proof_of_work

32 TradeBlock - Historical data. In: *TradeBlock* [online]. [cit. 2018-04-06]. Dostupné z: https://tradeblock.com/bitcoin/historical/1w-f-tsize_per_avg-01101

33 VERMEULEN, Jan. Bitcoin and Ethereum vs Visa and PayPal – Transactions per second. *Mybroadband* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html

34 Bitcoin Confirmations. *Buy Bitcoin Worldwide* [online]. [cit. 2018-04-06]. Dostupné z: https://www.buybitcoinworldwide.com/confirmations/

35 Predicting Bitcoin fees for transactions. *Earn* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://bitcoinfees.earn.com/

36 Softfork. *Bitcoin Wiki* [online]. [cit. 2018-04-06]. Dostupné z: https://en.bitcoin.it/wiki/Softfork

37 RADMAN, Jamie. A Simple Guide to What Bitcoin Forks Are and Why They Happen. *Bitcoin News* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://news.bitcoin.com/a-guide-to-what-a-bitcoin-fork-is-and-why-they-happen/

38 ISFELD, Kris. Bitcoin XT. *Investopedia* [online]. [cit. 2018-04-06]. Dostupné z: https://www.investopedia.com/terms/b/bitcoin-xt.asp

39 JP. Bitcoin classic končí, vyjadřuje podporu bitcoinu cash. *A1 Finance* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://a1finance.cz/investice/forex/digitalni-meny/bitcoin/bitcoin-classic-konci-vyjadruje-podporu-bitcoinu-cash

40 MADEIRA, Antonio. What is Bitcoin Unlimited. *CryptoCompare* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://www.cryptocompare.com/coins/guides/what-is-bitcoin-unlimited/

41 SPINNER, Ron. Bitcoin Cash. *Investopedia* [online]. [cit. 2018-04-06]. Dostupné z: https://www.investopedia.com/terms/b/bitcoin-cash.asp

42 Bitcoin Gold (BTG). *Bitcoin Gold* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://bitcoingold.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf

43 RAY, Shaan. What is Proof of Stake?. *HackerNoon* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://hackernoon.com/what-is-proof-of-stake-8e0433018256

44 BARANA, Paul. On Distributed Communications Series. *RAND* [online]. [cit. 2018-04-06]. Dostupné z: https://www.rand.org/pubs/research_memoranda/RM3420/RM3420-chapter1.html

45 MCGEW, Matt. The Disadvantages of a Centralized Network Scheme. *It Still Works* [online]. [cit. 2018-04-06]. Dostupné z: https://itstillworks.com/disadvantages-centralized-network-scheme-12213044.html

46 MCDUNNIGAN, Micah. Advantages & Disadvantages of Distributed Systems. *Techwalla* [online]. [cit. 2018-04-06]. Dostupné z: https://www.techwalla.com/articles/advantages-disadvantages-of-distributed-systems

47 PY, Frederic. What are the pros and cons between a centralized system and a decentralized system in terms of ownership and management?. *Quora* [online]. 2014 [cit. 2018-04-06]. Dostupné z: https://www.quora.com/What-are-the-pros-and-cons-between-a-centralized-system-and-a-decentralized-system-in-terms-of-ownership-and-management

48 Bitcoin mining difficulty. In: *Data.bitcoinity.org* [online]. [cit. 2018-04-06]. Dostupné z: https://data.bitcoinity.org/bitcoin/difficulty/2y?t=l

49 Hashrate Distribution. In: *Blockchain* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://Blockchain.info/pools

50 HOMAKOV, Egor. Stop. Calling. Bitcoin. Decentralized. *Medium* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27

51 51% Attack. *Learn Cryptography* [online]. [cit. 2018-04-06]. Dostupné z: https://learncryptography.com/cryptocurrency/51-attack

52 SILVER, Caleb. 51% Attack. *Investopedia* [online]. 2016 [cit. 2018-04-06]. Dostupné z: https://www.investopedia.com/terms/1/51-attack.asp

53 HOMAKOV, Egor. How to Destroy Bitcoin with 51%. *Meduim* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://medium.com/@homakov/how-to-destroy-bitcoin-with-51-pocked-guide-for-governments-83d9bdf2ef6b

54 EYAL, Ittay a Emin SIRER. Majority is not Enough: Bitcoin Mining is Vulnerable. *Cornell University* [online]. [cit. 2018-04-06]. Dostupné z: https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf

55 BOVERMAN, Alex. Timejacking & Bitcoin. *Culubas* [online]. 2011 [cit. 2018-04-06]. Dostupné z: http://culubas.blogspot.cz/2011/05/timejacking-bitcoin_802.html

56 Top 100 Cryptocurrencies by Market Capitalization. In: *Cryptocurrency Market Capitalizations* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://coinmarketcap.com/

57 ROSIC, Ameer. What is Ethereum? A Step-by-Step Beginners Guide. *Blockgeek* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://blockgeeks.com/guides/ethereum/

58 LEWIS, Antony. Ripple Explained: Medieval Banking with a Digital Twist. *CoinDesk* [online]. 2014 [cit. 2018-04-06]. Dostupné z: https://www.coindesk.com/ripple-medieval-banking-digital-twist/

