Ekonomická fakulta
Faculty of Economics
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Ekonomická Fakulta
Katedra aplikované matematiky a informatiky

Bakalářská práce

Bitcoin – historie, současnost a prognózy

Vypracovala: Petra Chvostová
Vedoucí práce: Ing. Petr Hanzal Ph.D.
České Budějovice 2018

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta ekonomická
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Petra CHVOSTOVÁ**
Osobní číslo: **E15491**
Studijní program: **B6209 Systémové inženýrství a informatika**
Studijní obor: **Ekonomická informatika**
Název tématu: **Bitcoin - historie, současnost a prognózy**
Zadávající katedra: **Katedra aplikované matematiky a informatiky**

Zásady pro vypracování:

Bitcoin je internetová platební síť a také v této síti používaná kryptoměna. Práce, která bude mít převážně kompilační charakter, zmapuje podrobně historii a současný stav problematiky. Zaměří se na podrobný popis filozofie, principů a výhod. Nakonec seznámí s úvahami o možnostech do budoucna.

Metodický postup:

1. Seznámit se se základními principy a východisky ("Bit gold" a "b-Money").
2. Prostudovat a zpracovat historické mezníky (od vzniku měny počínaje rokem 2009).
3. Od roku 2011 se o Bitcoinu pořádají mezinárodní konference. Prostudovat příslušné materiály, viz seznam zadané literatury.
4. Role "Bitcoin Foundation" starající se o infrastrukturu, sledování hrozeb a případné vylepšování protokolu, zajišťování konferencí a propagaci měny.
5. Současná praxe - praxe elektronického obchodování, ekonomické aspekty - výhody a nevýhody.
6. Úvahy o možnostech do budoucna.
7. Závěry.

Rozsah grafických prací: **dle potřeby**

Rozsah pracovní zprávy: **40 - 50 stran**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. **Bitcoin - history. Dostupné z WWW: <https://en.bitcoin.it/wiki/Category:History>.**
2. **České fórum o bitcoinu, dostupné z WWW: <https://bitcash.cz/>.**
3. **Davis, J.** *The Crypto-Currency* **[online]. The New Yorker, 10 October 2011. Dostupné z WWW: <http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency>.**
4. **Nakamoto, S. (2009.)** *Bitcoin: A Peer-to-Peer Electronic Cash System.* **Český překlad je dostupný z WWW: <http://jakfungujebitcoin.blogspot.cz/2015/06/slovo-vynalezce-bitcoinu_14.html>.**
5. **Materiály z mezinárodních konferencí o bitcoinu: New York, Praha (2011). Dostupné z WWW: <http://www.abclinuxu.cz/clanky/lehce-neformalni-reportaz-z-bitcoin-conference-2011>.**

Poznámka: k 1. 9. 2017 se měnil vedoucí práce

Vedoucí bakalářské práce: **Ing. Petr Hanzal, Ph.D.**
Katedra aplikované matematiky a informatiky

Datum zadání bakalářské práce: **16. ledna 2017**

Termín odevzdání bakalářské práce: **13. dubna 2018**

JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
EKONOMICKÁ FAKULTA
Studentská 13 (26)
370 05 České Budějovice

doc. Ing. Ladislav Rolínek, Ph.D.
děkan

RNDr. Jana Klicnarová, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 18. října 2017

Prohlašuji, že svoji bakalářskou práci jsem vypracovala samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

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

V Českých Budějovicích dne 9. 4. 2018

Petra Chvostová

Poděkování

Na tomto místě bych ráda poděkovala celé své rodině a přátelům, kteří mě podporovali po celou dobu mého studia. Dále bych chtěla poděkovat vedoucímu mé bakalářské práce Ing. Petru Hanzalovi Ph.D. za jeho cenné rady a připomínky. V neposlední řadě bych chtěla zmínit, že velké díky patří i původnímu vedoucímu, zesnulému doc. RNDr. Václavu Nýdlovi, CSc., díky kterému jsem se k tématu Bitcoin dopátrala.

OBSAH

1 Úvod ... 3

1.1 Cíle práce ... 4

2 Kryptoměny se zaměřením na Bitcoin ... 5

2.1 Původ Bitcoinu ... 6

2.1.1 B-money ... 6

2.1.2 Bit gold ... 7

2.2 Bitcoin ... 8

2.3 Satoshi Nakamoto ... 9

2.4 Historické milníky ... 10

2.5 Bitcoin Foundation ... 18

2.6 Mezinárodní konference ... 19

2.7 Princip fungování Bitcoinu ... 20

2.7.1 Peněženka a její adresa ... 20

2.7.2 Transakce ... 22

2.7.3 Těžba a Blockchain ... 24

2.8 Budoucnost Bitcoinu ... 26

3 Metodika ... 28

4 Praktická část ... 29

4.1 Komparace bitcoinových peněženek ... 29

4.1.1 Metoda párového porovnání ... 29

4.1.2 Výsledek párového porovnání ... 32

4.2 Využití poznatků v praxi ... 34

4.2.1 Trezor – příjem a odeslání transakcí ... 34

4.2.2 MyCelium – příjem transakcí ... 43

5 Závěr ... 47

6 Summary and keywords 48
7 Seznam použitých zdrojů 49
8 Seznam obrázků
9 Seznam tabulek

1 ÚVOD

Nápad vynalézt kryptoměny (digitální měny) vznikl jako řešení opakujících se krizí na finančních trzích. Můžeme říci, že jejich příchod byl již léta očekáván. S postupným rozvojem informačních technologií a ekonomie přišlo nejprve elektronické bankovnictví, ale to pro některé jedince nebylo dostačujícím pokrokem, právě díky zúčastněné třetí straně, bankám. Proto se lidé snažili vytvořit decentralizovanou měnu, která by byla dostupná všem, kdo by o ní měli zájem, a zároveň by se jednalo o rychlý obchod na velké vzdálenosti v rámci několika málo sekund. První nápady takovýchto měn se začaly objevovat již dříve, ale zatím se nikomu nepodařilo vyřešit problém dvojité útraty (o kterém si povíme dále). Tento problém vyřešil až na konci roku 2008 kdosi pod pseudonymem Satoshi Nakamoto s vynálezem první decentralizované digitální měny Bitcoin.

Bitcoin, jakožto nejznámější a zároveň první vynalezená kryptoměna, vznikla v roce 2009. Autorem je dodnes neznámá osobnost nebo možná skupina autorů skrývající se pod již zmíněným pseudonymem Satoshi Nakamoto. Stejně jako autor je i Bitcoin založený na anonymitě. Není závislý na žádném státu, státním orgánu či bance. Neexistuje třetí strana, která by ho ovládala. K potvrzení transakcí se používá open source peer-to-peer síť, která je kryptograficky šifrována. Bitcoin dnes můžete nakoupit na burzách a ve směnárnách (jak na internetových, tak v kamenných), můžete ho vyměnit s uživateli. Existují automaty, podobně jako jsou bankomaty, jen tyto slouží pro nákup či prodej Bitcoinů. Dnes i v České republice existují firmy, které platí výplaty svým zaměstnancům v bitcoinu či jiných kryptoměnách. Další možnou cestou je samotná těžba, ke které dříve stačily procesory počítačů (CPU), ty nahradily grafické karty (GPU) a dnes je potřeba speciálních těžebních strojů využívajících zákaznické integrované obvody (ASIC). Češi mají, co se týče Bitcoinu, dvě světová prvenství. Jedním z nich je vytvoření Slush Poolu, jedná se o seskupení těžařů založené Markem Palatinem.

Abyste měli kde vaše bitcoiny uchovat, je třeba vlastnit Bitcoin wallet, neboli bitcoinovou peněženku. Zde se nachází také více variant. Jednou z možností je papírová peněženka, kterou si vytisknete a máte jí i s veřejným a soukromým klíčem u sebe. Existují softwarové peněženky, které jsou dostupné na internetových stránkách nebo si můžete stáhnout samotnou aplikaci do počítače, mobilu či tabletu. V neposlední řadě je tu hardwarová peněženka, kde se jedná o druhé české prvenství. Stejně jako v prvním případě i tady hraje roli zakladatele Marek Palatinus.

S vašimi bitociny můžete dnes obchodovat na burzách, směňovat je za jiné kryptoměny či za fiat (zákonná měna, např. americký dolar) nebo si za ně můžete něco koupit.

S nápadem zpracovat bakalářskou práci na téma Bitcoin přišel v minulém roce můj původní vedoucí této práce doc. RNDr. Václav Nýdl, CSc. Nikdy dřív jsem o Bitcoinu neslyšela. Asi proto mě toto téma tak zaujalo, že jsem si hned začala vyhledávat odpovědi na otázky typu: Co je Bitcoin? Kde se vzal? Kdo za ním stojí? Jak funguje? Kde se k němu dostanu? Co s ním můžu provádět? Na odpovědi k těmto otázkám jsem přišla poměrně rychle. Zjistila jsem ale, že to, co nikde nenajdu, je jak si mám vybrat, kde své bitcoiny co nejlépe uschovávat. Na internetu najdete mnoho softwarových peněženek, možnosti k vytvoření papírové peněženky nebo si můžete zakoupit hardwarovou peněženku, ale těžko zjistíte, jakou a podle čeho si nejlépe vybrat. Každá z nich má jiné vlastnosti, je podporována jiným systémem nebo má jinou formu zabezpečení. Proto jsem se rozhodla v praktické části objektivně zpracovat, podle kterých kritérií si nejlépe vybrat vaši peněženku, které můžete věřit a budete s ní spokojeni.

1.1 Cíle práce

Cílem této práce je seznámit čtenáře s problematikou teoretického pozadí kryptoměn z historického hlediska se zaměřením na koncepty B-money a Bit gold, které byly základem pro vznik Bitcoinu. Hlavní část se pak věnuje této decentralizované měně zvané Bitcoin. Jsou zde představeny její hlavní historické milníky, role Bitcoin Foundation, samotný systém fungování, a v neposlední řadě možné vyhlídky pro Bitcoin do budoucna.

Cílem druhé části práce je vypracovat jednoduchý a přehledný systém výběru peněženky pro uschování bitcoinů. Podle čeho by se měl rozhodovat člověk, který uvažuje nad držením vlastních bitcoinů. Je zde použita metoda párového porovnání vybraných kritérií. Kritéria jsou porovnávána na základě předpokladu, že prioritou pro výběr je hlavně bitcoinová peněženka. Pro představu, jak taková peněženka vypadá a funguje, součástí praktické části je i ukázka dvou vybraných peněženek, podle výsledku komparace kritérií, a převodu jednoho dolaru mezi nimi, především jak nejvhodněji nastavit poplatek odesílané transakce. Cílem bakalářské práce je tedy zpracování komparace bitcoinových peněženek k využití pro běžné uživatele.

2 KRYPTOMĚNY SE ZAMĚŘENÍM NA BITCOIN

Kryptoměny mají základ v kryptografii, odkud pochází i jejich název. Kryptografie je matematická disciplína zabývající se šifrováním, tedy převodem zpráv v utajené podobě. Takovou zprávu lze přečíst pouze se znalostí šifrovacího klíče. Jelikož v síti Bitcoin odesílatel a adresát vlastní odlišné privátní klíče, jedná se o asymetrickou kryptografii. Bitcoin z poznatků kryptografie využívá asymetrickou kryptografii a hashovací funkce ke svému bezpečnému fungování.

Asymetrická kryptografie je skupina metod, kde klíč, který zprávu zašifrovává, je odlišný od klíče k její dešifraci. Tyto klíče není možné od sebe odvodit. Odlišnost klíčů umožňuje adresátovi šifrované zprávy nesdělovat odesílateli jeho tajný dešifrovací soukromý klíč, a naopak druhý veřejný klíč zpřístupnit. Jedním z prvků použití asymetrické kryptografie je digitální podpis, také známý jako elektronický podpis. Při podepisování zprávy, popřípadě pouze jejího hashe, se podpis spočítá pomocí soukromého klíče. To může učinit jen jeho vlastník. Jestliže tak vlastník učinil, může to naopak každý ověřit pomocí jeho veřejného klíče. Šifrování i podpis je možno kombinovat. Bitcoinový protokol používá algoritmus digitálního podpisu s využitím eliptických křivek, tedy ECDSA (Stroukal, D., & Skalický, J., 2015).

Pokud bychom si měli říci něco víc o hashi, jedná se o zobrazení z množiny dat obecné délky do množiny dat s omezenou délkou. Můžeme si to představit jako zobrazení souboru libovolné délky v množině 256-bitových čísel. Obecným požadavkem na hashovací funkci je uniformní pokrytí obrazů, tedy aby jednotlivé obrazy příslušely podobnému počtu vzorů. Požadavkem na krypto-grafickou hashovací funkci je navíc vysoká nelinearita. To znamená, že libovolně malá změna vzoru by měla způsobit libovolně velkou změnu obrazu. Zároveň je zde důležitý požadavek na symetrickou výpočetní složitost, v rámci které spočítat přímé zobrazení vzoru na obraz je snadné, ale spočítat obecně nejednoznačné inverzní zobrazení obrazu na vzor je extrémně obtížné. Příkladem hashovacích funkcí jsou různé kontrolní součty (XOR, rotace, tabulky) a CRC (tělesa nad dělením polynomů). Mezi kryptografické hashe patří např. funkce BLAKE, MD2-6, RIPEMD, SHA. Jak jsme si uvedli v příkladu, bitcoinový protokol používá poslední dvě jmenované - SHA-256 při těžbě bloků a RIPEMD.

Spolu s hashem pak souvisí hashovací rychlost. Tato veličina udává míru výpočetního výkonu uzlu nebo celé bitcoinové sítě. Její jednotkou je h/s – počet vypočtených hashů za sekundu. Odvozené jednotky jsou pak kh/s (kilohash; 1 kh/s = 1000 h/s), Mh/s

(megahash; 1 Mh/s = 1000 kh/s), GH/s (gigahash; 1 Gh/s = 1000 Mh/s), Th/s (terahash; 1 Th/s = 1000 Gh/s), PH/s (petahash; 1 Ph/s = 1000 Th/s), EH/s (exahash; 1 Eh/s = 1000 Ph/s) a další… Výkon celé sítě se za první čtyři roky zvýšil z 1 Mh/s na 10 Ph/s a do konce roku 2015 až na 550 Ph/s (tj. rozdíl o 11 dekadických řádů) (Stroukal, D., & Skalický, J., 2015).

Jako první decentralizovaná digitální měna přišel na svět bitcoin v roce 2009. Byl vytvořen anonymním člověkem nebo skupinou, která se nazývala Satoshi Nakamoto.

Pokud bychom si měli něco říci o digitálních měnách před rokem 2008, nebavili bychom se ještě o kryptoměnách, ale o něčem, co jim dalo základ pro budoucí tvorbu, jako například B-money a Bit gold.

2.1 Původ Bitcoinu

2.1.1 B-money

B-money byl předčasný návrh digitální měny vytvořený Wei Daiem jako „anonymní, distribuovaný elektronický peněžní systém“ (Satoshi Nakamoto odkazoval na návrh B-money ve svém protokolu). V eseji, publikované na kryptografickém emailovém seznamu v listopadu 1998, navrhl Dai dva protokoly. První protokol je nepraktický, protože vyžaduje vysílací kanál, který je nesrozumitelný a zároveň nesynchronní.

V prvním protokolu eseje je navrženo použití důkazu o pracovní funkci jako prostředku k vytvoření peněz. Daiovo B-money byly navrženy v souvislosti s diskusemi o emailovém seznamu. Týkaly se možných aplikací Hashcash, první symetrické funkce důkazu práce, která byla sama zveřejněna na stejném e-mailovém seznamu předchozí rok v květnu 1997 (podobně jako návrh B-money, samotný Bitcoin také využívá nákladovou funkci Hashcash jako důkaz práce při ražení nových mincí, zároveň se autor v protokolu Bitcoinu odkazuje právě na návrh B-money). V systému se peníze převádějí vysíláním transakce všem účastníkům, všem, kteří vedou účty ostatních. Transakce lze provést s možností možné opravy tím, že třetí strana souhlasí, že se stane rozhodčím. Pokud se neshodnou, každá strana pak vysílá argumenty nebo důkazy v jejich prospěch a každý z účastníků určuje opravné prostředky/pokuty ve svých účtech pro sebe.

Druhý protokol obsahuje pouze podmnožinu účastníků („servery“), kteří vedou účty, jež musí zveřejnit, a účastníky, kteří ověřující jejich zůstatky. Účastníci také ověřují, jestli peněžní nabídka není nafouknutá. Množství peněz jako kauce je povinno stát se serverem, který se ztratí, pokud je server považován za nečestný.

Alternativní metoda tvorby peněz je navržena prostřednictvím aukce, ve které účastníci nabízejí řešení výpočetních problémů známé složitosti (B-money, 2016).

2.1.2 Bit gold

V roce 2005 navrhl Nick Szabo mechanismus pro decentralizovanou digitální měnu, kterou nazval „Bit gold“ (můžeme přeložit jako bitové nebo digitální zlato). Bitové zlato nebylo nikdy implementováno, ale bylo nazýváno „přímým předchůdcem architektury Bitcoinu.“

Návrh Bit gold Szabo popisuje jako systém decentralizované tvorby nepopiratelného důkazu o pracovních řetězcích, přičemž každý z nich je připisován veřejnému klíči jeho objevitele, s použitím časových značek a digitálních podpisů. Říká se, že tyto důkazy o práci by měly hodnotu, protože by byly vzácné, těžko vyrobitelné, mohly být bezpečně uloženy a přeneseny. Szabova teorie ekonomiky těchto peněz je popsána v článku[1] o původu peněz (BitcoinWiki, 2016).

