Univerzita Pardubice
Fakulta ekonomicko-správní

Problematika bezpečnosti v oblasti kryptoměn

Aleš Pour

Bakalářská práce
2019

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Aleš Pour**
Osobní číslo:	**E16938**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Problematika bezpečnosti v oblasti kryptoměn**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je popsat problematiku bezpečnosti se zaměřením na oblast kryptoměn.

Osnova:
- Seznámení s kryptoměnami a jejich historie.
- Legislativa v oblasti kryptoměn v ČR a ve světě.
- Problematiky těžby kryptoměn.
- Platby a nákup pomocí kryptoměn.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN: 978-80-271-0742-1.
HOSP, Julian. Kryptomeny: Bitcoin, Ethereum, Blockchain, ICO&Co. jednoducho a zrozumiteľne. 1. Tatran, 2018. ISBN 978-80-222-0945-8.
ANTONOPOULOS, A. M. Mastering bitcoin: unlocking digital cryptocurrencies. Sebastopol, CA: O'Reilly, 2015. ISBN 978-1-449-37404-4
VIGNA, P. a M. CASEY. The age of cryptocurrency: how bitcoin and digital money are challenging the global economic order. New York: St. Martin's Press, 2015. ISBN 978-1-250-06563-6

Vedoucí bakalářské práce: **Ing. Jan Panuš, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **3. září 2018**

Termín odevzdání bakalářské práce: **30. dubna 2019**

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. září 2018

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne Aleš Pour

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu této bakalářské práce Ing. Janu Panušovi, Ph.D. za cenné rady a připomínky, které mi napomohly k vypracování práce.

ANOTACE

Práce bude sloužit k popisu fungování kryptoměn, jejich algoritmech a principech, bezpečnosti a bezpečnostními mechanismy s nimi spjatými. Dále pak k seznámení s ilegálními aktivitami, se kterými jsou kryptoměny spojovány.

KLÍČOVÁ SLOVA

kryptoměny, bezpečnost, bitcoin, blockchain

TITLE

Security issues in cryptocurrencies

ANNOTATION

This thesis will serve for better understanding of cryptocurrency function, algorithm, principals, security and security mechanisms, and for introduction of illegal activities, that cryptocurrencies are associated with.

KEYWORDS

cryptocurrency, security. bitcoin, blockchain

OBSAH

1 ÚVOD

Kryptoměny se v posledních letech dostávají mezi širokou veřejnost, jak bylo možné vidět na konci roku 2017 při obrovské „kryptománii“. Od té doby se o krytoměny a svět kolem nich zajímá čím dál více lidí. Zkrátka už to není jen téma pro IT nadšence a geeky.

V bakalářské práci na téma problematika bezpečnosti v oblasti kryptoměn bych chtěl popsat základní fungování a mechanismy kryptoměn. Na jakém principu kryptoměny staví, jaké se využívají algoritmy a jaké jsou základní kameny celého systému jako jsou kryptografie, technologie fenoménu zvaného blockchain nebo decentralizovaný systém.

Nemalá část práce je věnována kryptoměnám samotným, a to konkrétně zejména Bitcoinu, který je považován za vůbec první decentralizovanou kryptoměnu. V práci jsou ale zmíněny i kryptoměny další jako je na příklad Ethereum, Litecoin nebo Ripple.

Dále se v práci zabývám, jak kryptoměny získat a co všechno to obnáší. Uživatel má na výběr několik možností, jak kryptoměny získat, ať už to je nákupem v různých směnárnách, burzách nebo v bitcoinovém bankomatu. Nebo si kryptoměny vytěží sám, pomocí osobního počítače, či speciální techniky k tomu vytvořené.

Uživatel má také na výběr, jestli zůstane anonymní či nikoliv. Tomuto a okolnostem s tím spojeným jsem v této práci věnoval také pozornost.

Největší část práce je však věnována bezpečnosti kryptoměn, a to přechovávání a skladování. V práci jsou nastíněny základní možnosti ochrany a je zde vysvětleno na jakých principech fungují, a jak jsou tyto možnosti bezpečné. Na to navazuje několik bezpečnostních mechanismů, které mají za úkol zvýšit bezpečnost onoho skladování anebo zvýšení bezpečnosti transakcí.

Kryptoměny se na první pohled mohou zdát jako nástroj k ilegálním aktivitám. Tomuto tématu a skutečnostem s tím spojeným, jako jsou například ilegální tržiště, která nejsou dostupná z běžného viditelného internetu, jsem se zde věnoval také.