59 ROSIC, Ameer. What is Litecoin? A Basic Beginners Guide. *Blockgeek* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://blockgeeks.com/guides/litecoin/

60 ISFELD, Kris. Bitcoin Wallet. *Investopedia* [online]. [cit. 2018-04-06]. Dostupné z: https://www.investopedia.com/terms/b/bitcoin-wallet.asp

61 Hash Rate. In: *Blockchain* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://Blockchain.info/charts/hash-rate?timespan=all

62 Bitcoin Mining Hardware Guide. *Bitcoin Mining* [online]. [cit. 2018-04-06]. Dostupné z: https://www.bitcoinmining.com/bitcoin-mining-hardware/

63 AGRAWAL, Harsh. How To Buy Bitcoins With Cash In Any Country. *Coinsutra* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://coinsutra.com/buy-bitcoins-cash/

64 KHATWANI, Sudhir. Best Ways To Buy Bitcoins Without ID. *Coinsutra* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://coinsutra.com/best-ways-buy-bitcoins-without-id-buy-bitcoins-anonymously/

65 ČESKÁ REPUBLIKA. Předpis 368/2016 Sb. In: *Sbírka zákonů a mez. smluv*. Praha: Parlament České republiky, 2016, ročník 2016, částka 147, 368/2016. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=368&r=2016

66 VanityGen Sample Address. In: *Blockchain* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://Blockchain.info/address/1BoatSLRHtKNngkdXEeobR76b53LETtpyT

67 GOLDFEDER, Steven, Harry KALODNER, Dillon REISMAN a Arvind NARAYANAN. When the cookie meets the Blockchain: Privacy risks of web payments via cryptocurrencies. *Cornell University Library* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://arxiv.org/pdf/1708.04748.pdf

68 KHATWANI, Sudhir. 6 Ways To Guarantee Anonymity When Making Bitcoin Transactions. *Coinsutra* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://coinsutra.com/anonymous-bitcoin-transactions/

69 Obchodování s bitcoiny. *Česká národní banka* [online]. 2014 [cit. 2018-04-06]. Dostupné z: https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/stanoviska_a_odpovedi/pdf/obchodovani_s_bitcoiny.pdf

70 ALI. Bitcoin a jiné virtuální měny z pohledu práva. *CFOworld* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://cfoworld.cz/legislativa/bitcoin-z-pohledu-prava-4199

71 MATOCHA, JUDr. Jakub. Virtuální měny a trestní právo. *Pravní prostor* [online]. 2016 [cit. 2018-04-06]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/virtualni-meny-a-trestni-pravo

72 REDMAN, Jamie. Bitcoin Illegal in Nepal? Police Arrest Seven Individuals for Trading Operations. *Bitcoin.com* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://news.bitcoin.com/bitcoin-illegal-in-nepal-police-arrest-seven-individuals-for-trading-operations/

73 ACHESON, Noelle. Is Bitcoin Legal?. *Coindesk* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://www.coindesk.com/information/is-bitcoin-legal/

74 HELMS, Kevin. Russia Finalizes Federal Law on Cryptocurrency Regulation. *Bitcoin.com* [online]. [cit. 2018-04-06]. Dostupné z: https://news.bitcoin.com/russia-finalizes-federal-law-cryptocurrency-regulation/

75 BLOOMBERG. This Is How China Is Stifling Bitcoin and Cryptocurrencies. *Fortune* [online]. 2018 [cit. 2018-04-06]. Dostupné z: http://fortune.com/2018/01/17/china-bitcoin-cryptocurrency-crackdown/

76 REESE, Frederick. Bitcoin Regulation by State. *Bitcoin Market Journal* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://www.bitcoinmarketjournal.com/bitcoin-state-regulations/

77 Bip 39 Wordlists. *Github.com* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://github.com/bitcoin/bips/blob/master/bip-0039/bip-0039-wordlists.md

78 KHATWANI, Sudhir. What Is Mnemonic Phrase & Mnemonic Passphrase?. *Coinsutra* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://coinsutra.com/mnemonic-passphrase/

79 RUSSELL, Craig. Ledger Nano S—The Complete Guide. *Medium* [online]. 2017 [cit. 2018-04-06]. Dostupné z: https://medium.com/@trionkidnapper/ledger-nano-s-the-complete-guide-91d6b397f5cc

80 TUWINER, Jordan. Leger Nano S a recovery sheet. In: *Buy Bitcoin Worldwide* [online]. [cit. 2018-04-06]. Dostupné z: https://www.buybitcoinworldwide.com/wallets/ledger-nano-s/

81 DALE, Oliver. Trezor vs. Ledger Review:. *Blockonomi* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://blockonomi.com/trezor-vs-ledger/

82 TREZOR. In: *Penny WISE* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://pennywise.sg/product/trezor

83 PEREZ, Yessi Bello. KeepKey Launches New Bitcoin Hardware Wallet. In: *Coindesk* [online]. 2015 [cit. 2018-04-06]. Dostupné z: https://www.coindesk.com/keepkey-launches-new-bitcoin-hardware-wallet/