Jak sám autor Nick Szabo uvádí ve svém článku, že i zde byla hlavní myšlenka najít takový systém, který by nebyl závislý na jakékoli důvěryhodné třetí straně. Přišel tedy s návrhem bitového zlata, který je založen na výpočtu řetězce bitů z řetězce vyzvaných bitů, pomocí funkcí nazývaných různými způsoby - „funkce skriptu klienta“, „důkaz o pracovní funkci“ nebo „funkce spolehlivého porovnávání“. Výsledný řetězec bitů je důkazem práce (tzv. „proof of work“). Tam, kde je jednosměrná funkce obtížně spočitatelná, funkčnost bezpečného porovnávání ideálně směřuje s určitými konkrétními náklady, měřených v počítačích, ke zpětnému výpočtu (Szabo, 2005).

V roce 2008 byl vydán návrh Bitcoinu autorem, který se skryl pod jméno Satoshi Nakamoto. Jeho pravá identita zůstala tajemstvím, což dodnes vede ke spekulacím o dlouhém seznamu lidí, o nichž se předpokládá, že jsou Nakamoto. Ačkoli sám Szabo opakovaně popřel, že by jím byl, lidé o tom přesto spekulovali. (Biggs, J., 2013)

Nathaniel Popper napsal v článku časopisu The New York Times, že „nejpřesvědčivější důkaz poukázal na samotného amerického muže maďarského původu jmenovaného Nick Szabo.“ V roce 2008, před vydáním Bitcoinu, napsal Szabo na svém blogu komentář o záměru vytvořit živou verzi své hypotetické měny (Popper, 2015). Jak jsme si ale již uvedli dříve, nikdy se tak nestalo.

[1] Naleznete na stránce: http://unenumerated.blogspot.cz/2005/12/bit-gold.html

2.2 Bitcoin

Pokud se bavíme o jednotkách (měně), používáme název s malým ‚b' (bitcoin) a naopak velké ‚B', pokud jde o vynález nebo samotný systém.

Bitcoin je charakterizován několika jedinečnými vlastnostmi:

- *Decentralizace* – Nemá žádnou centrální autoritu, žádnou centrální banku. Vytváření mincí a potvrzování transakcí zajišťují jednotliví členové Bitcoin sítě kolektivně. Takový člověk se nazývá „miner" neboli těžař a ještě se mu budeme věnovat v jedné z podkapitol.
- *Žádný prostředník* – Již z předchozího bodu decentralizace vyplývá, že veškeré převody se posílají přímo a ihned skrze internet, bez prostředníků, bez bank či kreditních společností. Komunikace probíhá pomocí Peer-to-peer sítě.
- *Celosvětová a neznalá hranice* – Bitcoiny můžete v rámci několika sekund poslat na druhý konec světa a stejně tak uživateli, který stojí na metr od vás.
- *Neprolomitelná* – Princip Bitcoinové sítě se zakládá na kryptografii a silném šifrování, které zaručuje neprolomitelnost.
- *Transakční poplatky* – V začátcích Bitcoinu byly velmi nízké, skoro nulové, v současné době ale probíhá už tolik transakcí, že dostatečný poplatek je nutností.
- *(Pseudo)anonymní* – Transakce jsou definovány pomocí adres peněženek a žádnými osobními údaji.
- *Směnitelnost* – Bitcoiny můžete směnit za jakoukoli jinou měnu na světě.
- *Transparentní* – Projekt má zcela veřejné a otevřené zdrojové kódy, kdokoliv se může podívat a zkontrolovat přesné vnitřní fungování.
- *Dělitelnost* – Jednotka bitcoinu je dále dělitelná na osm desetinných míst, některá s vlastním názvem (viz Tabulka 1).

Tabulka 1: Dělitelnost bitcoinu

Jednotka	Množství v bitcoinech
1 BTC	1
1 cBTC („centibitcoin“)	0,01
1 mBTC („millibit“)	0,001
1µBTC („bits“)	0,000 001
1 Satoshi (sat.)	0,000 000 01

Zdroj: Autor práce

BTC je tří-symbolová zkratka jednotky bitcoinové měny.

Satoshi je nejmenší dělitelná jednotka pojmenovaná po zakladateli Satoshi Nakamoto.

Microbitcoin („bits“) má takovéto označení, protože tisíc jejích jednotek tvoří jeden bitcoin, zároveň jedna jednotka je tvořena stem sat.

Milibitcoin („milibit“) je takto označován z toho důvodu, že milion jednotek je roven jednomu bitcoinu, naopak stotisíc sat. tvoří jeden milibit.

2.3 Satoshi Nakamoto

Průvodní článek, protokol, tzv. „white paper“ byl 31. října 2008 publikován Satoshim Nakamotou, čož je jen pseudonym, pod kterým se autor ukryl. Výzkumný dokument byl nazván „Bitcoin: peer-to-peer elektronický hotovostní systém“. Byl implementován v prvním klientovi a uvolněn k open source komunitě v lednu 2009. Satoshi Nakamoto sám na internetovém fóru tvrdil, že se vývoji Bitcoinu věnoval od roku 2007. Ve spolupráci pokračoval s dalšími vývojáři softwaru až do poloviny roku 2010. Kolem této doby předal kontrolu nad úložištěm zdrojového kódu fanouškovi a vývojáři Gavinu Andresenovi. Nakamoto také přenesl několik souvisejících domén na různé významné členy komunity a poté zastavil svou účast v projektu, úplně se odmlčel. Před jeho nepřítomností provedl Satoshi Nakamoto všechny změny zdrojového kódu.

Dodnes nikdo stoprocentně neví, kdo pod pseudonymem Satoshi Nakamoto vymyslel něco tak geniálního, jako je právě Bitcoin. Co se týče informací, které o sobě Satoshi uvedl, tvrdil, že je mu 34 let a je Japonec. Jelikož jeho bezchybná angličtina v příspěvcích na fóru a v samotném „white paperu“ neobsahovala jakékoliv japonské slovo, jde spíše o někoho z anglicky mluvící země. Zároveň existuje zpráva jednoho fanouška (Švýcara Stefana Thomase), který prozkoumal nad 500 příspěvků, aby zjistil, kdo je Satoshi. Přinesl informaci, že Satoshi se musel v době své působnosti na fóru ukrývat někde

v časových pásmech -5 nebo -6 hodin Greenwichského času, pokud by chodil spát v obvyklém čase. To by ukazovalo na oblast Kanady a USA. (Stroukal, D., & Skalický, J., 2018)

Nakamoto měl velice dobrý důvod se skrývat. Lidé, kteří experimentují s měnou, většinou končí nejen krachem jejich vynálezů, ale zároveň se jejich činnost nezamlouvá státním vládám, a tak tyto vynálezce nechávají v některých případech zavřít do vězení. Neboť dosud nebylo zjištěno, kdo je autorem Bitcoinu, není ani možné tuto kryptoměnu zakázat. Je možné pouze velmi omezeně regulovat její využití.

2.4 Historické milníky

V této podkapitole budou rozebrány a popsány jednotlivé historické milníky od zrodu Bitcoinu po současnost.

Informace zde uvedené byly čerpány z bitcoin fóra (https://bitcointalk.org/) a anglické bitcoin wikipedie (https://en.bitcoin.it/wiki/) vytvořené členem fóra s konkrétními odkazy uvedenými v kapitole použitých zdrojů.[2]

Úplně první zmínku bychom mohli považovat v datu 18. srpna 2008, kdy byla zaregistrovaná doména „bitcoin.org“. Ve fóru bitcointalk.org administrátor s nickem theymos uvedl, že původním vlastníkem domény „bitcoin.org“ byl Satoshi Nakamoto, který ji registroval na stránkách https://www.anonymousspeech.com/, které povolují anonymní registrace domén (Bitcointalk.org, 8, 2012).

Satoshi Nakamoto publikoval 31. října 2008 dokument (tzv. „white paper“) s názvem „Bitcoin: A Peer-to-Peer Electronic Cash Systém“ v překladu „Bitcoin: peer-to-peer elektronický hotovostní systém“, v němž popisuje důvod vytvoření a vysvětluje praktický princip měny a jejich transakcí, který je v originále dostupný právě na doméně „bitcoin.org“.[3]

Následně byl projekt Bitcoin registrován 9. října 2008 na stránkách SourceForge.net, které se zaměřují na vývoj a distribuci softwaru na bázi open source (BitcoinWiki, 2010).

Historicky první blok, zvaný „Genesis block“, vznikl v „účetní knize“ blockchain 3. ledna 2009 a obsahoval pouze jednu transakci o hodnotě 50 BTC (Blockexplorer.com, 2009).

[2] BitcoinWiki není datována, proto autorka používá rok 2010, kdy byla stránka vytvořena
[3] Viz. https://bitcoin.org/bitcoin.pdf

První verze Bitcoin 0.1 byla vydána 9. ledna 2009 (oznámena na kryptografickém mailingovém seznamu).[4] Kód byl sestaven pomocí Microsoft Visual Studia pro Windows a postrádal příkazový řádek s rozhraním. Jelikož byla měna tak dobře propracovaná, mnoho spekulací se přiklání k názoru, že za vývojem stála spíše skupina než jednotlivec (nebo akademický vědec, který alespoň zčásti ovládá programování). Zahrnovala generační systém, který je schopný vytvořit celkem 21 milionů Bitcoinů. Předpokládá se, že do roku 2140 budou všechny Bitcoiny vytěženy (BitcoinWiki, 2010).

12. ledna 2009 proběhla první transakce mezi Satoshim a Halem Finneym (Harold Thomas Finney, počítačový vědec a vývojář). Jelikož nejméně prvních sto transakcí bylo generováno jako „nepotvrzených", tato transakce se objevila až v bloku č. 170[5] (Bitcointalk.org, 8, 2012).

První oficiální stanovení kurzu bylo 5. října 2009 na webu New Liberty Standard. Cena jednoho dolaru se rovnala 1,309.03 BTC. Tato cena byla vysoce nadhodnocena (Bitcointalk.org, 8, 2012). Oficiálně se obchodovalo za cenu méně než setinu dolaru.

Bitcoin software development channel byl registrován 9. října 2009 na freenode IRC. Jedná se o stránky vytvořené pro diskusi o vývoji softwaru.

Druhá verze, tedy Bitcoin 0.2, byla vydána 16. prosince 2009.

Po jejím zavedení můžeme přisuzovat dni 30. prosince 2009 první nárůst obtížnosti.

V následujícím roce vznikla 6. února 2010 první burza Bitcoin Market. Obchodování na stránkách začalo 17. března 2010 (BitcoinWiki, 2010).

Laszlo Hanyecz, programátor žijící na Floridě, uskutečnil 22. května 2010 první a zároveň nejslavnější platbu v historii bitcoinu za objednávku pizzy od Papa John's v hodnotě 10 000 BTC, což bylo v přepočtu 25 USD. V zimě 2017 by to byla pětina miliardy USD (Bitcointalk.org, 2010).

Zajímavý je ale příběh, který se za nákupem odehrál. Na diskusním fóru Laszlo napsal 18. května 2010 příspěvek s nabídkou: „Zaplatím 10 000 bitcoinů za pár pizz... za dvě velké, aby mi něco zbylo na další den. Rád si nechám kus pizzy na pozdější ďobání (...). Pokud máte zájem, dejte vědět, nějak se domluvíme. Díky Laszlo." Na to přišla reakce od jednoho Angličana, který následně na internetu našel Papa John's pizzerii, kterou Laszlo doporučil, zavolal do obchodu a objednal pizzu, za kterou zaplatil 25 dolarů

[4] Viz. https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html

[5] Viz. https://blockchain.info/block/00000000d1145790a8694403d4063f323d499e655c83426834d4ce2f8dd4a2ee

kartou. Pizzu přivezli Laszlovi do domu, a tak poslal Angličanovi 10 000 BTC na jeho peněženku. Na fóru informoval, že pizza dorazila a že si na ní on i dcera moc pochutnali. K příspěvku přidal i fotografie, jak „ďobají."

Třetí verze, tedy Bitcoin 0.3, byla vydána 6. července 2010.

O Bitcoin se začalo zajímat mnohem více uživatelů, což mělo za následek nárůst ceny za jeden Bitcoin. Cena se v průběhu pouhých pár dní až zdesetinásobila. 12. července 2010 se začala navyšovat hodnota výměny, během pěti dní z přibližně 0.008 USD/BTC na 0.08 USD/BTC.

17. července 2010 byla založena Jadem McCalebem burza Mt.Gox, nazývaná „Mount Gox" nebo prostě „Gox". Byla nejpoužívanějším burzovním měnovým trhem od jejího založení až po její insolvenci koncem roku 2013.

V srpnu se objevila první a doposud jediná chyba v programu. Umožňovala uživatelům provádět transakce dvakrát. 15. srpna 2010 se díky chybě dokonce podařilo vytvořit při jedné transakci až 184 miliard bitcoinů, což je vzhledem k omezenému počtu bitcoinů skutečně zarážející číslo. Transakce ale byla během hodin odhalena a vymazána ze záznamů a ani sami autoři o ní moc nemluví.

První použití dělení alokace generační odměny proběhlo 14. září 2010 k vytěžení bloku č. 79 764.

29. září 2010 se díky nepotvrzujícím se mikrotransakcím uspíšilo vydání verze Bitcoin 0.3.13.

Směnný kurz se začal zvedat 7. října 2010 po několika plochých měsících z 0,06 USD/BTC.

Bitcoin-otc trading channel byl registrován 17. října 2010 na freenode IRC. Sloužil pro obchodování na volném trhu (otc tedy tzv. over-the-counter znamená v překladu přes pult) (BitcoinWiki, 2010).

27. října 2010 zveřejnil slush na fóru možnost poolové těžby s dostatkem informací a odkazy na web, facebookové a twitterové stránky a zároveň blog (Bitcointalk.org, 2010).

28. října 2010 byla zahájena první transakce s krátkým prodejem. Jednalo se o půjčku 100 BTC umožněnou díky Bitcoin-otc trading channel (BitcoinWiki, 2010).

Cena vytěžených Bitcoinů dosáhla 6. listopadu 2010 jednoho milionu dolarů. Tato cena byla kalkulována v čase, kdy jeden Bitcoin stál 0.05 USD.

7. prosince 2010 uživatel jménem doublec, člen bitcoinového fóra, sestavil klienta Bitcoind, který byl sepsán pro mobilní počítač Nokia N900. Následující den mu ribuck poslal v první portable-to-portable Bitcoin transakci 0,42 BTC pomocí Bitcoindu.

16. prosince 2010 Bitcoin Pooled Mining, provozovaný slushem, našel svůj první blok. Jedná se o skupinu uživatelů, která je vedena slushem (přezdívka Čecha jménem Marek Palatinus) a dodnes provozuje web https://slushpool.com/ pro těžbu Bitcoinu (BitcoinWiki, 2010).

V lednu 2011 se zprovoznil a otevřel Silk Road. Jednalo se o webovou stránku, nezákonný trh s drogami, kde bylo možné platit bitcoiny právě pro nemožnost vystopování původu transakcí (Be a BITCOIN Millionaire: Beginner to master). Ať už šlo o prodej či nákup, dělalo to Bitcoinu špatnou pověst. I ta ale byla přínosná, protože se o něj začalo zajímat více lidí a s tím rostla i cena.

2. ledna 2011 byly standardizovány jednotky Tonal Bitcoin (TBC). Jde o reprezentaci systému Bitcoin zaměřeného na lidi, kteří upřednostňují systém v jednotkách Tonal.

28. ledna 2011 byl vytvořen blok č. 105000. To znamená, že bylo vytvořeno 5,25 milionů bitcoinů, což je jen něco málo přes čtvrtinu z celkového počtu téměř 21 milionů.

Bitcoin dosáhl 9. února 2011 parity s americkým dolarem a dotkl se hodnoty 1 USD za BTC u společnosti Mt.Gox (BitcoinWiki, 2010).

14. února 2011 australský člen diskuzního fóra jako historicky první nabídl vozidlo k prodeji za bitcoiny. Jednalo se o Celica Supra z roku 1984, které Australan nabídl za 3000 BTC, ke komentáři přiložil i fotografie. Jeho nabídku ale nikdo nepřijal, tedy co se týče příspěvků na fóru (Bitcointalk.org, 2010).

25. února 2011 je registrovaná adresa WeUsCoins.com, která slouží jako zdroj informací o Bitcoinu. WeUseCoins.com zveřejnili 22. března 2011 virální video s názvem „What is Bitcoin?“, které dnes (v době psaní práce) má bezmála 8 470 000 zhlédnutí. 24. dubna 2014 pak zveřejnili ještě novější verzi, která již má téměř 5 492 600 zhlédnutí.

Mark Marie Robert Karpelès (pod přezdívkou MagicalTux) koupil 1. března 2011 mtgox.com od zakladatele Jeda McCaleba.

Time Magazine zveřejnili 16. dubna 2011 článek o Bitcoinu.

Směnný kurz dosáhl 2. června 2011 výše 10 USD za 1 BTC u společnosti Mt.Gox (BitcoinWiki, 2010).

Uživatel fóra allinvain prohlásil, že mu bylo z bitcoinové peněženky ukradeno 25 000 BTC (přibližně 375 000 USD).

19. června 2011 byla ohrožena databáze Mt.Gox a uživatelská tabulka, která obsahovala podrobnosti o desítkách tisíc uživatelských jménech, e-mailových adresách a heslech, z nichž některá byla příliš jednoduchá, byla vypuštěna na veřejnost.