2 KRYPTOLOGIE

Kryptologie pochází z řeckého výrazu kryptós, což znamená skrytý. Je to věda zabývající se kryptografií a kryptoanalýzou. Tedy o metodách utajování, skrývání významu zpráv, které jsou čitelné nebo zobrazitelné pouze díky specifickým znalostem, a o metodách „luštění“ neboli rozkrývání takto zašifrovaných zpráv. (Hub, 2013, s.45)

2.1 KRYPTOGRAFIE

Kryptografie je matematická disciplína zabývající se převodem zpráv z utajené nebo do utajené podoby. Tedy nějaký otevřený text, který je zašifrován do textu nesrozumitelného, který případný útočník nemůže nijak zneužít. Naopak oprávněný uživatel se správným dešifrovacím klíčem může zprávu převést do původní podoby. Šifrovat však lze nejen otevřený text, ale jakákoliv data, jako jsou například video záznamy, zvukové stopy nebo obrázky.

K rozluštění zprávy je třeba znát klíč, který by měl vlastnit oprávněný uživatel. Rozlišujeme kryptografii symetrickou a asymetrickou.

V symetrické kryptografii se pro šifrování používá stejný klíč jako pro dešifrování. Tedy jedna strana zvolí šifrovací klíč a předá klíč straně druhé. Následně odesílatel zašifruje zprávu pomocí daného klíče, který mají obě strany stejný, a odešle straně druhé. Po přijetí zašifrované zprávy druhá strana použije kód pro dešifrování. Tím získá původní text. Takto lze komunikovat i na stranu druhou.

Mezi nejznámější symetrické šifry patří například Caesarova šifra, která funguje na principu posouvání pozic písmen abecedy. Klíčem je pak číslo o kolik je abeceda posunuta. (Hub, 2013, s.47)

Asymetrické algoritmy používají jiný klíč pro šifrování než pro dešifrování. Klíč, který se používá pro šifrování se nazývá veřejný klíč a klíč určený pro dešifrování se nazývá soukromý klíč. Tyto klíče musí být navzájem neodvoditelné. Soukromý klíč pak musí být tajný, může k němu mít přístup pouze vlastník.

Odesílatel vytvoří zprávu, kterou chce odeslat straně druhé. Zašifruje ji veřejným klíčem příjemce a vytvořenou zašifrovanou zprávu zašle příjemci. Příjemce pak použije svůj soukromý klíč k dešifrování zprávy a tím získá původní text. Pro komunikaci jsou tedy třeba dva páry klíčů.

Mezi výhody asymetrického algoritmu patří, že veřejné klíče mohou být dostupné všem, není tedy třeba rozesílat klíče nikomu. (Hub, 2013, s.49-50)

Asymetrický algoritmus se v praxi využívá například k elektronickému podpisu. Vlastník při podepisování zprávy podpis spočítá pomocí jeho soukromého klíče, což může učinit jen on sám. Následně si pak každý může ověřit, zda je podpis opravdu původního majitele pomocí jeho veřejného klíče. (Stroukal, 2018, s.114)

2.2 KRYPTOMĚNY

Kryptoměna je druh digitální měny nebo elektronických peněz na síti zvané blockchain. který se zpravidla programuje do kryptografického algoritmu. Mezi nejznámější kryptoměny se řadí například Bitcoin nebo Ethereum.

Každá kryptoměna je utvořena na decentralizované síti. Uživatelům této sítě je umožněno převádět tokeny jiným uživatelům, ale i nakupovat nebo prodávat zboží na internetu, a mnoho dalšího.

2.3 CENTRALIZACE A DECENTRALIZACE

Centralizace znamená, že něco spravuje jedna centrální instituce, například vláda nebo centrální banka. Centralizovaný systém má tedy nějaký centrální bod, který zodpovídá za chod onoho centralizovaného systému. Při selhání centrálního bodu může dojít k pádu celého systému, což může mít v některých případech katastrofální následky.

Naopak decentralizovaný systém je absolutně otevřený a přístupný téměř kdykoliv. Má předem stanovená pravidla, kterými se musí každý uživatel řídit. Decentralizovaný systém tedy není závislý, na rozdíl od centralizovaného, na žádné centrální instituci. Jedná se většinou o P2P síť, kde si jsou všichni uživatelé rovni a správa sítě je mezi ně rozprostřena.