84 Bitaddress.org. In: *Bitaddress.org* [online]. 2018 [cit. 2018-04-06]. Dostupné z: https://www.bitaddress.org

85 BECKER, Canton. BIP38 password-encrypted paper wallets. *Bitcoinpaperwallet.com* [online]. 2014 [cit. 2018-04-06]. Dostupné z: https://bitcoinpaperwallet.com/bip38-password-encrypted-wallets/

86 Mobile Operating System Market Share Worldwide - March 2018. *Statcounter* [online]. [cit. 2018-04-06]. Dostupné z: http://gs.statcounter.com/os-market-share/mobile/worldwide

7. Seznam obrázků

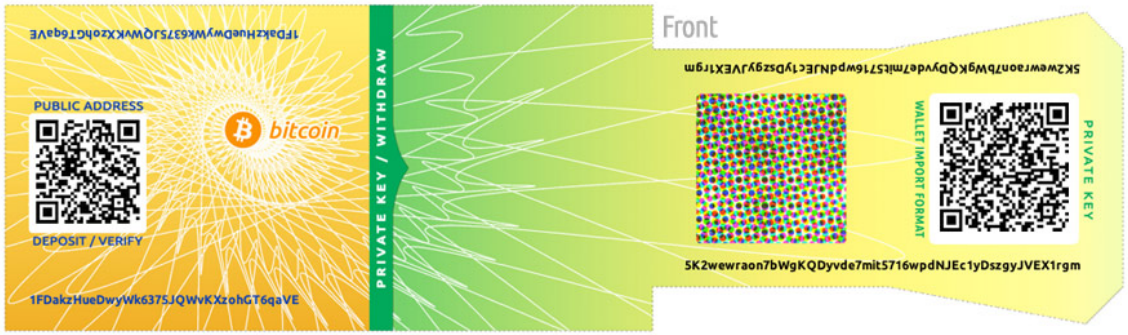
8. Seznam tabulek

9. Přílohy

Příloha 1

Ukázky dalších papírových peněženek

bitcoinpaperwallet.com



bitaddress.org

Papírová peněženka ve formátu csv – index, adresa, soukromý klíč

1,"129BEKfwKcKxWBBRDHU9gAfNVUdzf1mezn","L4Zpx2w4KPKaaKRzPoDMJyHWBPRYLX8zjX9YLdc9k5hmhAqNSNT5"
2,"1Dgv9TJXRLKFAWPP78EgxsCo4Fmd1X1wzm","L2XJAT8FnY4LJU24kvFn1yPhCBG8VRBAZ5TZ9o5ym5omsHPfQKbT"
3,"1PcYtX44TuLHFrEoyD83JG3274xWV43FBP","L2WSAoSZdKmLcfxWtYUJgeV5j6BrC5uTkaH9yTFsab212QcuBYGp"

Rozdělená papírová peněženka

Příloha 2

SMS příkazy pro peněženku Coinapult

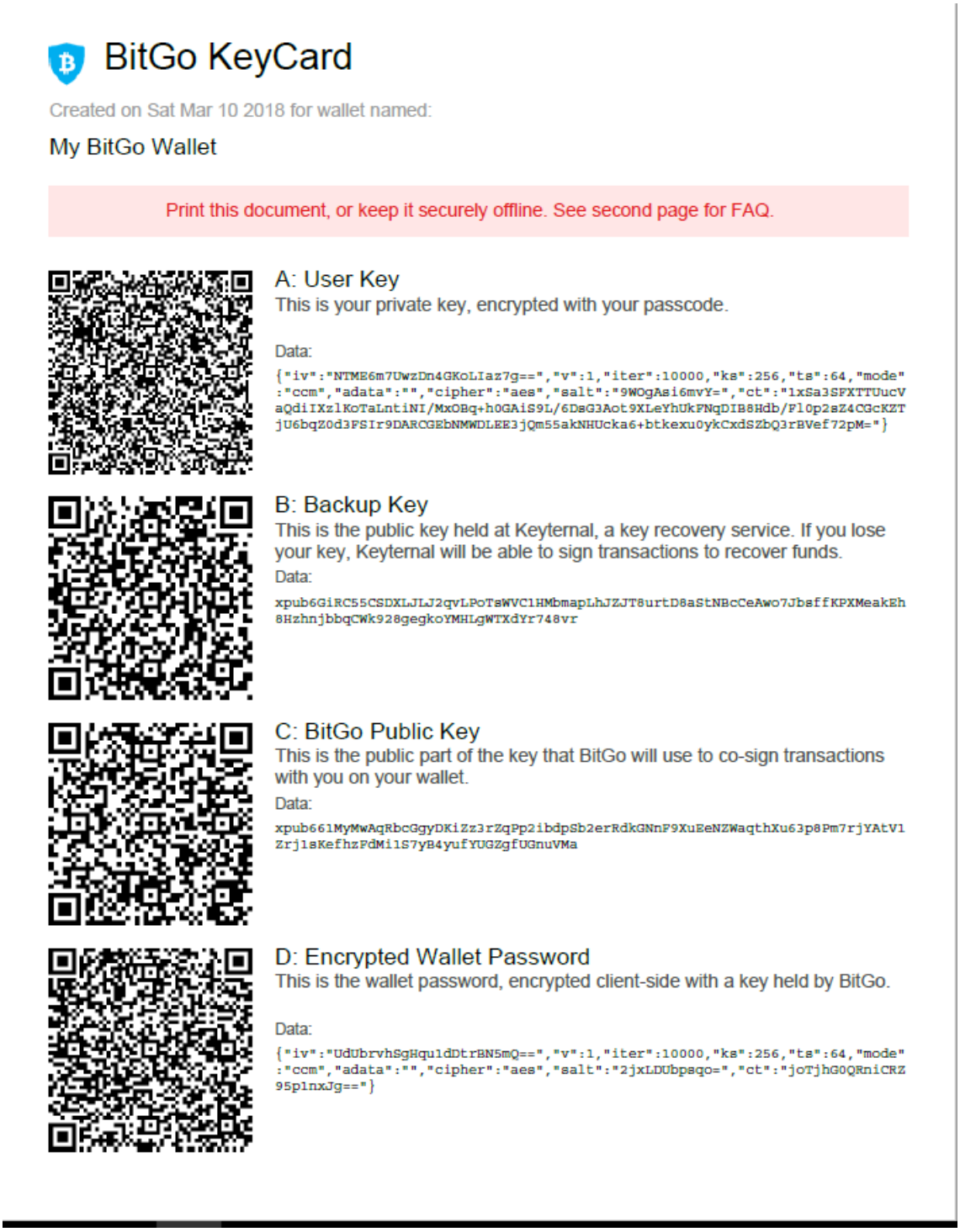
Send commands to one of the following numbers