Někdo mohl přistupovat k účtu administrátora v Mt.Goxu a zadávat objednávky k prodeji stovek tisíc falešných bitcoinů, což způsobilo, že cena Mt.Goxu se snížila z 17,51 USD na 0,01 USD za 1 BTC. Společnost Mt.Gox oznámila, že tyto obchody budou zrušeny. Obchodování u společnosti Mt.Gox bylo zastaveno po dobu 7 dní (a také krátce u TradeHill a Britcoin, zatímco jejich bezpečnost byla přezkoumána).

Někteří uživatelé z uniklé databáze Mt.Gox používali stejné jméno uživatele v MyBitcoin a jejich hesla byla napadena. Přibližně 600 z nich bylo vyřazeno z účtů MyBitcoin. Jeden uživatel ztratil více než 2000 BTC (BitcoinWiki, 2010).

19. července 2011 byla zaznamenána první transakce obdržená manažerem Mika Hearna, Tadekem pomocí NFC (Groups.google.com, 2011).

První mezinárodní konference o Bitcoinu se konala na světové výstavě World Expo 20. srpna 2011 v New Yorku.

25. listopadu 2011 se konala první evropská Bitcoin konference v Evropě. Akce se uskutečnila v Praze v České republice.

V červnu 2012 byla založena v San Franciscu v Kalifornii Coinbase, bitcoinová peněženka a platforma.

Již třetí Bitcoinová konference se konala v Londýně 15. a 16. září 2012.

27. září 2012 byla založena Bitcoin Foundation, o které se dočtete v samostatné podkapitole.

15. listopadu 2012 publikační platforma WordPress.com oznámila přijetí bitcoinu jako platební metody za placené funkce systému.

28. listopad 2012 byl označen jako den zeslabení měny. Blok č. 210 000 byl první s blokovou dotací na odměnu pouze 25 BTC.

6. prosince 2012 získala první bitcoinová burza bankovní licenci v Evropě (BitcoinWiki, 2010).

V roce 2012 se objevila na trhu společnost bitpay.com, která dodnes nabízí firmám možnost zprovoznění plateb bitcoiny na jejich stránkách. Již v druhém roce působnosti počet takových obchodů stoupl z jednoho tisíce na patnáct tisíc. (Stroukal, D., & Skalický, J., 2018)

19. února 2013 byla uvedena do oběhu 8. verze Bitcoin Client.

28. března 2013 hranice trhu bitcoinu překročila 1 miliardu USD se skoro 11 miliony vytěženými Bitcoiny.

Směnný kurz dosáhl 1. dubna 2013 výše 100 USD za 1 BTC na burze Mt.Gox i dalších významných burzách (BitcoinWiki, 2010). Do konce měsíce se ale dokázal vyšplhat ještě výš, a to na 266 dolarů.

2. května 2013 vyšel na svět první Bitcoin ATM (bankomat na nákup a prodej bitcoinů) umístěný v San Diegu v Kalifornii.

V srpnu 2013 Německo prohlásilo Bitcoin za právní měnu (Be a BITCOIN Millionaire: Beginner to master).

V říjnu 2013 byl zatčen Ross William Ulbricht, jakožto zakladatel webové stránky Silk Road, která byla zastavena spolu s jeho zatčením. Zároveň bylo z účtu Silk Road zabaveno přibližně 26 000 bitcoinů a z účtu, který měl údajně patřit Ulbrichtovi, později dalších 144 000 bitcoinů (Hill, K., 2013). Ulbricht byl odsouzený na doživotí bez možnosti propuštění.

Cenu bitcoinu to ovlivnilo pouze na jeden den. A stejně rychle jako poklesla, vystoupala zase na původní částku.

Náhlé skoky kryptoměny nastaly pak v listopadu, kdy velký americký tvůrce her Zynga začal podporovat Bitcoin. V tomtéž měsíci jedna z vysokých škol Kypru povolila platby školného pomocí bitcoinů (Be a BITCOIN Millionaire: Beginner to master).

Společnost Virgin Galactic, která plánuje soukromé lety do vesmíru, v listopadu 2013 oznámila, že přijímá bitcoin. Nabídku v té době využilo pár jedinců, a tak vycestovali do vesmíru za pouhých 250 mincí bitcoinu za jedince.

V polovině měsíce pak cena 1 mince překročila cenu 1000 dolarů.

Za celé čtyři roky působnosti Bitcoinu se hlavně v roce 2012 a 2013 začalo mluvit o Bitcoinu nejen v televizních zprávách, ale objevovaly se i fotografie na sociálních sítích, na kterých byli lidé vyfoceni s věcmi, produkty, které už reálně zakoupili za bitcoin.

Lidé si ho natolik oblíbili, že se začali objevovat projekty, jako byl projekt Satoshiho les. Jednalo se o založení domova pro bezdomovce na Floridě, který byl financován pouze bitcoiny.

Zároveň se objevovaly i první poplašné zprávy z řad televizí a článků v magazínech, které informovali například o tom, že thajská centrální banka zakázala používat bitcoin. Jelikož ale nejde zjistit původ vlastníka adresy, není možné tento zákaz nijak kontrolovat. Takovýchto falešných zpráv se objevuje dodnes mnoho (Stroukal, D., & Skalický, J., 2018).

V lednu 2014 začíná Bitcoin nahrazovat euro v Irsku. Velký počet společností souhlasil přijímat platby za služby v bitcoinech.

24. ledna 2014 Čína znovu povolila obchodování s bitcoiny.

7. února. 2014 burza Mt.Gox pozastavila veškeré transakce z důvodu podezření o masovém útoku prostřednictvím zranitelnosti transakcí (tzv. maleabilitu transakcí, kterou si ještě zmíníme). Tento důvod se ale nikdy nepotvrdil (Be a BITCOIN Millionaire: Beginner to master). Burza nakonec zavřela 24. února stránky a o pár dní později zkrachovala oficiálně.

Problémy s transakcemi byly nalezeny v průběhu dalších dní i v jiných hlavních burzách. V důsledku toho poklesla cena bitcoinu z 1163 USD pod cenu 1000 USD a nakonec se ustálila mezi osmi a devíti sty dolary.

Plno lidí si nebylo jisto, jak mají na tuto událost reagovat. Tomu ale pomohlo rozšíření automatů i do jiných zemí. Lidé tak nemuseli nakupovat na burzách a mohli využít nákupů rovnou přes automat bez vstupu na burzu.

Ustálená cena se ale znovu propadla, a to až k 340 americkým dolarům.

V srpnu 2014 ministr financí Velké Británie nakoupil bitcoin za 20 liber, aby ukázal jeho pozitivní postoj k digitální měně bitcoin.

V tomto roce se v České republice objevila první hardwarová peněženka zvaná TREZOR, druhé z českých prvenství (prvním byl Slushpool). Zároveň se otevřel institut krypoanarchie Paralelní Polis v pražských Holešovicích, které je dodnes hlavním centrem pro bitcoinovou komunitu v České republice.

V prosinci 2014 oznámila společnost Microsoft začátek přijímání plateb v bitcoinech. To je názorná ukázka toho, že i v dobách, kdy klesá cena, nemusí s ní klesat i poptávka.

V lednu 2015 pak Jakub Jedlický, český expert na kryptoměny, otevřel na Vysoké škole ekonomické v Praze kurz Kryptoměny a další alternativní měnová řešení ve světové praxi. Byl to již druhý kurz týkající se kryptoměn na této škole.

V tomto roce se masivněji rozšířil seznam míst, kde je možné utratit bitcoiny. Známými firmami byly Dell, T-mobile v Polsku, čerpací stanice Lukoil v Pobaltí, Movietickets v USA, polský letecký dopravce LOT nebo například BitBrno, která umožnila nákup jízdenek MHD za bitcoin. Takovýchto společností bylo tisíce po celém světě.

V Paralelní Polis se začaly konat každé úterý Bitcoin meetupy, kam může přijít kdokoli a může se dozvědět nejen více o Bitcoinu, ale i o jiných kryptoměnách. Jedná se o přednášky a následné debaty zaměřené jak na informativní základ, tak také na ekonomický kontext.

Zajímavostí v dubnu roku 2015 je založení mikrostátu Liberland na pomezí Chorvatska a Srbska, který založil Čech Vít Jedlička. Měnou mikrostátu mělo být také použití Bitcoinu nebo jiné podobné kryptoměny. Tato zpráva rychle obletěla svět. Objevilo se statisíce zájemců o občanství v novém státě a zároveň vzrostl zájem mezi médii o měnu budoucnosti. Cena bitcoinu tak vzrostla z 200 dolarů až k 500 dolarům.

V září 2015 se Čína rozhodla provádět kapitálové kontroly, což vedlo investory k zaměření se na zahraniční investice až v řádech desítek miliard dolarů. Čína se tak následně rozhodla zaměřit se na kontrolu přeshraničních toků financí. Přestože mnoho spekulantů se bálo, že tyto události povedou cenu bitcoinu dolů, stal se pravý opak a bitcoin si tak polepšil růstem ceny.

I u nás v Evropě měl Bitcoin úspěch. Evropský soudní dvůr rozhodl, že se na směnu bitcoinů nevztahuje DPH. Některé státy totiž vedly spor, zda se jedná o zboží nebo něco jiného.

V roce 2016 se ujaly termíny mezi českou bitcoinovou komunitou, a to „hodl“ a „hodler“. Jedná se o překlad z angličtiny, kde hodl znamená držení bitcoinů i přes výkyvy ceny a hodler je pak ten, kdo „hodluje“.

V srpnu 2016 přišla jedna z největších burz Bitfinex o 120 tisíc bitcoinů, což ale ve srovnáním s krachem Mt.Gox nebyla taková katastrofa. Bitfinex reagovala rychle a postupně splatila všechny ztráty. Tím získala i svou důvěru zpět. Tato ztráta trhem moc neotřásla, protože burza již nebyla jedinou ve svém oboru.

Přidávaly se stále nové obchody, které podporují platby bitcoiny, mezi ně patří např. švýcarské dráhy nebo herní portál Stream. O prázdninách roku 2017 se připojil i největší český e-shop Alza (Stroukal, D., & Skalický, J., 2018), která zároveň umístila ve svém showroomu v Praze jeden z automatů. Jejich počet se za poslední dva roky již zdvojnásobil a na celém světě jich je téměř osm set. V České republice je můžete k dubnu 2018 nalézt v Praze, Brně, Ostravě, Plzni, Karlových Varech, Hradci Králové, Děčíně a Liberci.

Bitcoin zároveň v roce 2017 pomohl zachránit několik životů v hrůze a utrpení. Svědčí o tom příběhy venezuelských lidí, kteří v době, kdy Venezuela stála na pokraji zhroucení, nakoupili bitcoiny. Jejich peníze tak nepodlehly hyperinflaci a oni si za výdělek v kryptoměně pořídili letenky ze země.

Toto vše pomohlo k masivnímu růstu ceny. Ze 400 dolarů, kolik stál bitcoin v roce 2016, se cena vyhoupla na přelomu s rokem 2017 na 1000 dolarů a růst pokračoval po

celý rok až k částce 20 000 dolarů za jeden bitcoin. Tento nárůst byl obrovský, avšak ne největší v historii bitcoinu.

V posledních letech se začalo ukazovat jako problém původní nastavení omezení počtu transakcí za jednotku času. Doposud vše fungovalo, jak mělo, jen s postupným nárůstem uživatelů se začala síť zahlcovat. Názory komunity se začaly lišit. Někteří chtěli systém zachovat, tak jak funguje od počátku, a jiní chtěli najít řešení, jak zvětšit propustnost sítě a zároveň zlevnit transakce. Čínští těžaři kolem společnosti Bitmain nechtěli provádět změny, protože jejich těžařské stoje jim umožňovaly těžit o 20 % více bitcoinů než ostatním. Tato informace ale byla dlouho utajovaná, a tak když už vyšla na povrch, tito těžaři se rozhodli pro vytvoření vlastního Bitcoinu s názvem Bitcoin Cash. Druhá část komunity, která zůstala u původní měny, přišla s řešením SegWitu, který si specifikujeme v jiné podkapitole (Stroukal, D., & Skalický, J., 2018).

Snad tou nejnovější zajímavostí a zároveň informací na pobavení je aprílový článek (Kasík, 2018) na stránkách iDnes.cz, který uvádí, že čeští poslanci se shodli na vytvoření devíti nových kryptoměn, podobným Bitcoinu, které budou fungovat paralelně s českou korunou.

2.5 Bitcoin Foundation

Jako první se zmínkou o americké neziskové organizaci Bitcoin Foundation přišel časopis Forbes s článkem psaným jedním z členů představenstva nadace (Matonis, 2012). Bitcoin Foundation byla založena v září roku 2012. Má za úkol standardizovat, chránit a podporovat používání kryptoměny Bitcoin ve prospěch uživatelů po celém světě. Kromě toho také finančně sponzoruje úsilí hlavního vývojového týmu, má na starost financování jádrové infrastruktury, jako je zkušební síť a DNS seed note, publikování souboru osvědčených postupů pro integraci bitcoinů, koordinaci reakcí na podnikání a mediální šetření a pořádání každoroční Bitkoinové konference. První konference se konala v Silicon Valley.

Navíc nejen jednotlivým členům poskytuje Bitcoin Foundation možnost, také jednotlivým korporátním podnikům ze všech průmyslových odvětví je umožněno podílet se na rozšiřování sítě Bitcoin a platformy.

Hlavním záměrem pro vytvoření společnosti Bitcoin Foundation bylo to, že bude řízena členy a bitcoinovou komunitou, včetně plánování do budoucna. Jak je uvedeno ve struktuře správy, jednotliví a průmysloví členové společnosti budou mít hlasovací práva

v souladu s články a stanovami nadace Bitcoin Foundation. Roční individuální členství činí 2,5 BTC s možností životnosti 25,0 BTC; firemní členství je 500 BTC pro stříbrnou vrstvu, 2 500 BTC pro zlatou vrstvu a 10 000 BTC pro platinovou vrstvu. Dnes by uživatele členství stálo 10 dolarů za měsíc nebo 100 dolarů za rok, jak uvádí nadace na svých webových stránkách (Foundation, 2018).

Mezi první členy představenstva patří Gavin Andresen (tentýž, kterému Satoshi předal pravomoc), Mark Karpeles, Jon Matonis, Patrick Murck, Charlie Shrem a Peter Vessenes.

Výkonný ředitel Vessenes prohlásil: "Doufám, že nadace Bitcoin Foundation bude organizací, která se zaměřuje na veškerou vaši energii a talenty na propagaci Bitcoinu, jeho ochranu a zvyšování legitimity prostřednictvím standardizace. Bitcoin je podle mého názoru internetovou měnou a je tak vzrušující být součástí této rušivé a poutavé technologie!" (Matonis, 2012).

Dnes je na postu výkonného ředitele představenstva Llew Claasen, předsedou je Brock Pierce. Více předsedou je Bobby Lee a mezi další členy také patří Bruce Fenton, Elizabeth McCauley, Michael Perklin, Francois Pouliot, Vinny Lingham. Tito členové se zajímají o vývoj v oblasti digitálního světa i mimo nadaci, což potvrzuje jejich účast i na jiných projektech. Například Elizabeth McCauleyová je vedoucí globálního obchodního vývoje na Coinsecure, největší indické burze s bitcoiny (Foundation, 2018).

Dne 29. března 2016 byla Bitcoin Foundation uvedena britskou společností Richtopia jako 27. v seznamu 100 nejvlivnějších blockchainových organizací. V průběhu času se ale s vývojem nových měn a zakládáním nových organizací posouvá v seznamu na 53. místo (Richtopia, 2016).

2.6 Mezinárodní konference

Správa a vývoj sítě Bitcoinu je důležitý, ale zároveň je důležité o něm informovat svět. Nejen to. Zároveň zájemce o informace v této oblasti je třeba vzdělávat. K tomu slouží veškeré přednášky a konference původně vedené jen mezi pár set lidmi. Dnes už jde o tisíce účastníků ročně.

První Bitcoinová konference se konala 20. srpna 2011 na světové výstavě World Expo v New Yorku. Oznámení se objevilo o čtyři měsíce dříve na fóru, kde bylo zároveň oznámeno, že bude streamovaný přenos na stránkách OnlyOneTV.com. (Bitcointalk.org, 2011)

Druhá konference se uskutečnila 25. listopadu téhož roku. Jednalo se o první Bitcoinovou konferenci v Evropě. Akce se konala v Praze v České republice.

Dalšího roku proběhla 15. a 16. září v Londýně již třetí a jediná konference v roce 2012, která očekávala okolo 300 návštěvníků.

První tři konference nebyly vedeny pouze na téma Bitcoinu. Téma této kryproměny bylo pouze malou částí celé konference. Další konference se už týkaly jen Bitcoinu a na konci každé bylo místo i pro diskuzi.

Existují záznamy z pražské a londýnské konference. Jejich odkazy jsou uvedeny na fóru, kam se každý jednoduše dostane přes článek o dalších dvou konferencích konaných v roce 2013.