Canada (Vancouver, BC)	+1 778-654-6270
UK	+44 20 3322 2126

List of Commands

Command	Aliases	Description	Arguments	Example	Confirmation required?
help me	?	Print the help menu		help me	No
bal		Return your balance. If the bitcoin value of all balances is desired, you can specify a second parameter to indicate whether the balance should shown be in bitcoins (1) or not (0)	['both' | 'confirmed' | 'unconfirmed'] [0 | 1]	bal	No
address	addr	Get a new bitcoin address		address	No
history	hist, txs	Returns your 5 most recent transactions		history	No
rate	rates, price	Returns the Coinapult rate for the specified currency against BTC	[amount in bitcoins] ['USD' | 'EUR' | 'GBP' | 'XAU' | 'XAG']	rate 1.42 XAU	No
yes		Confirm a command	code	yes abc012	No
send		Send bitcoins to an email address, bitcoin address, or phone number	address amount	send someone@example.com 0.42	Yes
invoice		Send an invoice to an email address or phone number.	address amount currency	invoice someone@example.com 0.25 BTC	Yes

KeyCard - peněženky BitGo



BitGo KeyCard

Created on Sat Mar 10 2018 for wallet named:

My BitGo Wallet

Print this document, or keep it securely offline. See second page for FAQ.

A: User Key

This is your private key, encrypted with your passcode.

Data:

{"iv":"NTME6m7UwzDn4GKoLIaz7g==","v":1,"iter":10000,"ks":256,"ts":64,"mode":"ccm","adata":"","cipher":"aes","salt":"9WOgAsi6mvY=","ct":"lxSa3SFXTTUucVaQdiIXzlKoTaLntiNI/MxOBq+h0GAiS9L/6DsG3Aot9XLeYhUkFNqDIB8Hdb/Fl0p2sZ4CGcKZTjU6bqZ0d3PSIr9DARCGEbNMWDLEE3jQm55akNHUcka6+btkexu0ykCxdSZbQ3rBVef72pM="}

B: Backup Key

This is the public key held at Keyternal, a key recovery service. If you lose your key, Keyternal will be able to sign transactions to recover funds.

Data:

xpub6GiRC55CSDXLJLJ2qvLPoTsWVC1HMbmapLhJZJT8urtD8aStNBcCeAwo7JbsffKPXMeakEh8HzhnjbbqCWk928gegkoYMHLgWTXdYr748vr

C: BitGo Public Key

This is the public part of the key that BitGo will use to co-sign transactions with you on your wallet.

Data:

xpub661MyMwAqRbcGgyDKiZz3rZqPp2ibdpSb2erRdkGNnP9XuEeNZWaqthXu63p8Pm7rjYAtV1ZrjlsKefhzPdMi1S7yB4yufYUGZgfUGnuVMa

D: Encrypted Wallet Password

This is the wallet password, encrypted client-side with a key held by BitGo.

Data:

{"iv":"UdUbrvhSgHquldDtrBN5mQ==","v":1,"iter":10000,"ks":256,"ts":64,"mode":"ccm","adata":"","cipher":"aes","salt":"2jxLDUbpsqo=","ct":"joTjhG0QRniCRZ95p1nxJg=="}

Příloha 3

Papírová záloha peněženky Armory a privátních klíčů

ARMORY

Paper Backup for Armory Wallet

Wallet Version:	1.35c
Wallet ID:	2ixd98wzf
Wallet Name:	Primary Wallet
Backup Type:	Single-Sheet (Unencrypted)

WARNING: Anyone who has access to this page has access to all the bitcoins in this wallet! Please keep this page in a safe place.