Tyto konference se konaly 17. - 19. května v San Jose, v Kalifornii a ve Vídni 1. - 3. října. (Bitcoinmagazine.com, 2013)

Každý rok poté přibývalo stále více a více událostí a států, kde se konference konaly. Každá z nich by však měla být oznámena na bitcoinovém fóru v sekci „Meetups“. Dnes se uskutečňují měsíčně (někde i častěji) na několika místech na světě, proto je jejich seznam tak široký. Každý den v roce je minimálně jedno takové setkání se sta až tisíci návštěvníky. Jejich seznam je možné nalézt například na stránkách týkajících se setkání a konferencí.[6]

2.7 Princip fungování Bitcoinu

Jak Bitcoin funguje, si můžete ve stručnosti dohledat a dočíst na mnoha stránkách na internetu. Problémem je, že většina těchto stránek téma pouze zmíní, protože ne každý této problematice rozumí v takové míře, aby mohl dávat rady. Sama jsem se zúčastnila několika přednášek vedených odborníky v Paralelní Polis[7] i v Českých Budějovicích. Nejen základy získané na těchto přednáškách, ale i s podpora knihy Stroukal, D., & Skalický, J. (2018) a „white paperu“ (Nakamoto, 2009), mi pomohly zpracovat přehled toho, jak Bitcoin funguje, který je uveden v dalších podkapitolách.

2.7.1 Peněženka a její adresa

Peněženka (Wallet) je software, který spravuje soukromé klíče bitcoinových adres uživatele. Taková peněženka nejen že uvádí zůstatky na daných adresách, ale zároveň

[6] https://www.meetup.com/topics/bitcoin/
[7] Hackerspace Institut Kryptoanarchie v Praze

umožňuje odesílání plateb, vedení historie transakcí nebo evidenci známých adres (tzv. adresář). Starší verze první peněženky Bitcoin-Qt, kromě vlastností peněženek obecně, obsahovala i možnost těžit nové bloky. Jednalo se tak o plnohodnotného klienta sítě. Implementace peněženky tak může mít několik podob. Kromě konvenční aplikace (Bitcoin Core, Mycelium, Armory, Elecrum) existuje možnost online služby (např. Blockchain.info, BitGo, Coin.Space), papírová peněženka nebo hardwarová peněženka (TREZOR, Ledger). Ještě si některé podrobněji projdeme v druhé části práce. Jelikož adresy uživatele (a k ní příslušné klíče) jsou spravovány bitcoinovou peněženkou, je důležité vědět, kdo je jejich vlastníkem.

S peněženkou úzce souvisí pojmy privátní a veřejný klíč.

Privátní (také jinak soukromý) klíč je jeden ze dvou typů klíčů pro asymetrickou kryptografii.[8] Tento klíč musí zůstat tajný a zná ho pouze jeho majitel. Používá se k zašifrování (podepisování) odesílané zprávy a dešifrování naopak přijímané zprávy. V bitcoinové síti se pomocí soukromého klíče tzv. podepisuje zpráva s informací, kdo bude novým disponentem odesílaných bitcoinů (přesněji adresátem vznikající transakce). Každá bitcoinová adresa vlastní právě jeden soukromý klíč, který je uložen v bitcoinové peněžence.

Veřejný klíč je druhý typ klíče pro asymetrickou kryptografii. Veřejný je z toho důvodu, že ho může kdokoliv použít k zašifrování zprávy nebo k ověření podpisu. V bitcoinové síti lze vypočítat samotnou adresu příjemce platby z veřejného klíče.

Bitcoinová adresa je podobně jako číslo bankovního účtu jednoznačnou identifikací příjemce a odesílatele platby. Její fyzickou podobou je dlouhé číslo zakódované v řetězci alfanumerických znaků s následujícími vlastnostmi:

- Samotná délka je 27–34 znaků.
- Rozlišují se velká a malá písmena.
- Začíná označením verze – číslicí ‘1’ nebo ‘3’ (novější, podporuje SegWit[9]).
- Neobsahuje typograficky zaměnitelné znaky ‘0’, ‘O’; ‘I’, ‘l’.
- Poslední znaky obsahují kontrolní součet (zabezpečení proti špatnému opsání/vykopírování).

[8] Tento pojem jsme si již vysvětlili na začátku celé kapioly
[9] SegWitu bude zmíněn v kapitole Budoucnost Bitcoinu

příklady:

1NHkNd4jV66vBGYapRwbND6vgAycPEFn9D

35zFwvbdVtKAne3emUQHb3uJnXYzX1UWsk

Bitcoinovou adresu je možné vygenerovat offline (bez spolupráce sítě), neboť je pouze hashem veřejného klíče (stačí mít pár klíčů pro asymetrickou kryptografii a následně se aplikuje posloupnost funkcí Base58 (version + RIPEMD-160(SHA-256(pubkey)) + SHA-256^2(version + RIPEMD-160(SHA-256(pubkey)))[0..3])[10]. Generování adresy je očividně lehká operace, a proto je zde možnost vygenerovat novou adresu pro každou další transakci. Tento princip znesnadňuje jejich stopování. Uživatel může prokázat vlastnictví konkrétní adresy tím, že podepíše určitou zprávu soukromým klíčem příslušejícím k dané adrese. Díky tomuto faktu se nikomu, kdo o sobě doposud prohlásil, že je Satoshi Nakamoto, nepodařilo jeho tvrzení prokázat.

QR kód („Quick Response“) je dvourozměrný čárový (spíše „čtverečkový“) kód pro optické strojové zpracování. Je tvořen černými čtverečky v matici o velikosti 21 x 21 až 177 x 177 polí na bílém pozadí. Uživatel si může načíst samotnou adresu pro odeslání transakce nebo již předpřipravenou hodnotu transakce spolu s adresou. Tři charakteristické kontrastní rohy matice slouží k normalizaci velikosti, orientace a úhlu obrazu. Kód s největší maticí může nést až 2953 bajtů, běžně používané velikosti nesou desítky až stovky alfanumerických znaků (např. právě bitcoinovou adresu). Kód obsahuje čtyř-úrovňové zabezpečení Reed-Solomon, díky kterému je odolný proti chybám (znečištění části kódu, ustřižený roh apod.).

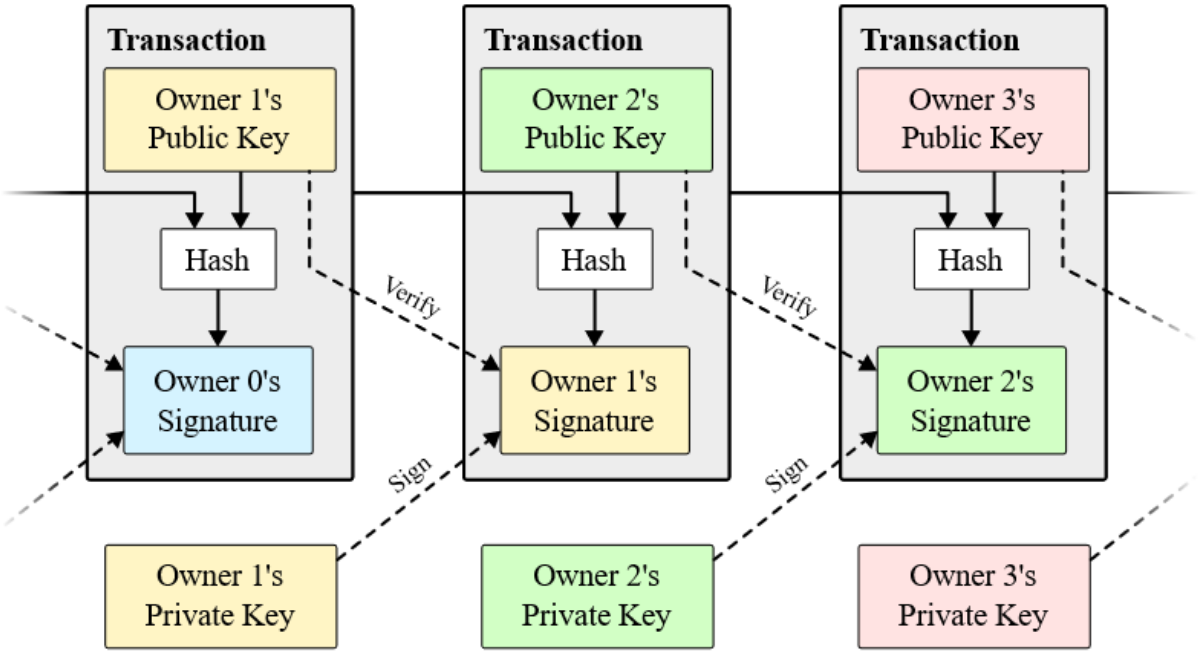
2.7.2 Transakce

Transakce je informace o převodu bitcoinů z jedné adresy na adresu jinou. Interně se jedná o datovou strukturu obsahující dvojici množin tzv. vstupů a výstupů. Vstup zde představuje výstup z nějaké předchozí, již existující, transakce. Výstup pak představuje množství bitcoinů, které z něho lze uvolnit. Celkový objem transakce je roven součtu hodnot všech jejích vstupů. Celkový objem je možné mezi výstupy nové transakce rozdělit libovolně v případě, že součet jejich hodnot není větší. Pokud by byl menší, rozdíl pak představuje poplatek za transakci. Speciálním typem transakce, který obsahuje pouze výstupy, je „generující transakce“, kterou si popíšeme ještě v podkapitole těžby. Výstup je dále používán (na vstupu nové transakce) jako jeden celek, není dělitelný (a pouze

[10] Operátor ‚+‘ zde značí zřetězení, třetí operand je zabezpečení (první 4 bajty hashe klíče)

jednou použitelný). K tomu, aby mohl být výstup uvolněn pro další vstup, je třeba podepsat danou transakci soukromým klíčem, který patří k jeho adrese. To pak dává jedinečné právo k výstupu pouze jejímu majiteli. Ve skutečnosti je systém nárokování výstupu obecnější a umožňuje vytvářet složité podmínky, které musí být pro jeho použití splněny (např. uvolnění výstupu více podpisy, heslem, postdatování, atd.). Složitějším a kombinovaným podmínkám říkáme „smlouvy “ a programují se ve skriptovacím jazyce, jehož triviální větou je i běžná podmínka na výše zmíněný podpis klíčem patřícím k adrese.

Obrázek 1: Interní generování adres při transakcích



Zdroj: (Nakamoto, 2009)

Maleabilita transakce je možnost pozměnění anoncované (tzn. dosud nepotvrzené) transakce takovým způsobem, že samotný význam jejích dat nebude pozměněn, ale rozdíl se ukáže v její binární podobě (v konkrétním podpisu vstupu), kde se změní její hash („TXID“). V případě, že by se do blockchainu dostala namísto původní transakce takováto pozměněná verze (potvrzena může být jen jedna z nich), mohl by si nevhodně navržený software (takový, který potvrzenou transakci identifikuje na základě jejího hashe a nikoliv obsahu) myslet, že k transakci vůbec nedošlo. Software se následně může pokusit transakci zopakovat uvolněním jiných bitcoinů, kterými disponuje (jiných výstupů na jím spravovaných adresách). Tím by danou platbu provedl vícekrát. Co je hlavní, mohl by si myslet, že výstupy vycházející z první pozměněné transakce má stále k dispozici. To by znamenalo potíže při vzniku budoucí transakce s touto chybou na

vstupu. Přestože je tento problém znám od roku 2011, řádně se projevil počátkem roku 2014 v souvislosti s krizí nejznámější a nejstarší bitcoinové burzy Mt.Gox, která zdůvodnila dočasné pozastavení výběru bitcoinů právě díky tomuto problému. To mělo za následek nejen pokles kurzu, ale i snížení její důvěryhodnosti. Popisovaný problém byl odstraněn ve verzi 0.8 referenčního klienta. Některé burzy (a jiné velké služby) přesto používají svůj customizovaný software.

Poplatek za transakci tvoří rozdíl mezi hodnotou výstupů a vstupů dané transakce. Výši poplatku určuje zadavatel (odesílatel) transakce. Bitcoiny, které tvoří tento rozdíl, připadnou v rámci generující transakce tomu, kdo vytěží blok, který tuto transakci zahrnuje a potvrzuje. Tyto poplatky za transakce jsou motivací k zahrnutí do těženého bloku. Právě tato teorie nám odůvodňuje, proč těžba po vytvoření všech 21 milionů bitcoinů neskončí. Další těžení už sice nebude vytvářet nové bitcoiny, ale každý těžař spolu s vytěžením bloku obdrží poplatky v daném bloku zahrnuté.

Transakce je považována za potvrzenou ve chvíli, kdy je zapsána v blockchainu („účetní knize“). Čím více je novějších bloků, než ve kterém je transakce uvedena, tím bezpečnější je pokládat ji za nevratnou. Rozdíl počtu bloků mezi aktuálně těženým blokem a blokem, který danou transakci zahrnuje, se nazývá počet potvrzení. U transakcí s větším objemem se v praxi často požaduje počet potvrzení větší nebo roven šesti.

2.7.3 Těžba a Blockchain

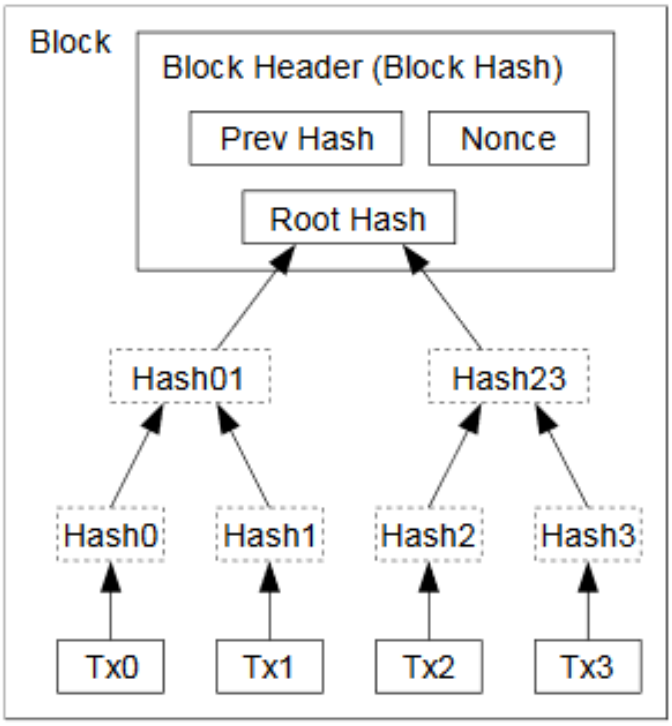
Těžba je proces výpočtů prováděných pomocí speciálních těžebních strojů, které hledají další blok, který by napojily do blockchainu. Takový blok je nalezen, pokud splňuje podmínku, že jeho hash (přesněji hash vypočtený z dat, která obsahuje) je nižší než určitý cíl (parametr „target“ – číslo začínající na mnoho nul v zápisu počtem číslic hashe). Tento cíl se odvozuje z momentální obtížnosti, která se mění každých 2016 bloků v závislosti na rychlosti jejich nalezení tak, aby průměrná rychlost generování nových bloků činila 1 blok za 10 minut. Pokud blok tuto podmínku nesplňuje, je nutné jej pozměnit (obsahuje k tomu určené pole „nonce“, které může nabývat libovolné hodnoty) a pak může hash přepočítat.

Jak už jsme si uvedli výše, v každém bloku existuje i tzv. generující transakce. Díky těmto transakcím vznikají stále nové bitcoiny. Tyto transakce jsou bez reálných vstupů. Místo nich se objevuje parametr „coinbase“, nesoucí libovolná data. Objem takovéto

transakce je roven součtu nově vygenerovaných bitcoinů a poplatků za ostatní transakce v daném bloku. Množství takto vygenerovaných nových bitcoinů je 50 BTC pro blok 0 a každých 210 tis. bloků. Zhruba každé čtyři roky se tato hodnota snižuje na polovinu. Toto exponenciální snižování má za následek omezené množství bitcoinů. Maximální množství bitcoinů je, jak jsme si již několikrát zmínili, 21 milionů (jakožto součet geometrické posloupnosti) a vzhledem k rychlosti generování bude všech 21 milionů vytěženo v roce 2140. Výstupy z generující transakce připadnou tomu, kdo daný blok vytěžil. Generující transakce může být zároveň jedinou transakcí obsaženou v bloku. Takto tomu bylo například u prvních desítek tisíc bloků.

Jedním typem útoku (problémem, se kterým se potýkali všichni, kdo chtěli vynalézt kryptoměnu před bitcoinem, a Satoshi jako jediný tento problém vyřešil) na bitcoinovou síť je dvojitá útrata. Jedná se o útok, kdy se útočník snaží použít stejné bitcoiny vícekrát (tzn. že tentýž výstup již existující transakce chce použít jako vstup pro více nových transakcí). Čím větší počet potvrzení příjemce platby požaduje, než ji uzná za provedenou, tím hůře se útok realizuje. Útočník by musel co nejrychleji vytěžit alternativní bloky, čímž by obětoval svůj výpočetní výkon k útoku, jehož nejistota úspěchu roste s počtem potvrzení, které musí svojí alternativní větví blockchainu „obejít“.

Obrázek 2: Vnitřní struktura bloku



Zdroj: (Nakamoto, 2009)

Blockchain je označován jako veřejná, decentralizovaná „účetní kniha“ Bitcoinu.[11] Jedná se o spojový seznam bloků, ve kterém každý z nich má v sobě odkaz na své předky. Tím rozumíme, že se bloky spojí v seznam takovým způsobem, že hash předchozího bloku je obsažen v bloku následujícím. Jedinou výjimkou je tzv. „Genesis block“. Takto je označován úplně první vytěžený blok, který místo hashe předka obsahoval hodnotu 0. Jelikož předek bloku je jeden, graf vztahů mezi bloky je strom, který obsahuje větve s několika málo výhonky délky jedna až dva. Ale jelikož se vždy pracuje pouze s nejdelšími, těmi, které bylo nejtěžší spočítat, jedná se o jeden lineární řetězec, který známe jako blockchain. Bloky obsažené ve větvích, které nejsou zahrnuty v řetězci, se ignorují. Naopak bloky zahrnuté v blockchainu spolu s jejich transakcí jsou považovány za potvrzené. Tento způsob tvorby a ukládání nových bloků v blockchainu zajišťuje jejich nepřepsatelnost. Pokud by někdo chtěl změnit blok uvnitř řetězce, právě kvůli vlastnosti bloku, kde každý obsahuje hash předka, musel by přepočítat všechny po něm následující. To by zároveň znamenalo, že by se nepočítalo s nejdelší větví.