The following two lines backup all addresses *ever generated* by this wallet (previous and future). This can be used to recover your wallet if you forget your passphrase or suffer hardware failure and lose your wallet files.

Root Key:	whks ttjh snni dddw uefh tiii kgif anrf ngag karr okfo isso jddg jwnn rikh gtwg hash dkuu

The following QR code is for convenience only. It contains the exact same data as the two lines above. If you copy this backup by hand, you can safely ignore this QR code.

```
Created:       2018-Mar-18 09:50pm
Wallet ID:     2ixd98wzf
Wallet Name:   Primary Wallet

--------------------------------------------------------------------------------
The following is the same information contained on your paper backup.
All NON-imported addresses in your wallet are backed up by this data.

Root Key:      whks ttjh snni dddw uefh tiii kgif anrf ngag
               karr okfo isso jddg jwnn rikh gtwg hash dkuu
--------------------------------------------------------------------------------

1Jwug2BiXtw3RN4SD2DGyR2rnkMs39iEzd
   PrivBase58: 5KNXyi sHpH6L PtRnnM cdeKFh ZK19ST FLgoim LacSfW NFSZbr dSC
   PrivHexBE : cceb 6dc7 1ee0 28e8 e469 45f6 6f91 6a93 d18a f4f5 08a4 1e72 0119 e8d9 9bc4 06a9
1Jq7Z2Sbm4eH2NMRnTLoyXGNTM94fp3xNk
   PrivBase58: 5JMwyq PyAjfg zvDM4e CiYje7 Dd5MPp qxDjXP sv6L8F ANA93f zBG
   PrivHexBE : 47e4 7f78 04df f8f9 69bb c478 7158 a02f 390d e888 e812 011f 7d71 7076 31ae 02e5
1AVSnMbW4CW7wKRddMzSHjypBRUBhCgtCt
   PrivBase58: 5JC3Xw cbLkiz A8RLBx hzQDqP 2eancy Dm1Sd2 v39MWz ZLpw75 aBo
   PrivHexBE : 3167 5ceb ccd6 b5b9 4e37 dd47 c53e 7cc0 406a 2782 f0cb ac96 d34b 881f 1b8a c341
1KWGulsSDdeV8vRktRGUptYXx3qxc4CtZB
   PrivBase58: 5JfUAJ FYJBRg zu3UUq k3GRG8 nQioRT 3DDkvp uXTKka tz49qF nWN
   PrivHexBE : 6fac b74a 85d1 354a 2f13 6e21 4ab2 16b0 d40a 82d6 c451 6afe ee44 77ce d48d 70d6
```

Papírová záloha peněženky Armor opatřená SecurePrintem

ARMORY

Paper Backup for Armory Wallet

CRITICAL: This backup will not work without the SecurePrint™ code displayed on the screen during printing. Copy it here in ink:

Code: fwMDUJHE3PX.

Wallet Version: 1.35c
Wallet ID: 34dubio5R
Wallet Name: Primary Wallet
Backup Type: Single-Sheet (SecurePrint™)

WARNING: Anyone who has access to this page has access to all the bitcoins in this wallet! Please keep this page in a safe place.

The following two lines backup all addresses *ever generated* by this wallet (previous and future). This can be used to recover your wallet if you forget your passphrase or suffer hardware failure and lose your wallet files.

Root Key:	jfug ttdj oeka idgs jkti tsiw sokf einw eguw
	aoft duhj asts doeh jdrg akij fsui rkod gjdt

The following QR code is for convenience only. It contains the exact same data as the two lines above. If you copy this backup by hand, you can safely ignore this QR code.

Fragmented backup peněženky Armory

ARMORY

Paper Backup for Armory Wallet

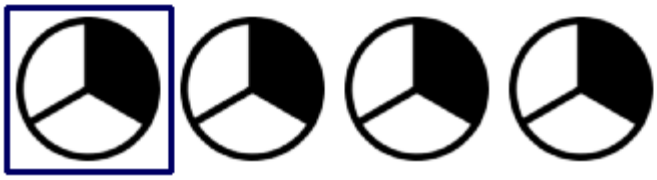
Wallet Version:	1.35c
Wallet ID:	34dubio5R
Wallet Name:	Primary Wallet
Backup Type:	Fragmented Backup (3-of-4) (Unencrypted)
Fragment:	**36TUPE7-#1**

Any subset of **3** fragments with this ID (**36TUPE7**) are sufficient to recover all the coins contained in this wallet. To optimize the physical security of your wallet, please store the fragments in different locations.

The following is fragment **#1** for this wallet.

ID:	0301 3ae7 0eb8 9fd1
F1:	nrjg okdi dhew kjau teon onrj tato wthh uwrt
F2:	jggg hruu tekr soes siwu tfne adss uist diod

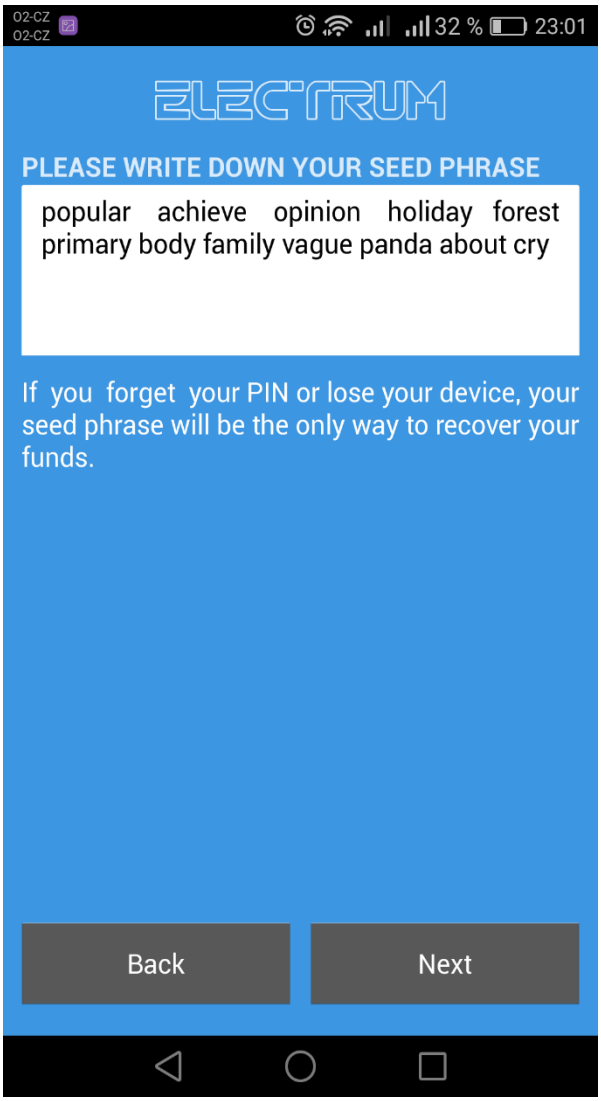
The following QR code is for convenience only. It contains the exact same data as the three lines above. If you copy this backup by hand, you can safely ignore this QR code.

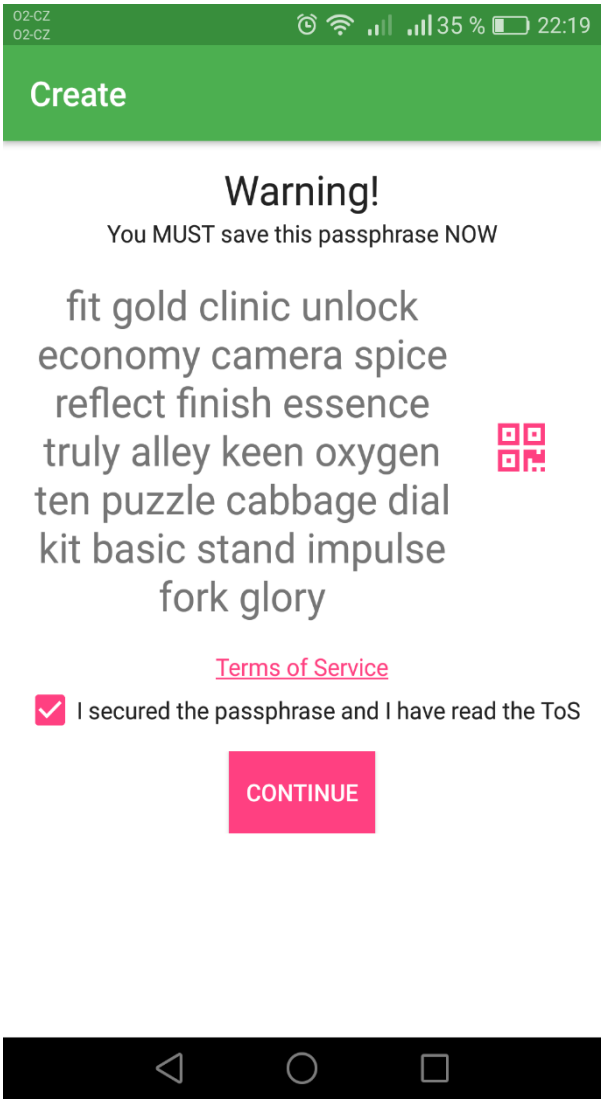


#1

Příloha 4

Ukázka uloženého obrázku obnovovací fráze mobilních peněženek Electrum (vlevo) a GreenAddress (vpravo).