Blok je nejvýznamnější datová struktura bitcoinového protokolu. Jak už bylo mnohokrát zmíněno, blok zahrnuje množinu transakcí, čímž je všechny (ty v něm zahrnuté) potvrzuje. Právě jedna transakce v bloku je označena za „generující“ a pouze díky ní vznikají nové bitcoiny. Validní blok musí mít určitou kryptografickou vlastnost, jejíž splnění je náročné na výpočetní výkon. Samotná náročnost je proměnná v čase. To umožňuje zpětnovazebnou regulaci, aby byla dosažena stabilita průměrné rychlosti generování nových bloků a tím i deterministické inflace měny. S tímto úzce souvisí termín „proof of work“. Jedná se o koncept, který nám říká, že Bitcoin je založený na důkazu o vynaložení úsilí nebo provedení práce. Těžaři dnes pomocí těžařských strojů hledají správná seskupení hashů a právě ti, kterým se to podaří jako prvním, dostávají za odvedenou práci odměnu. Zatím ještě v podobě nových bitcoinů a poplatků zahrnutých v transakcích jimi vytěženého bloku. Jiný koncept by byl například tzv. „proof of stake“.

2.8 Budoucnost Bitcoinu

Jelikož v minulém roce 2017 byla bitcoinová síť zahlcena množstvím uživatelů a transakcemi, které zasílali, potvrzování těchto transakcí trvalo v mnoha případech nejen hodiny, ale někdy se jednalo i o dny. Zároveň s nárůstem doby potvrzení narůstala i výše

[11] Záznam o všech blocích najdete např. na stránkách https://blockchain.info/

poplatku za transakce. Proto vývojáři uvažovali, jak síti ulehčit. Komunita se rozdělila na část, která přešla na novou kryptoměnu s názvem Bitcoin Cash a problém vyřešila zvětšením velikosti bloků, a druhá část, jež přišla s nápadem nazvaným SegWit (zkratka Segregated Witness). Dříve byly transakce tvořeny zároveň vstupním a výstupním scriptem. Nový druh transakcí, s použitím SegWitu, vkládá podpisová data (vstupní script) mimo samotnou transakci. Tato data se nezapisují do blockchainu, ale do vedlejší databáze. To snižuje velikost přenášených a zapisovaných dat do blockchainu, a tedy zajišťuje i nižší výši poplatku až o 75 %. Přestože již toto vylepšení funguje, je v tomto případě zařazena do budoucnosti, protože je tomu tak pouze u některých velmi málo peněženek. Do budoucna tuto aktualizaci, doufejme, zařadí více peněženek do svého fungování.

Další možné vylepšení do budoucna se nazývá Lightning Network, které bude umožňovat zapisovat transakce mimo blockchain. Dnes je, dá se říct, v testovací fázi a doufejme, že brzy toto vylepšení budou peněženky také využívat.

S teorií, co nastane, až se vytěží všech 21 milionů bitcoinů, souvisí další možný předpoklad týkající se využití těžby. V budoucnu můžeme předpokládat přísun stále více těžařů, kteří využití těžařských strojů uvidí spíše jako zdroj, vytápění bytů (díky jejich výdeji tepla), než jako výdělečnou činnost.

3 METODIKA

Pokud jste se rozhodli investovat do kryptoměny BITCOIN, je další a tím nejdůležitějším rozhodnutím, jakou peněženku budete používat pro úschovu vašich bitcoinů. Existuje několik variant, které jsou na trhu dnes dostupné a liší se v mnoha vlastnostech. Tato část práce nám představí ty nejdůležitější vlastnosti, které porovnáme pomocí metody párového porovnání. Komparace se zakládá na vlastnostech, kritériích: zabezpečení, multiměnovosti, vlastnictví klíčů, rychlosti přístupu, jazyce, aktualizacích, zpracování, velikosti, kompatibilitě s operačním systémem a na ceně. Výsledek komparace využijeme k výběru dvou peněženek, které vyhovují vedoucím kritériím. Představíme si, proč by jedna z nich měla mít přednost ve výběru a z jakých hlavních důvodů tomu tak je.

4 PRAKTICKÁ ČÁST

4.1 Komparace bitcoinových peněženek

4.1.1 Metoda párového porovnání

Vlastnosti bitcoinových peněženek, které použijeme jako kritéria (K1-K10) pro párové porovnání (jak je vidět v tabulce č. 2) si nejprve představíme.

K1 – zabezpečení – Peněženky můžeme dělit podle stavu na online, jež jsou vždy připojeny k síti, nebo offline, které je možé mít kdekoli u sebe a nejsou připojeny k internetu. Pro bezpečnost našich bitcoinů je lepší offline peněženka, do které potenciální útočník nemá možnost přístupu pomocí internetového připojení.

K2 – multiměnovost – Dnes již existují i další kryptoměny, které je třeba také uschovat v peněžence, proto se někteří vývojáři bitcoinových peněženek rozhodli rozšířit si možnosti a zpřístupnit nastavení i pro úschovu jiných kryptoměn, nejen bitcoinu. Jelikož nás ale zajímá pouze kryptoměna bitcoin, toto kritérium zřejmě nebude mít velkou váhu. Tato vlastnost některých peněženek je zde uvedena z důvodu představení základních charakteristik, ale nebude příliš ovlivňovat výsledek zkoumání.

K3 – vlastník klíčů – V teoretické části bylo již zmíněno, že existují dva druhy klíčů. Soukromý klíč by měl zůstat znám pouze vlastníkovi peněženky, pro uchování bezpečí, co se týče přístupu k peněžence a jejím transakcím. U tohoto kritéria je pro nás důležité, že jsme vlastníky soukromého klíče pouze my, a ne jiný server.

K4 – přístup – Toto kritérium je velice podobné prvnímu kritériu – zabezpečení. Liší se tím, z jakého pohledu se na něj díváme. První kritérium bylo z pohledu přístupu potencionálního útoku, zatímco zde nahlížíme na přístup nás, jako uživatelů, k vlastní peněžence a jejímu použití. Existují papírové peněženky, u kterých není možné navolit částku, jež se poté odesílá. S takovouto peněženkou je využíván pouze vytištěný QR kód a adresa peněženky. Což je zcela nepraktické, pokud je cílem odeslání transakce, za něco zaplatit, a není možné nastavit částku či poplatek, se kterým se transakce odešle. Proto tato peněženka, pokud by použitím metody párového porovnání splňovala vedoucí kritéria, nebude pak vybrána pro ukázku transakce. Tímto kritériem myslíme, že máme blízko po ruce (ať jsme kdekoliv) přístup k nastavení podrobností možných plateb.

K5 – jazyk – Peněženky jsou dostupné po celém světě, a tak je pro nás příjemnější, když je možné v nastavení peněženky nastavit jazyk, kterému rozumíme a jsme schopni tímto jazykem peněženku ovládat. Pro nás je tedy kritériem možnost nastavení češtiny.

K6 – aktualizace – S postupem času se i samotná síť Bitcoinu vyvíjí a pro nás je důležité, zda peněženka reaguje na tyto změny. Jak bylo zmíněno v teoretické části, příkladem nejnovějšího vývoje je tzv. SegWit. Pokud chceme jít s vývojem vpřed, je důležité, aby vývojáři uznávali vylepšené aktualizace. Kritérium aktualizace v tomto případě vidíme jako vlastnost peněženky, která je průběžně aktualizována a umožňuje práci s adresami podporujícími SegWit.

K7 – zpracování – Vzhled aplikace může některé začátečníky přilákat. Nedílnou součástí každé peněženky je proto také její vzhled. Nejedná se však o jedno z hlavních kritérií, které by mělo rozhodovat o výběru peněženky, což je potřeba si uvědomit při jejím výběru. Ve vybraných kritériích je zpracování peněženky jako ukázka, že na vzhledu by nemělo záležet. Až se dostaneme k výsledků párového porovnání, uvidíme, jestli tomu tak je.

K8 – velikost – Velikost, kterou by online peněženka zabírala v paměti zařízení, je třeba vzít v úvahu. Některé peněženky stahují celý blockchain, který má aktuální velikost blízkou 160 GB. Předpokládáme tedy, že bychom raději peněženku menší velikosti. Touto výhodou disponují offline peněženky, které nezabírají žádnou paměť.

K9 – kompatibilita – Jde nám o kompatibilitu s operačním systémem, kterým je naše zařízení vybaveno, bez níž by peněženku nebylo možné využívat. Toto kritérium je v některých případech výchozí pro volbu peněženky.

K10 – cena – Ne všechny na trhu dostupné peněženky jsou zdarma. Pro běžného uživatele je cena jednou z hlavních rozhodujících charakteristik a je pro něj tudíž příhodnější nižší pořizovací cena peněženky, což je pouze výchozí předpoklad, jehož výsledek nám ukáže následující zkoumání.

Výchozí předpoklady pro komparaci

Předpokládejme, že chceme vlastnit bitcoiny ve vyšší peněžní hodnotě za účelem hodlování (držení po delší dobu) a zároveň chceme začít používat bitcoin jako platební měnu v běžném životě. Tudíž, pokud chceme využívat peněženku k transakcím kdekoliv, je třeba vzít v úvahu rychlost přístupu. Jsme ochotni si pořídit zařízení, které by bylo vybaveno operačním systémem, který danou peněženku podporuje, a velikostí potřebnou k uložení peněženky. Zároveň jsme ochotni za pořízení peněženky zaplatit částku v uvážené míře (dle našich finančních možností).

Tabulka 2: Metoda párového porovnání

	K1	K2	K3	K4	K5	K6	K7k	K8	K9	K10
K1		1	1	1	1	1	1	1	1	1
K2			3	4	5	6	7	8	9	10
K3				3	3	3	3	3	3	3
K4					4	6	4	4	4	4
K5						6	5	8	9	10
K6							6	6	6	6
K7								8	9	10
K8									8	8
K9										10
K10										

Zdroj: Autor práce

V tabulce jsou jednotlivá kritéria uvedena v prvním sloupci a řádku. Všechna kritéria porovnáváme mezi sebou vzájemně. Ve zbytku tabulky je pak uvedeno pouze číslo kritéria, které je v porovnání oproti druhému důležitější.

Z tabulky vyplývá, že zabezpečení je pro nás důležitější než všechna ostatní kritéria. Pokud vlastníme nějaké peníze, je pro nás nejdůležitější, aby byly v bezpečí a nedostala se k nim žádná nežádoucí osoba. Naopak multiměnovost není nijak důležitá oproti jiným kritériím, čímž jsme si potvrdili náš předpoklad, že nás při výběru nezajímá podpora jiných kryptoměn. To, abychom byly vlastníky soukromého klíče, je důležitější než všechna kritéria kromě zabezpečení. Případ, kdy bychom nebyly vlastníky soukromého klíče, se týká hlavně webových peněženek. Pokud bychom se rozhodli nakoupit bitcoiny na burze, kde si vytvoříme právě takovouto webovou peněženku, doporučuji, co nejrychleji po nákupu poslat bitcoiny na jinou, bezpečnější peněženku. Rychlost přístupu má přednost před multiměnovostí, jazykem, zpracováním, velikostí, kompatibilitou a cenou. Peněženku si chceme pořídit, abychom mohli platit bitcoiny a tudíž k nim měli rychlý přístup. Proto jsme schopni velikost úložiště, operační systém a cenu přizpůsobit, neboť jsou oproti rychlosti přístupu méně zásadní. Peněženku jsme ochotni využívat i v jiném jazyce, než sami preferujeme, pokud předpokládáme, že defaultním jazykem je například angličtina nebo jazyk, ve kterém budeme stále rozumět pokynům nutným k použití peněženky. Podpora aktualizací je důležitější než všechna kritéria kromě zabezpečení peněženky a vlastnění soukromých klíčů. Vzhled peněženky pro nás není

nijak zásadní, a tak se objevil v tabulce pouze jednou, a to v porovnání s multiměnovostí. Jelikož chceme vlastnit bitcoinovou peněženku a nezajímají nás jiné kryptoměny, je pro nás zásadnější její vzhled, než zda-li podporuje i ostatní známé kryptoměny. Velikost, kterou peněženka zaujímá v paměti, je důležitější než multiměnovost, jazyk, její vzhled, kompatibilita nebo cena. Raději bychom si pořídili jiné zařízení, se kterým bude kompatibilní, nebo bychom za její pořízení byli ochotni zaplatit vyšší částku, než aby využívala většinu paměti a tím i zpomalovala chod zařízení. Jelikož jsme ochotni si pořídit nové zařízení, kompatibilita je přednější pouze před multiměnovostí, jazykem a vzhledem. Upřednostňujeme pořízení peněženky co nejlevnější před multiměnovostí, vzhledem a kompatibilitou.

S tabulkou a jejími výsledky dále pracujeme v následující podkapitole.

4.1.2 Výsledek párového porovnání

Porovnaná kritéria z předchozí tabulky nyní zpracujeme (výsledky jsou uvedeny v tabulce č. 3). Z celé tabulky č. 2 bylo sečteno, kolikrát se které kritérium objevilo jako důležitější. Výsledek nám tvoří absolutní četnosti. Kritériím poté dle výše četnosti určíme jejich pořadí důležitosti. Následuje váha (relativní četnost) jednotlivých kritérií. Celkem jsme kritéria porovnávali pětačtyřicetkrát, proto absolutní četnost každého kritéria bude vydělena číslem čtyřicet pět, následně vynásobena stem a zaokrouhlena na dvě desetinná místa. Získáme tak procentuální váhu každého z kritérií.

Tabulka 3: Absolutní četnost, pořadí a váha jednotlivých kritérií

	Absolutní četnost	Pořadí kritéria	Váha (relativní četnost)
K1	9	1	20 %
K2	0	10	0 %
K3	8	2	17,78 %
K4	6	4	13,33 %
K5	2	8	4,44 %
K6	7	3	15,56 %
K7	1	9	2,22 %
K8	5	5	11,11 %
K9	3	7	6,67 %
K10	4	6	8,89 %

Zdroj: Autor práce

Z tabulky č. 3 vyplývá, že svoji budoucí peněženku budeme vybírat následovně.

Nejdůležitější pro výběr peněženky bude její zabezpečení. Tzn. že upřednostníme offline peněženku před online verzí. Poté budeme dbát na to, abychom po vytvoření peněženky my sami (jedině my) vlastnili soukromý klíč. Následně je žádoucí, aby peněženka podporovala aktualizace bitcoinové sítě. Dále je potřeba, abychom měli rychlý přístup do jednoduššího zadávání transakcí pro praktické využití v terénu. Pátou vlastnost v pořadí zastává velikost, kterou peněženka zaujímá v paměti. Chceme, aby její velikost byla co nejmenší. Poté nás bude zajímat cena jejího pořízení (pokud možno co nejnižší). Až po ceně za pořízení je žádoucí dbát na to, zda je peněženka podporována operačním systémem v našem zařízení. Jazyk upřednostníme před vzhledem a multiměnovostí. V neposlední řade nás bude zajímat její vzhled, na kterém v porovnání s předchozími kritérii příliš nezáleží. A jako poslední v pořadí je možné si vybrat čistě bitcoinovou nebo multiměnovou peněženku.

Samozřejmě se tento výběr vztahuje hlavně (ale ne pouze) na typ uživatele, který jsme si upřesnili před použitím metody párového porovnání.

Tabulka 4: Vlastnosti vybraných peněženek

	Bitcoin Core	Electrum	BitAdress Paper	Blockchain	MyCelium	Coin.Space	Trezor
Typ	desktopová	desktopová	papírová	webová	mobilní	mobilní	hardwarová
verze	0.16.0	3.1.2.	3.3.0	3.43.8	2.9.11.7	2.6.1	1.5.2
K1	online	online	offline	online	online	online	offline
K2	ne	ne	ne	ano	ne	ano	ano
K3	ano	ano	ano	ne	ano	ne	ano
K4	ne	ne	ne	ano	ano	ano	ano
K5	ano	ne	ne	ne	ano	ne	ano
K6	ano	ano	ne	ne	ne	ne	ano
K8	180 GB a více	43,5 MB	0 MB	0 MB	63,91 MB	21,14 MB	0 MB
K9	Windows Mac Linux	Windows Mac Linux	papír	web	Android	Android Windows iOS	hardware
K10	zdarma	zdarma	zdarma	zdarma	zdarma	zdarma	89€[12]

Zdroj: Autor práce

Pro názornost bylo vybráno několik konkrétních peněženek, které byly porovnány v rámci zkoumaných kritérií a následně vybrána ta nejpříhodnější z nich pro předpokládaného uživatele. Výsledky vlastností peněženek jsou uvedeny v tabulce č. 4. Je zde vynechán řádek pro vzhled, neboť ten je zcela individuální a každý jedinec si ho

[12] Cena je uvedena bez DPH

porovná sám. Dvě z porovnávaných peněženek (Trezor a MyCelium) jsou využity pro ukázku odeslání a příjmu transakce v následující kapitole s názvem Využití poznatků v praxi.

4.2 Využití poznatků v praxi

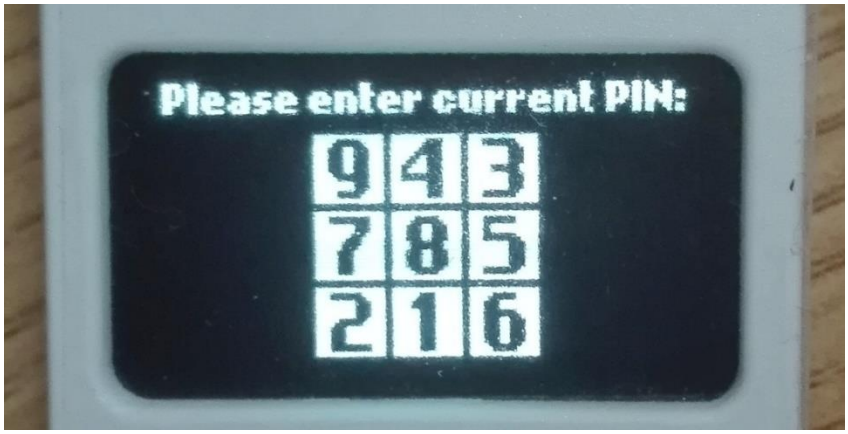
Z tabulky č. 4 v předchozí podkapitole jsou vybrány dvě peněženky, na kterých si vyzkoušíme zaslat a přijmout transakci. První přihlášení a nastavení peněženek si nebudeme představovat, protože obě peněženky pro začátečníky ukazují pokyny při prvním spuštění. Nás zajímá až následná manipulace, jak zaslat a přijmout transakci, především jak nejvhodněji nastavit poplatek odesílané transakce.

4.2.1 Trezor – příjem a odeslání transakcí

Vybranou peněženkou pro zaslání transakce je Trezor. V komparaci z předchozí podkapitoly tato peněženka, jako jediná z vybraných, nejlépe splňovala kritéria. Jakožto hardwarová peněženka je offline (můžeme si ji představit jako USB flashdisk). Je multiměnová (podporuje více kryptoměn, např. Bitcoin Cash, Bitcoin Gold, Dash, Litecoin, Zcash, Ethereum a několik dalších) a v tomto případě jsme my vlastníky soukromého klíče (respektive soukromý klíč je uložen v samotném Trezoru). Stejně tak, jako je možné ji ke flashdisku přirovnat vzhledem, je to možné i použitím. Pokud chceme manipulovat s bitcoiny uloženými v Trezoru, připojíme ho pomocí kabelu k zařízení (počítači či mobilnímu telefonu, který podporuje OTG), díky kterému s ním můžeme komunikovat a provádět transakce. Trezor podporuje český jazyk a zároveň využívá aktualizace SegWit. Jedinou nevýhodou je její cena, ale naším cílem je bezpečně uschovat bitcoiny, a tudíž jsme ochotni si za co nejbezpečnější peněženku připlatit.

Pro přístup k manipulaci s bitcoiny uloženými v Trezoru je potřeba načíst stránku https://wallet.trezor.io/ a poté připojit Trezor pomocí kabelu k zařízení. Po propojení se zobrazí tabulka (vzhledově stejná s numerickou klávesnicí, 3 x 3), na které je třeba zadat PIN kód. To provedeme následujícím způsobem. Podíváme se na Trezor, kde je zobrazena podobná klávesnice, ale číslice jsou zde v jiném pořadí (viz obrázek č. 3). V prohlížeči neuvádíme v přesném znění náš PIN kód. Vždy se musíme podívat, kde první, druhé a další číslo PIN kódu leží v tabulce na obrazovce Trezoru a podle toho je zadávat ve správném pořadí na správném místě v tabulce v prohlížeči. Tedy například by náš PIN byl 123456, v prohlížeči zadáme čísla 219863.

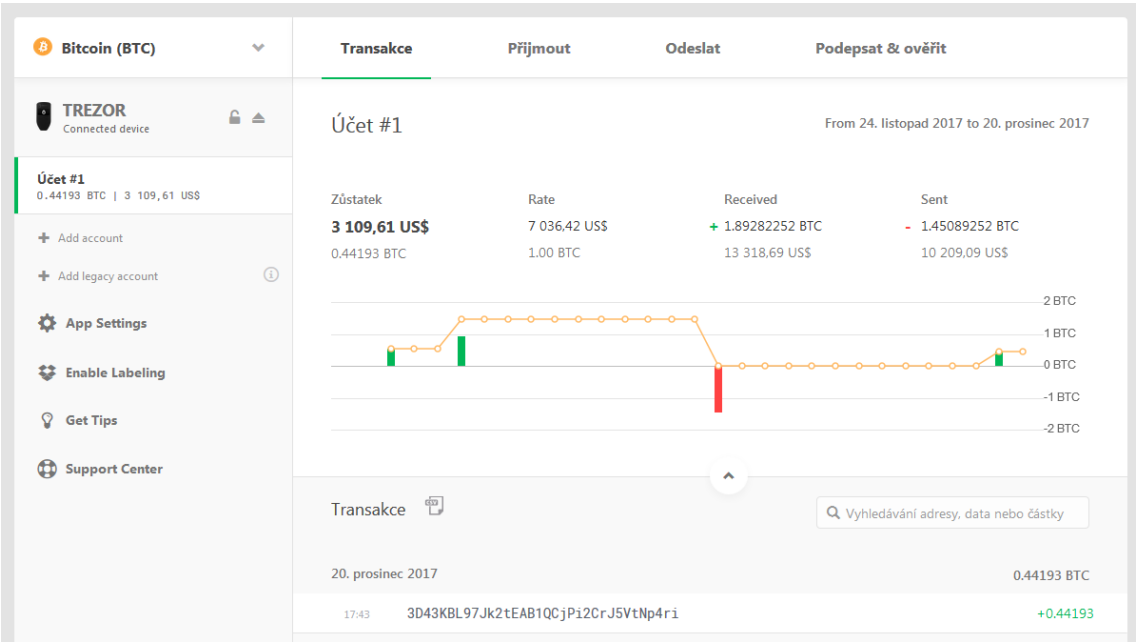
Obrázek 3: Tabulka s pomíchanými čísly



Zdroj: Autor práce

Obsah webové stránky, která se zobrazí v prohlížeči (je vidět na obrázku č. 4) po správném zadání PIN kódu, ukazuje reálný aktuální stav peněženky. V levém sloupci vidíme, že se nacházíme v bitcoinové peněžence (v Trezoru). Nachází se zde také karty pro nastavení, support center a další, které pro naší cílovou manipulaci aktuálně nejsou potřeba. Pro účet s názvem „Účet #1" se v pravé části v záložce Transakce vyobrazí graf, na kterém je možné vidět pohyb transakcí tohoto účtu v čase. Nad grafem je zůstatek uvedený v BTC a námi zvolené měně (v tomto případě se jedná o americký dolar) při aktuálním kurzu, který se zobrazuje napravo od zůstatku. Také se zobrazí celková hodnota doručených a odeslaných transakcí od první do poslední změny na účtu. Pod grafem se poté nacházejí všechny proběhlé transakce zvlášť rozepsané.

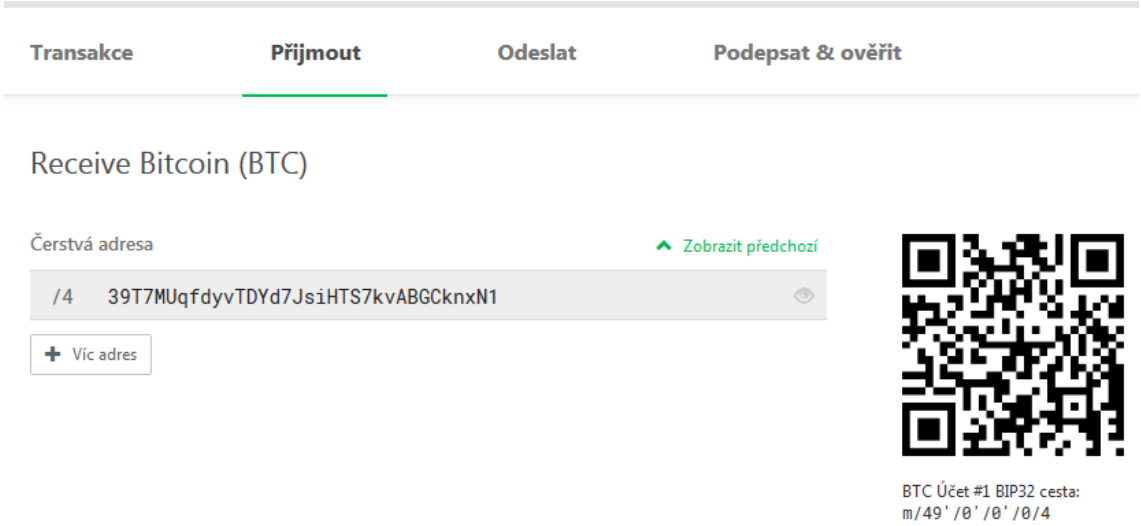
Obrázek 4: Vstupní stránka Trezoru



Zdroj: Autor práce

Přesuneme se do záložky Přijmout (viz obrázek č. 5), která se nachází napravo od záložky Transakce. Zde je vidět QR kód a tzv. čerstvá adresa, na které je možné přijmout transakci z jiné adresy. Tady prokazatelně vidíme, že se jedná o adresu, která podporuje SegWit (první značkou je zde číslo 3).

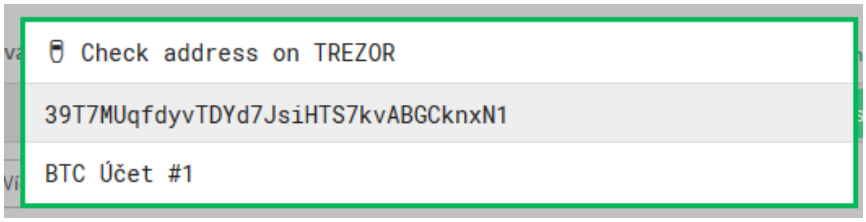
Obrázek 5: Vzhled záložky Přijmout



Zdroj: Autor práce

Tuto adresu je možné zkopírovat do schránky a zaslat možnému odesílateli transakce nebo si ji může, tak jak ji vidí (pokud je nadosah, my mu ji samozřejmě ukážeme), opsat ručně do svého zařízení, kam zadává transakci. Pokud bychom adresu otevřeli, zobrazí se notifikace pro kontrolu adresy (viz obrázek č. 6).

Obrázek 6: Notifikace pro kontrolu adresy v prohlížeči

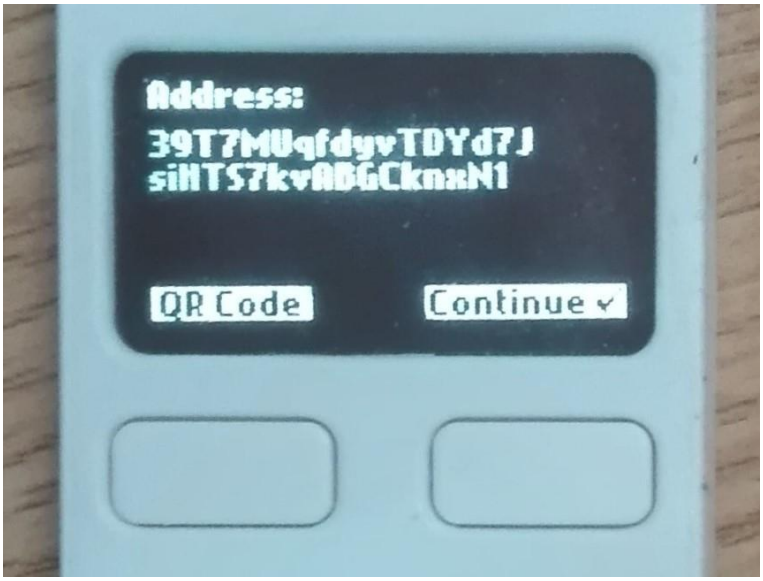


Zdroj: Autor práce

Podobná notifikace se zobrazí také na Trezoru (viz obrázek č. 7), kam nás první notifikace odkazuje. Abychom mohli dále pracovat, je potřeba potvrdit, zda jsou adresy uvedené v obou notifikacích totožné.

Tuto kontrolu potvrdíme zmáčknutím pravého tlačítka na Trezoru (značí potvrzení a pokračování). Pokud bychom chtěli vidět QR kód (například aby si ho mohl ten, kdo bude posílat transakci nám, naskenovat), stiskli bychom levé tlačítko, které nám QR kód zpřístupní podobně jako nyní adresu.

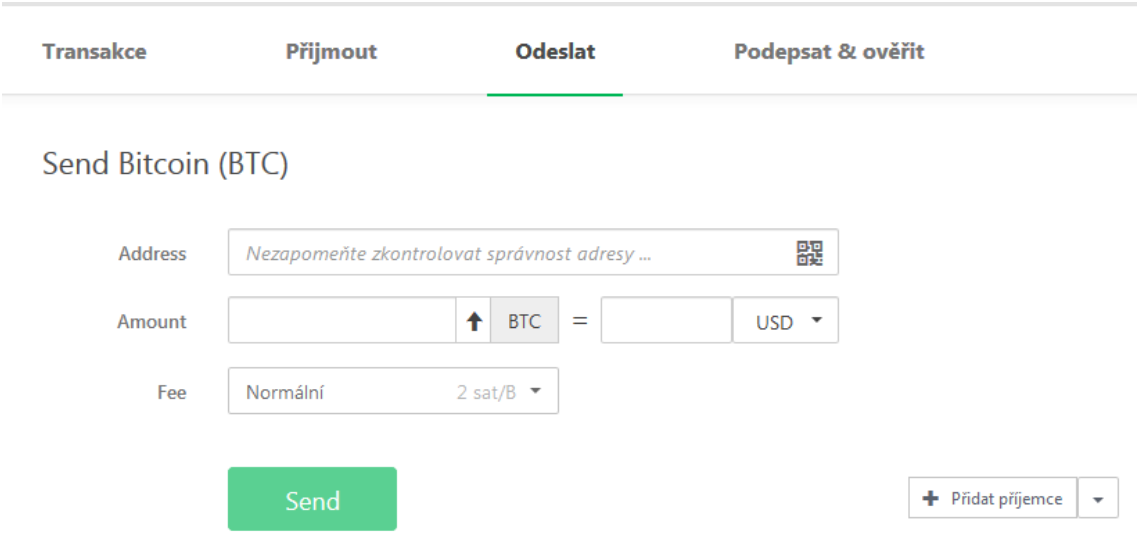
Obrázek 7: Notifikace pro kontrolu adresy v Trezoru



Zdroj: Autor práce

Pro odeslání transakce z Trezoru se přesuneme do záložky Odeslat (viz obrázek č. 8), která se nachází napravo od předchozí záložky Přijmout. Zde vidíme pole pro zadání potřebných informací, která jsou třeba vyplnit, abychom mohli transakci zaslat.

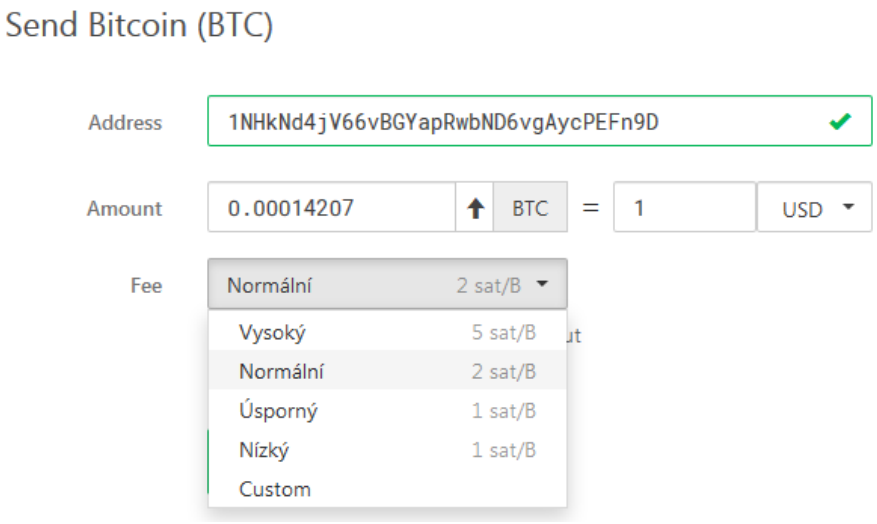
Obrázek 8: Vzhled záložky Odeslat



Zdroj: Autor práce

Do pole adresy příjemce zadáme adresu v celém znění. V našem případě byla zadána adresa mobilní peněženky MyCellium, která nepodporuje SegWit. Částku můžeme zadat buďto v BTC nebo naopak v jiné měně, kterou sami vybereme. Pro tuto ukázku byl zvolen jeden americký dolar, který budeme posílat. Je důležité nastavit správný poplatek (viz obrázek č. 9), podle toho, kdy chceme, aby byla transakce potvrzena.