Příloha 5

Program btc recovery

Dostupný na adrese: https://github.com/gurnec/btcrecover

Potřebný software pro správnou funkci:

1. Python 2.7 (novější není podporován)
2. Microsoft Visual C++ Compiler for Python 2.7
3. Microsoft Visual C++
4. Pywin32
5. PyCrypto2.6
6. Libsodium
7. PyOpenCL

Software je vhodné instalovat ve výše uvedeném pořadí. Vše kromě posledních dvou má svůj vlastní instalátor a instaluje se tedy pouze poklepáním na exe soubor. Knihovnu libsodium je nutné nakopírovat do složky s pythonem, po rozbalení složky s libsodium vybereme libsodium-1.0.13-msvc\x64\Release\v141\dynamic a soubor libsodium.dll nakopírujme do kořenového adresáře Pythonu (obvykle C:\Python27). Druhým souborem ke zkopírování je PyOpenCL….whl, které je potřeba zkopírovat do C:\Python27\Scripts. Po instalaci a nakopírování výše uvedených programů otevřeme příkazový řádek a pomocí příkazu cd přejdeme do složky C:\Python27\Scripts. Několika jednoduchými příkazy doinstalujeme chybějící knihovny:

1. pip install Pylibscrypt
2. pip install Coincurve==5.2.0 pysha3
3. pip install Protobuf
4. pip install pyopencl-2018.1.1+cl12-cp27-cp27m-win_amd64.whl - název se bude lišit podle stažené verze

Nyní máme vše potřebné pro běh btc recovery a můžeme se přesunout k ostatním příkazům.

Otestování výpočetního výkonu – pro testování je potřeba soubor peněženky:

```
btcrecover.py --wallet bcp.dat --performance --no-dupchecks
```

Tento příkaz je velmi důležitý pro dešifrování na grafické kartě. Pro optimalizace výpočtu je nutné nastavit dvě další hodnoty a tím jsou --local-ws a --global-ws. Oba přepínače chceme nastavit na co nejvyšší hodnotu. U --local-ws nám automaticky

program sdělí maximální hodnotu, pokud jí překročíme. U --global-ws je nutné postupovat pokus omyl a musí se jednat o násobky --local-ws. Pro grafickou kartu AMD RX580 8GB bylo nejlepší nastavení 256 a 32768.

```
btcrecover.py --wallet bcp.dat --performance --enable-gpu
```

Po tomto nastavení se výpočetní výkon zvýšil ze 490 h/s na 1150 h/s. Další zvýšení --global-ws již nepřineslo výrazné zlepšení, do 20 h/s. Příkaz tedy vypadá takto:

```
btcrecover.py --wallet bcp.dat --performance --enable-gpu --local-ws 256 --global-ws 32768 --no-dupcheck
```

Přepínač --no-dupcheck zabraňuje přetečení paměti a neočekávanému vypnutí systému. Pro reálné dešifrování pouze vyměníme --performance za --paswordlist. Kromě passwordlistu je možné použít i tokenlist. Příkaz tokenlist dělá kombinace ze vstupního souboru na rozdíl od passwordlistu, který zkouší jednotlivé řádky souboru. U tokenlistu můžeme nastavit délku sestavovaného hesla za pomoci přepínačů --token-min a -- token-max, kterými nastavíme minimální a maximální délku hesla pro omezení počtu možností. Bez tohoto nastavení je vytvářeno heslo maximální možné délky ze vstupní abecedy. Program dělá kombinace bez opakování, tzn. při vstupní abecedě abc nám vytvoří 15 kombinací o délce 1, 2 a 3 znaky. Nastavit je možné i kombinace s opakováním a to pomocí přepínače --typos # kde za # dosadíme číslo, kolikrát chceme daný znak opakovat. Spolu s tímto přepínačem je potřeba použít --typos-repeat, kterým programu sdělíme, že chceme znaky opakovat. Tento příkaz má omezení na vstupní abecedu, pokud se naše abeceda skládá z 3 znaků, zvolením čísla 4 se již víc hesel nevytvoří.

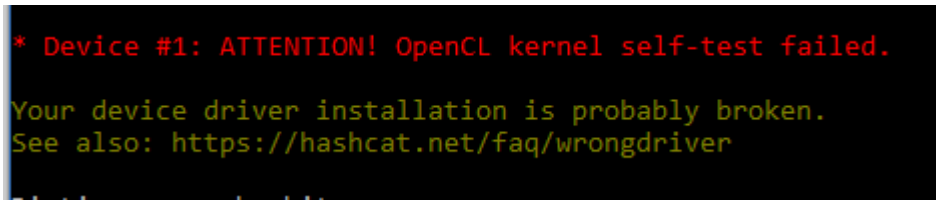
Pokud se vyhledání hesla podaří, dostaneme tento výpis:

```
C:\btcrecover-master>C:\python27\python btcrecover.py --passwordlist pass1.txt --wal
Starting btcrecover 0.17.10 on Python 2.7.14 64-bit, 16-bit unicodes, 32-bit ints
Wallet difficulty: 202,203 SHA-512 iterations
Using 16 worker threads
0 of 1 [------------------------------------------] 0:00:00, ETA:  --:--:--
Password found: 'jakub'
```

Program HashCat

Dostupný na adrese: https://hashcat.net/hashcat/

Program HashCat nepotřebuje všechny pomocné softwary jako v případě btc recovery. Pokud jsou nainstalované, je zajištěná naprostá funkčnost. HashCat je možné používat pouze přes příkazovou řádku. PowerShell konzole není podporovaná. Před samotným dešifrováním je vhodné udělat testovací hash, u kterého známe heslo. Lze použít ze stránek https://hashcat.net/wiki/doku.php?id=example_hashes. Otestování se provede stejně jako v případě dešifrování, jen si hash ze stránek zkopírujeme (11300 pro Bitcoin Core/Knots peněženku) do textového souboru a dáme ji na vstup. Do souboru s hesly vložíme uvedené heslo. V případě chybného ovladače grafické karty, který nepodporuje OpenCL, nemusí dojít k nalezení hesla i v případě, že ho daný slovník obsahuje. Indikace problému může vypadat takto:



Na rozdíl od btc recovery tento program neumí pracovat přímo se soubory peněženky, ale je potřeba vytvoření jejich hashe. To se provede za pomoci programu bitcoin2john.py pro peněženku Botcoin Core/Knots a electrum2john.py pro peněženku Electrum, který nám vytvoří hash pro hashcat. Tyto programy jsou dostupné na adrese: https://github.com/magnumripper/JohnTheRipper/tree/bleeding-jumbo/run.

Příkaze je následující:

```
C:\python27\python bitcoin2john.py wallet.dat > wallethash.txt
```

Předpokládám, že jsem ve složce se souborem bitcoin2john.py a soubor peněženky wallet.dat je také ve stejné složce. Tímto příkazem se nám vytvoří hash peněženky do souboru wallet.txt, který použijeme pro program HashCat. Vytvoření hashe peněženky Electrum provedeme totožně, pouze vyměníme bitcoin2johny za electrum2johny a soubor s peněženkou.

Prvním příkazem si otestujeme výkonost naší grafické karty k posouzení, jestli není optimálnější použít btc recovery.

```
hashcat64.exe -b -m 11300 --optimized-kernel-enable
```

Pro moji grafickou kartu je počet hashů za vteřinu skoro dvounásobný a to sice 2070 h/s. Tento program je tedy lépe optimalizovaný pro použití na GPU.

Dešifrování započneme tímto příkazem:

```
hashcat64.exe -m 11300 btc.txt pass.txt -O --force
```

-m 11300 - nám specifikuje hash, kterou chceme dešifrovat (16600 Electrum), btc.txt je soubor s hashí peněženky z předchozího kroku, pass.txt je soubor s naším slovníkem hesel, -O je zkratka pro --optimized-kernel-enable a --force slouží pro přeskakování chyb. Pokud se nám povede heslo najít, bude se nacházet v souboru hashcat.potfile (ve složce programu). Pro přehlednost je možné si zvolit výstupní soubor pomocí přepínače -o, například -o vysledek.txt. Lze specifikovat i celou cestu, tedy -o C:\test\vysledek.txt. Pro formát výstupního souboru je přepínač --outfile-format + číslo, ideální se jeví --outfile-format 2, který vypíše pouze heslo.

Pokud se heslo podaří nalézt, bude výpis příkazové řádky vypadat následovně:

```
Session..........: hashcat
Status...........: Cracked
Hash.Type........: Bitcoin/Litecoin wallet.dat
Hash.Target......: $bitcoin$96$7b9a6f7c5a3cdd78db2e7645eb29f9e8a78bb45...082c42
Time.Started.....: Sat Mar 17 20:43:23 2018 (0 secs)
Time.Estimated...: Sat Mar 17 20:43:23 2018 (0 secs)
Guess.Base.......: File (pass1.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:       12 H/s (0.11ms) @ Accel:128 Loops:64 Thr:1 Vec:2
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 6/6 (100.00%)
Rejected.........: 0/6 (0.00%)
Restore.Point....: 0/6 (0.00%)
Candidates.#1....: $HEX[6e766d31323309] -> $HEX[6a616b7562]
HWMon.Dev.#1.....: N/A
```

Tento program podporuje celou řadu hashí a je možné dešifrovat i jiné šifry. Také jsou zde možnosti kombinování „útoků“, které se nastavují přepínačem -a + číslo. Správné číslo najdeme po zadání hashcat64.exe --help. Nejsou nutné žádné ruční optimalizace jako v případě btc recovery. Pro co nejlepší výsledek může být potřeba přeinstalovat ovladač grafické karty dle stránek výrobce programu.

Dešifrování zálohy mobilní peněženky Bitcoin Wallet

Po nalezení pinu k peněžence Bitcoin Wallet je potřeba použít software decrypt_bitcoinj_seed. Tento software je dostupný na:

https://github.com/gurnec/decrypt_bitcoinj_seed.

Obsluha programu je velice jednoduchá. Jedinou podmínkou pro funkčnost je nainstalovaný Python, protože je vyžadován btcrecovery, který nám detekoval pin, budu předpokládat, že je již nainstalován. Před spuštěním programu je vhodné si nakopírovat soubor peněženky do složky s programem. Spuštění provedeme poklepáním na decrypt_bitcoinj_seed.pyw, otevře se nám dialogové okno pro zvolení naší peněženky. Po zvolení peněženky budeme vyzváni k zadání pinu. Pokud zadáme správný pin, dostaneme frázi pro obnovení v grafickém výstupu. V případě zadání špatného pinu dostaneme varování.