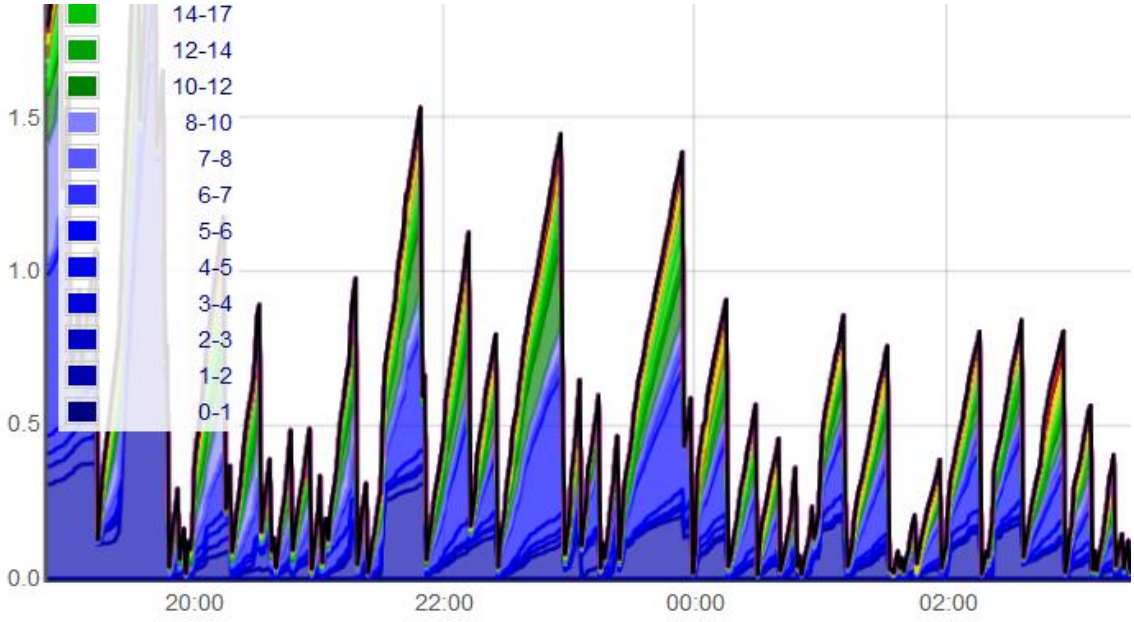
Obrázek 9: Možnosti nastavení poplatků



Zdroj: Autor práce

Jak ale takový poplatek zvolit, abychom ho nenastavili vyšší, než je potřeba, ale abychom ušetřili. Jednou z možností je nahlížet do tzv. mempoolu (zkratka pro memory pool), který nalezneme například na adrese https://jochen-hoenicke.de/queue/#1,24h, na níž nás zajímá především poslední graf (příklad je na obrázek č. 10), se kterým budeme pracovat. Všechny odeslané transakce, které čekají na potvrzení, se totiž řadí do fronty od transakce s nejvyšším poplatkem po ten nejnižší. Jakmile se vytěží další blok, těžaři v něm zahrnou transakce ze začátku fronty. Poslední na řadu tedy přijdou transakce s nejnižším poplatkem. Do bloků se vejde přibližně stejné množství dat (asi 1 MB) a ne transakcí.

Obrázek 10: Výřez grafu mempoolu



Zdroj: Autor práce

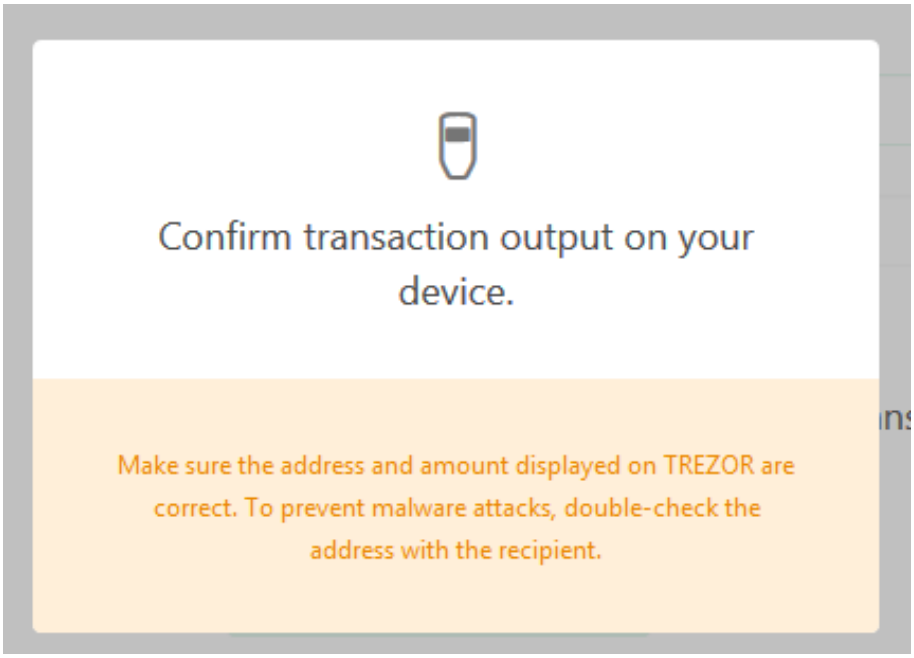
Graf (na obrázku č. 10) uvádí množství MB, které mempool aktuálně obsahuje. Na ose X je vyobrazen čas a na ose Y jsou uvedeny MB. Graf je barevně odlišen podle výše poplatků (sat/B), které pro odeslané transakce byly vybrány. Nás tedy zajímá, v jaké výši je třeba zvolit poplatek, aby byl zahrnut v prvním bloku (pokud trváme na zapsání transakce v co nejbližší době), tzn. abychom se s vybraným poplatkem vešli v grafu nejlépe pod 1 MB. Kdybychom tedy zasílali transakci a v předchozích hodinách mempool vypadal stejně jako na obrázku č. 10, s největší pravděpodobností bychom se vešli do prvního bloku, i kdybychom poplatek nastavili na nižší než 1 sat/B. Naopak zpětně vidíme, že pokud bychom zasílali transakci v době chvíli před půlnocí, bylo by potřeba poplatek nastavit minimálně na výši 6 sat/B, aby se transakce s největší pravděpodobností vešla do prvního vytěženého bloku. Pokud ale na potvrzení nespěcháme, nezáleží na výši poplatku, nabízí se nejběžnější normální, úsporný nebo nízký poplatek.

Protože v době, kdy byla transakce připravena k odeslání, jsme z příslušného grafu vyčetli, že aby byla transakce zahrnuta v prvním bloku, je třeba výši poplatku nastavit na minimálně 2 sat/B, poplatek je tedy nastaven na normální, což představuje právě 2 sat/B.

Všechna pole jsou již vyplněna, a tudíž vybereme tlačítko send (odeslat).

V tento okamžik se zobrazí notifikace (viz obrázek č. 11), která nás upozorňuje, že je potřeba informace o transakci potvrdit na Trezoru. Zároveň nás informuje, že je nutné informace potvrdit dvakrát, abychom zabránili možným malwarovým útokům.

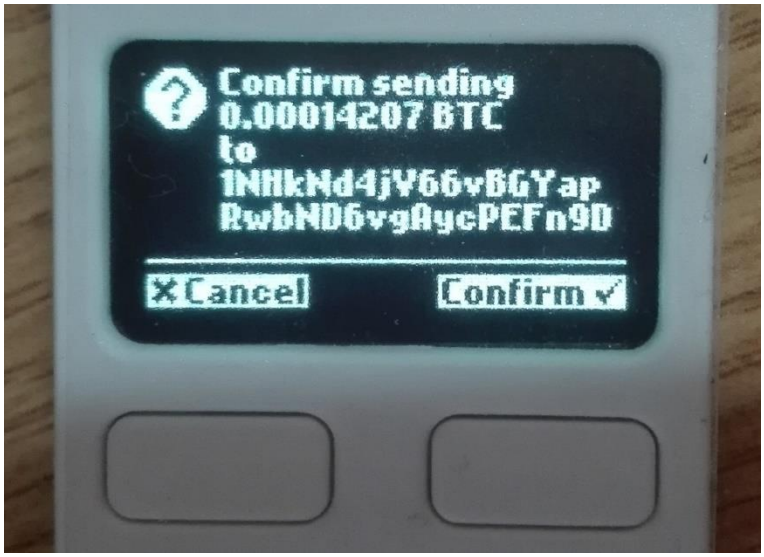
Obrázek 11: Notifikace pro potvrzení odchozí transakce v prohlížeči



Zdroj: Autor práce

Na obrázku č. 12 se zobrazí na Trezoru první notifikace k potvrzení, která informuje o výši částky k odeslání a zároveň nám říká, na jakou adresu bude částka zaslána. Pokud souhlasíme s informacemi zde uvedenými, pak notifikaci potvrdíme pravým tlačítkem.

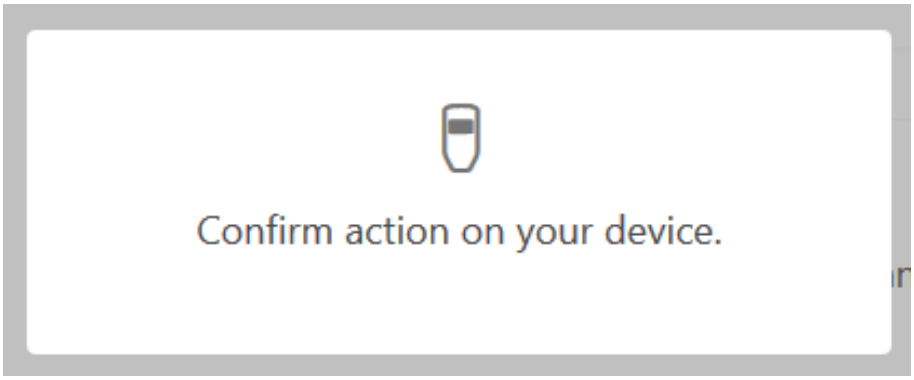
Obrázek 12: Notifikace pro potvrzení odchozí transakce v Trezoru



Zdroj: Autor práce

Následně se notifikace v prohlížeči změní (viz obrázek č. 13) a oznamuje, že je potřeba potvrdit novou akci na Trezoru.

Obrázek 13: Druhá notifikace pro potvrzení odchozí transakce v prohlížeči



Zdroj: Autor práce

Na obrazovce Trezoru nyní vidíme nové informace o transakci. Trezor se nás ptá, zda chceme zaslat právě takovouto částku s poplatkem, který je pod částkou vyobrazen.

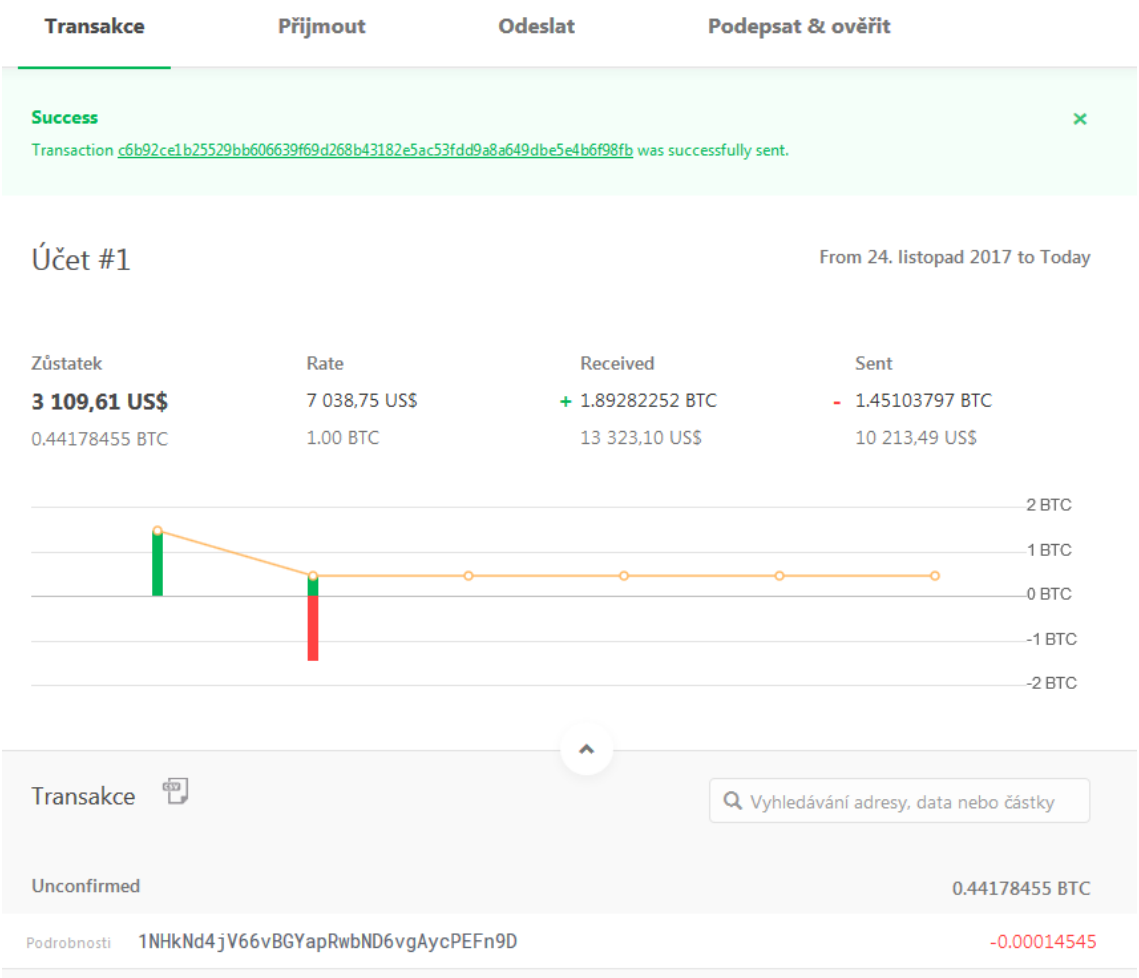
Opět tuto notifikaci potvrdíme pravým tlačítkem, což je poslední krok k odeslání transakce.

Obrázek 14: Druhá notifikace pro potvrzení odchozí transakce v Trezoru

Zdroj: Autor práce

V tento okamžik (7. 4. 2018 v čase 19:26:53) je transakce odeslána a pravá část obrazovky prohlížeče (viz obrázek č. 15) nás informuje notifikací o úspěšném odeslání transakce s uvedením jejího kódu. Pod grafem přibyla v seznamu tato nová transakce, která ještě není potvrzena (není zahrnuta v blockchainu). Pokud rozklikneme kód transakce, budeme přesměrováni na stránku (viz obrázek č. 16) s podrobnými informacemi o provedené transakci.

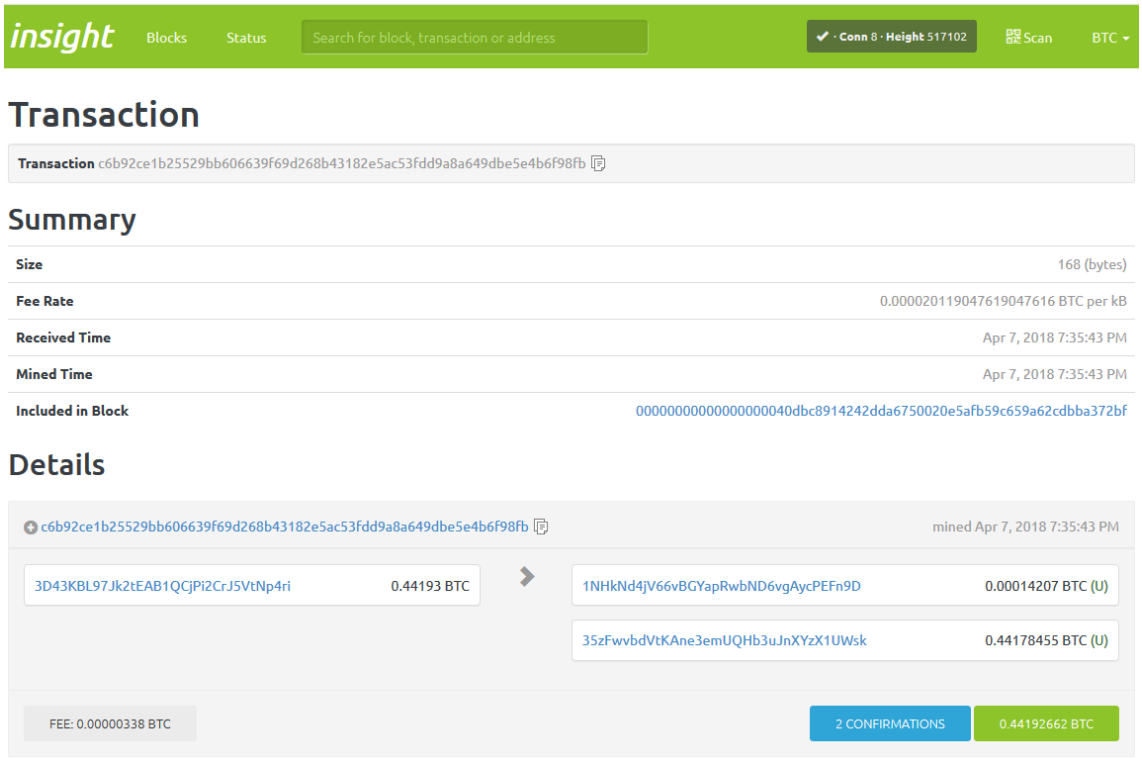
Obrázek 15: Transakce proběhla úspěšně



Zdroj: Autor práce

Zde (na obrázku č. 16) je uveden nejen kód naší transakce, ale také velikost, kterou zaujímá v bytech. Vidíme, že poplatek byl nastavený v dostačující výši a transakce byla do devíti minut (19:26:53 až 19:35:43) zahrnuta v bloku (jeho číslo je zde také uvedeno) a zapsána v blockchainu. Ve spodní části je pak vlevo zobrazeno, z jaké adresy byla transakce zaslána, a vpravo cílová adresa zasílané částky a nová adresa, kde zůstal zbytek bitcoinů po zaslání (ten samý účet v Trezoru, pouze s jinou adresou).

Obrázek 16: Podrobnosti o transakci



Zdroj: Autor práce

4.2.2 MyCelium – příjem transakcí

Druhá vybraná peněženka je mobilní peněženka MyCelium, která v komparaci z předchozí kapitoly sice nevyšla jako druhá nejlepší pro náš výběr, ale můžeme si na ní ukázat rozdíl týkající se výše poplatku, jelikož nevyužívá SegWitu. Po otevření aplikace v mobilním telefonu zadáme PIN kód v přesném znění šesti cifer. Pokud tak učiníme a kód je správný, zobrazí se nám vstupní obrazovka MyCelia, kterou vidíme na obrázku č. 17. Zde je vidět, že název účtu je také „Účet 1“ jako u Trezoru, vidíme tzv. čerstvou adresu, na které je možné přijmout transakci z jiné adresy, a QR kód. Následující informace je zůstatek uvedený v BTC a námi zvolené měně (v tomto případě se jedná o českou korunu) při aktuálním kurzu, který se zobrazuje pod tlačítky dle zdroje směnového kurzu, který je možný zvolit v nastavení aplikace. Aktuálně je nastaven Bitstamp. Prvními tlačítky jsou zde Odeslat, Fotoaparát a Přijmout. Tlačítko Odeslat bychom použili pro zaslání transakce, ale tato ukázka není součástí práce (bude však zmíněna při obhajobě). Fotoaparát bychom použili podobně jako tlačítko pro odeslání, ale už bychom nemuseli nastavovat cílovou adresu, popřípadě částku k odeslání, protože fotoaparátem bychom naskenovali QR kód cílové adresy (jedná se o možnost v cílové peněžence

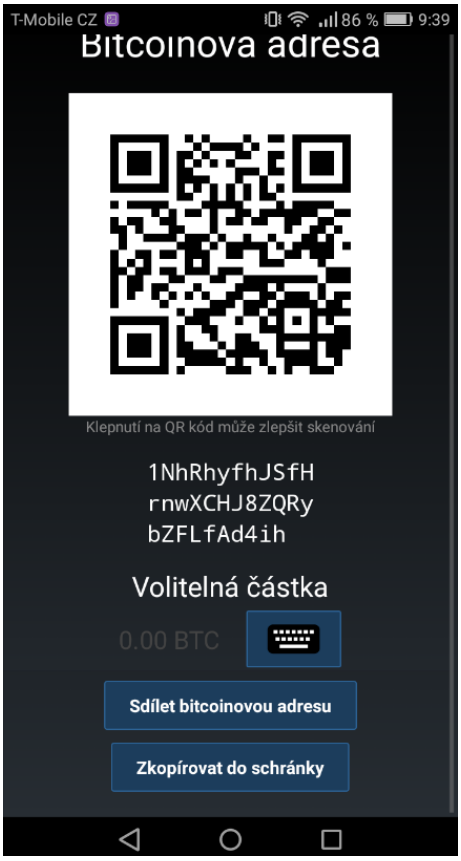
nastavit i částku k přijetí, tím pádem se QR kód změní a my můžeme naskenovat obě tyto informace najednou). Zmáčknutím tlačítka Přijmout se zobrazí zvětšený QR kód a bitcoinová adresa. (viz obrázek č. 18)

Obrázek 17: Vstupní obrazovka MyCelia

Zdroj: Autor práce

Adresu je možné přímo z aplikace sdílet nebo zkopírovat do schránky a zaslat možnému odesílateli transakce nebo si ji může, tak jak ji vidí, opsat ručně do svého zařízení, kam zadává transakci. Pokud ale odesílatel stojí vedle nás, je nejjednodušší zadat volitelnou částku, načež se QR kód změní a je v něm uložená informace nejen o naší adrese pro zaslání ale také částka, kterou odesílatel poté nemusí zadávat do svojí peněženky. My jsme předchozí adresu (na obrázku č. 17 je uvedena čerstvá adresa po přijetí transakce) zkopírovali a zaslali odesílateli (vlastníkovi Trezoru), který ji poté vložil do pole adresy příjemce v prohlížeči (viz obrázek č. 9).

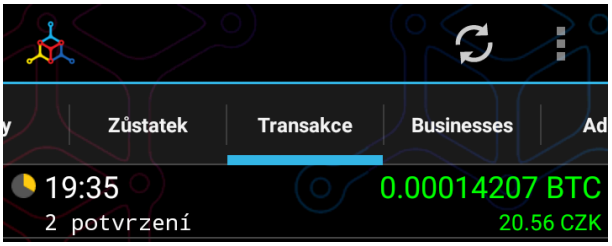
Obrázek 18: Bitcoinová adresa



Zdroj: Autor práce

Počkali jsme, až odesílatel vyplní potřebné informace a potvrdí odeslání transakce. Brzy poté jsme se přesunuli v naší peněžence do záložky Transakce (viz obrázek č. 19), kde se o devět minut poté objevila přijatá transakce, která po dvaceti minutách měla již dvě potvrzení (tzn. za blokem, v němž je transakce zahrnuta, přibyly již další dva).

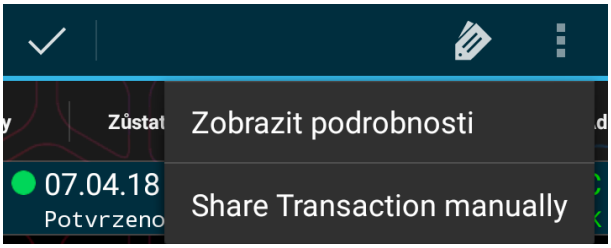
Obrázek 19: Přijatá transakce



Zdroj: Autor práce

Pokud bychom chtěli v naší peněžence MyCelium zobrazit podrobnosti dané transakce (jak přijaté, tak potvrzené), nejprve tuto transakci vybereme a poté v pravém horním rohu zvolíme tříbodové tlačítko, které nám nabízí možnosti (viz obrázek č. 20). Následovně klikneme na Zobrazení podrobností a objeví se důležité informace o transakci (na obrázku č. 21).

Obrázek 20: Možnosti vybrané transakce



Zdroj: Autor práce

Zde vidíme ID přijaté transakce z Trezoru, která byla potvrzena v bloku č. 517101. Údaje na obrázku č. 21 jsou ze čtvrtého dne po obdržení transakce, abychom také viděli, že počet potvrzení přibývá a po čtyřech dnech jich je již 630. Dále je v podrobnostech uveden datum a čas zahrnutí transakce do daného bloku, její vstupní a zároveň obě výstupní adresy. Jako příjemci je nám také umožněno vidět výši poplatku.

Obrázek 21: Podrobnosti transakce

Zdroj: Autor práce

5 ZÁVĚR

Teoretická část práce byla věnována historii, současnosti a budoucnosti kryptoměny zvané Bitcoin. Byly vysvětleny zásadní souvislosti vzniku a používání měny.

Praktická část byla zaměřena na způsob výběru vhodné peněženky pro budoucí uživatele této měny. Pro výzkum byla použita metoda párového porovnání deseti vybraných kritérií, abychom zjistili, v jakém pořadí kritérií nejlépe vybírat naší budoucí peněženku pro nejbezpečnější uschování a manipulaci s bitcoiny. Následně bylo sečteno, kolikrát se v metodě daná kritéria vyskytují (tedy jejich absolutní četnost) a vypočtena váha jednotlivých kritérií (tedy relativní četnost), načež jsme mohli kritéria seřadit do pořadí od 1 (nejdůležitějšího kritéria) do 10 (to nejméně důležité). Bylo zjištěno toto výsledné pořadí kritérií (od nejdůležitějšího po nejméně důležité): zabezpečení, vlastnictví klíčů, aktualizace, rychlost přístupu, velikost, cena, kompatibilita s operačním systémem, jazyk, zpracování a multiměnovost. Byla vytvořena tabulka, která obsahovala celkem sedm možných peněženek výběru a jejich vlastnosti podle vybraných kritérií. Na základě této tabulky byla vybrána hardwarová peněženka Trezor, která jako jediná nejlépe splňovala požadavky vyplývající z použití metody párového porovnání. Na této peněžence bylo příkladně ukázáno, jak se v peněžence orientovat, a především jakým způsobem lze přijmout a odeslat transakci z Trezoru. Při odesílání transakce je vždy potřeba nastavit její poplatek. V praktické části je tedy také uvedeno, jakým způsobem vybrat výši daného poplatku (abychom nenastavili poplatek za vyšší částku, než je potřeba). Po ukázce zaslání transakce bylo představeno, jak v druhé vybrané peněžence MyCelium transakci přijmout. Peněženka MyCelium byla vybrána pro ukázku rozdílu, co se týče kritéria aktualizací. Trezor představuje peněženku podporující SegWit, tedy poplatky jsou zde nižší, a naopak MyCelium, která SegWit nepodporuje, obsahuje nastavení vyšších poplatků.

Autorka si sama vyzkoušela využít obě dvě vybrané peněženky a postup transakcí zaznamenala v této bakalářské práci. Výsledkem práce je tudíž zhodnocení podstatnosti jednotlivých kritérií pro výběr bitcoinové peněženky, její následné využití při porovnání několika běžně dostupných peněženek a názorný příklad odeslání a přijmutí transakce dvou různých peněženek s vysvětlením podstatných rozdílů.

6 SUMMARY AND KEYWORDS

The aim of this thesis is to familiarize the reader with the problematics of the theoretical background of cryptocurrencies from the historical perspective, focusing on the concepts of B-money and Bit gold, which were the basis for the creation of Bitcoin. The main part is devoted to this decentralized cryptocurrency called Bitcoin. It itroduces Bitcoin‘s main milestones, the Bitcoin Foundation, the functioning system itself, and eventually Bitcoin's prospects for the future.

The aim of the second part of this thesis is to develop a simple and clear system for selecting a wallet as the storage of bitcoins. What should be decided by a person who considers holding his own bitcoins. Here is used a compairing method of selected criteria. Criteria are compared based on the prerequisite that the priority for selection is mainly the bitcoin wallet. For the idea of how this wallet looks and works, the practical part also includes a sample of two selected wallets, based on the comparison of the criteria, and the transfer of one dollar between them. The aim of this bachelor thesis is to process the comparation of selection procedur for use by ordinary users.

Keywords

bitcoin (BTC), Cryptocurrency, digital currency, Satoshi Nakamoto, wallet, transaction, adress, mining, block, blockchain, Trezor

7 SEZNAM POUŽITÝCH ZDROJŮ

Be a BITCOIN Millionaire: Beginner to master [Online]. Prometheus MMS. Retrieved from https://books.google.cz/books?id=Jjw4DAAAQBAJ&printsec=frontcover&dq=inauthor:%22Prometheus+MMS%22&hl=cs&sa=X&ved=0ahUKEwiZs8f75p7aAhXQyaYKHRFYA0QQ6AEIKDAA#v=onepage&q&f=false

Biggs, J. (2013) Techcrunch.com: Who Is The Real Satoshi Nakamoto? One Researcher May Have Found The Answer. TechCrunch [Online]. Retrieved January 29, 2018, from https://techcrunch.com/2013/12/05/who-is-the-real-satoshi-nakamoto-one-researcher-may-have-found-the-answer/

Bitcoinmagazine.com. (2013) The Two Bitcoin Conferences of 2013 [Online]. Retrieved March 22, 2018 from https://bitcoinmagazine.com/articles/the-two-bitcoin-conferences-of-2013-1357866416/

Bitcointalk.org. (2010) Bitcointalk.org: Pizza for bitcoins? [Online]. Retrieved February 09, 2018, from https://bitcointalk.org/index.php?topic=137.msg1195#msg1195

Bitcointalk.org. (2010) Bitcointalk.org: [2.5+ EH] Slush Pool (slushpool.com); World's First Mining Pool [Online]. Retrieved February 09, 2018, from https://bitcointalk.org/index.php?topic=1976

Bitcointalk.org. (2010) Bitcointalk.org: Car for Sale – Australia [Online]. Retrieved February 09, 2018, from https://bitcointalk.org/index.php?topic=3485.0

Bitcointalk.org. (2011) Bitcointalk.org: Bitcoin Conference 2011 NYC [Online]. Retrieved March 22, 2018 from https://bitcointalk.org/index.php?topic=6150.0

Bitcointalk.org. (2012) Bitcointalk.org: Earliest Block With A Spend [Online]. Retrieved February 09, 2018, from https://bitcointalk.org/index.php?topic=91806.msg1012234#msg1012234

Bitcointalk.org. (2012). Bitcointalk.org: How did Satoshi register bitcoin.org? [Online]. Retrieved February 08, 2018, from https://bitcointalk.org/index.php?topic=103369.msg1135218#msg1135218

Bitcointalk.org. (2012) Bitcointalk.org: Historical Price Data for 2009 [Online]. Retrieved February 09, 2018, from https://bitcointalk.org/index.php?topic=104287.msg1143955#msg1143955

BitcoinWiki. (2010) BitcoinWiki: Category:History [Online]. Retrieved February 09, 2018, from https://en.bitcoin.it/wiki/Category:History

BitcoinWiki. (2016) BitcoinWiki: Bit gold proposal [Online]. Retrieved January 29, 2018, from https://en.bitcoin.it/wiki/Bit_Gold_proposal

Blockexplorer.com: Genesis block [Online]. Retrieved February 09, 2018, from http://www.blockexplorer.com/b/0

B-money. (2016) BitcoinWiki: B-money [Online]. Retrieved January 28, 2018, from https://en.bitcoin.it/wiki/B-money

Foundation. (2018) Become a member – Bitcoin Foundation [Online]. Retrieved March 22, 2018 from https://bitcoinfoundation.org/membership/

Groups.google.com. (2011) Groups.google.com: NFC initiated Bitcoin payments with Bitcoin Wallet for Android – Skupiny Google [Online]. Retrieved March 08, 2018 from https://groups.google.com/forum/#!topic/bitcoinj/HFKFhMY31bs

Hill, K. (2013) The FBI's Plan For The Millions Worth Of Bitcoins Seized From Silk Road Retrieved February 09, 2018, from https://www.forbes.com/sites/kashmirhill/2013/10/04/fbi-silk-road-bitcoin-seizure/#3be551a22848

Kasík, Pavel. (2018) Investice do budoucnosti, dušují se politici. Česko má vlastní kryptoměnu [Online]. Retrieved March 22, 2018, from https://technet.idnes.cz/ceska-

oficialni-kryptomena-bitcoin-alternativa-f57-
/sw_internet.aspx?c=A180321_192937_sw_internet_pka

Matonis, Jon. (2012) Bitcoin Foundation Launches To Drive Bitcoin's Advancement [Online]. Retrieved March 22, 2018 from https://www.forbes.com/sites/jonmatonis/2012/09/27/bitcoin-foundation-launches-to-drive-bitcoins-advancement/#17d19532d868

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System* [Online]. (2009). Retrieved from https://bitcoin.org/bitcoin.pdf

Popper, N. (2015) The New York Times: Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin [Online]. Retrieved January 29, 2018, from https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html

Richtopia. (2016) List of Top 100 Blockchain Organisations by Influence [Online]. Retrieved March 22, 2018 from http://richtopia.com/top-lists/top-100-blockchain

Stroukal, D., & Skalický, J. (2015). *Bitcoin: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha.

Stroukal, D., & Skalický, J. (2018). *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky* (2., rozšířené vydání). Praha: Grada Publishing.

Szabo, N. (2005) Satoshi Nakamoto Institute: Bit Gold [Online]. Retrieved January 29, 2018, from http://nakamotoinstitute.org/bit-gold/

8 SEZNAM OBRÁZKŮ

Obrázek 1: Interní generování adres při transakcích
Obrázek 2: Vnitřní struktura bloku
Obrázek 3: Tabulka s pomíchanými čísly
Obrázek 4: Vstupní stránka Trezoru
Obrázek 5: Vzhled záložky Přijmout
Obrázek 6: Notifikace pro kontrolu adresy v prohlížeči
Obrázek 7: Notifikace pro kontrolu adresy v Trezoru
Obrázek 8: Vzhled záložky Odeslat
Obrázek 9: Možnosti nastavení poplatků
Obrázek 10: Výřez grafu mempoolu
Obrázek 11: Notifikace pro potvrzení odchozí transakce v prohlížeči
Obrázek 12: Notifikace pro potvrzení odchozí transakce v Trezoru
Obrázek 13: Druhá notifikace pro potvrzení odchozí transakce v prohlížeči
Obrázek 14: Druhá notifikace pro potvrzení odchozí transakce v Trezoru
Obrázek 15: Transakce proběhla úspěšně
Obrázek 16: Podrobnosti o transakci
Obrázek 17: Vstupní obrazovka MyCelia
Obrázek 18: Bitcoinová adresa
Obrázek 19: Přijatá transakce
Obrázek 20: Možnosti vybrané transakce
Obrázek 21: Podrobnosti transakce

9 SEZNAM TABULEK

Tabulka 1: Dělitelnost bitcoinu

Tabulka 2: Metoda párového porovnání

Tabulka 3: Absolutní četnost, pořadí a váha jednotlivých kritérií

Tabulka 4: Vlastnosti vybraných peněženek