Decentralizovnaou síť využívá valná většina kryptoměn. To v praxi znamená, že kryptoměny nespravují žádné centrální instituce a prakticky je nelze regulovat. Tato síť se nazývá blockchain.

P2P, tedy peer-to-peer je označení typu počítačových sítí, kde jsou všechny uzly na stejné úrovni, tedy jsou rovnocenné a jednotliví uživatelé spolu komunikují bez jakéhokoliv prostředníka, či centrálního uzlu, na rozdíl od rozhraní klient-server.

U spojení klient-server z pravidla platí, čím více uživatelů je do sítě připojeno, tím je rychlost přenosu pomalejší. U peer-to-peer spojení je tomu právě naopak. Čím více lidí je propojeno do peer-to-peer, tím je přenos dat rychlejší.

Typickým příkladem jsou tzv. torrenty, přes které mohou uživatelé sdílet data, které buď mohou stahovat, ale i poskytovat ostatním uživatelům. (Stroukal, 2018, s.24)

2.4 BLOCKCHAIN

Blockchain je strukturovaný, vzájemně propojený seznam transakcí (blocků). Můžeme ji také nazvat jako decentralizovaná účetní kniha, ve které jsou zaznamenány veškeré transakce. Může být zobrazen jako jednoduchá databáze nebo jako textový soubor.

Každý block je identifikován svou hash funkcí. Hash je definován použitím cryptografického algoritmu. Hash je zobrazení délky množiny dat obecné délky, do délky dat omezené. S tím souvisí pojem zvaný hash rate, který udává míru výpočetního výkonu, tedy počet pokusů o nalezení správného řešení na vytěžení blocku. (Stroukal, 2018, s.84-85, Hosp, 2018, s.65)

Všechny blocky také odkazují na svůj předešlý block, známý jako rodičovský. Tato informace je obsažena v hlavičce každého blocku. První block blockchainu je nazýván „genesis block“. (Hosp, 2018, s.38)

3 BITCOIN

Bitcoin je soubor technologií, které spolu tvoří základy digitální měny. Je to decentralizovaná P2P síť, spravující historii platebních transakcí mezi svými uzly. Jednotky této měny, nazývané bitcoiny jsou využívány pro ukládání a převod hodnoty právě po své P2P síti. Bitcoin využívá hashovací algoritmus SHA-256. (Antonopoulos, 2015, s.1, Stroukal, 2018, s.20)

3.1 SATOSHI NAKAMOTO

Bitcoin byl vytvořen v roce 2008 anonymním vývojářem, který se prezentuje pod pseudonymem Satoshi Nakamoto. Dodnes se netuší, kdo se pod daným pseudonymem schovává. Sám Satoshi o sobě tvrdil, že mu bylo 34 let, a že pochází z Japonska. To se však zdá velmi nepravděpodobné z důvodu jeho perfektní angličtiny a absence jakéhokoliv japonského slova v konverzacích na fórech. Naopak se zdá velmi pravděpodobné, že Satoshi pochází z anglicky mluvící země, nejspíše pak z Velké Británie, jelikož několikrát chybně použil americký dialekt.

Existují dokonce spekulace, že pod pseudonymem Satoshi Nakamoto se skrývá celá skupina odborníků na kryptografii, informatiku a ekonomii, jelikož se zdá být nepravděpodobné, že by samotný člověk dokázal vyvinout takto sofistikovanou technologii. (Stroukal, 2018, s.24)

Podle výpočtů vlastní Satoshi 1-2 miliony bitcoinů v hodnotě několika miliard amerických dolarů. Jde o několik adres, ve kterých jsou bitcoiny rozloženy. (Hosp, 2018, s.121)

3.2 VZNIK

Satoshi Nakamoto pracoval na Bitcoinu, podle jeho tvrzení, od roku 2007. Oficiálně ho pak představil v roce 2008 ve white paperu a krátce po tom zaregistroval doménu bitcoin.org.

Následující odstavec je ukázka white paperu Bitcoinu. White paper se používá k představení nějakého produktu, technologie nebo služby.

„Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence

of events witnessed, but proof that it came from the largest pool of CPU power." (Nakamoto, 2009)

První block vytěžil Satoshi sám a to 3. ledna 2009. Tomuto blocku s názvem 00000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f se později začalo říkat Genesis block. (Stroukal, 2018, s.37)

Za vytěžení prvního blocku dostal Nakamoto odměnu 50 BTC, které byly připsány na adresu 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. V současné chvíli je na této adrese 65.44021956 BTC. (TheOpenLedger, 2015)

Satoshi pevně zafixoval zásobu (supply) měny na 21 milionů bitcoinů (přesně je to tedy 20 999 999,9769 BTC). Z toho tedy plyne, že bitcoinů je omezené množství. Po vytěžení všech 21 milionů bitcoinů už nebude možné vytěžit ani jeden nový. Stát by se tak mělo v roce 2140. (Stroukal, 2018, s.37)

Jelikož je bitconů omezené množství, dá se čekat, že jeho cena s časem poroste. Bylo by tedy nemožné platit celým jedním Bitcoinem a z toho důvodu jsou odvozené jeho menší jednotky. mBTC (milibitcoin = 0,001BTC), μBTC (mikrobitcoin = 10^{-6} BTC) a satoshi (0,01 μBTC = 10^{-8} BTC). Jednotka satoshi je nejmenší dělitelnost bitcoinu.

3.3 FORK

Fork je změna pravidel fungování sítě, která představuje nějakou novou funkci Bitcoinu. Po takovéto změně je možno generovat nové, pozměněné blocky. Pokud tedy všichni těžaři, uzly a uživatelé přejdou na nový SW, nenastane žádná změna.

Problém nastane tehdy, když se změnou všichni nesouhlasí a odmítnou přejít na novou verzi. Pokud tato změna je navržena tak, že je kompatibilní s verzí starou, přejdou na nový SW pouze těžaři. Takováto změna se nazývá softfork.

Pokud však je navržena změna protokolu, která není zpětně kompatibilní, nazýváme ji hardfork. Uživatelé, kteří nepřejdou na verzi novou nemohou síť dále využívat. Těžaři, kteří zůstanou na starší verzi sítě generují blocky staré, nad posledním blockem před hardforkem. Výsledkem hardforku může být rozdělení blockchainu. Příklady hardforku Bitcoinu jsou Bitcoin Cash Bitcoin SV, Bitcoin Gold nebo například Bitcoin Diamond. (Stroukal, 2018, s.125-128)

3.3.1 Bitcoin Cash

Bitcoin Cash, zkráceně BCH, je tedy výsledkem hardforku Bitcoinu, který se stal 1. srpna roku 2017. Důvodem tohoto forku byl SegWit, který Bitcoin nepřijal, na rozdíl od BCH z důvodu jiných požadavků na těžbu. Ačkoliv se to nepředpokládalo, Bitcoin Cach se drží v top desítce největších kryptoměn z pohledu market kapitalizace. (Hosp. 2018, s.123-124).

3.4 Cena

Na obrázku č.1 je zobrazena cena BTC k americkému dolaru za poslední dva roky. Můžeme si všimnout, že cena bitcoinu je extrémně volatilní. Například kolem června 2017 se pohybovala cena za jeden bitcoin kolem dvou a půl tisíc dolarů, na konci roku, tedy o půl roku později se cena vyšplhala na neuvěřitelných dvacet tisíc amerických dolarů. Což je přibližně desetinásobné zvýšení ceny jen za tak krátkou dobu.

Obrázek 1 Cena bitcoinu *Zdroj: Kurzy.cz*

4 ALTCOIN

Existují ale ještě jiné kryptoměny než jen Bitcoin, nazývají se altcoiny. Tedy alternativní coiny k bitcoinu, jelikož bitcoin je považován za hlavní kryptoměnu. Tyto altcoiny jsou povětšinou jen přepracovanou verzí Bitcoinu, nebo jiných coinů.

Na webové stránce coinmarketcap.com se v současné chvíli (březen 2019) nachází přes dva tisíce různých kryptoměn. Většina těchto měn nestojí ani za zmínku, jelikož díky open-source kódu bitcoinu si svou kryptoměnu mohl vytvořit takřka každý, tak většina těchto měn postrádá jakýkoliv smysl. (Stroukal, 2018, s.142)

Příkladem může být Trump-coin nebo Putin-Coin, jejichž market kapitalizace nepřesahuje ani 150 tisíc amerických dolarů, což je v porovnání s hlavními měnami, které se pohybují v řádech desítek miliard USD, absolutně zanedbatelné. (Coinmarketcap, 2019)

4.1 LITECOIN

Litecoin je vůbec nejznámějším derivátem Bitcoinu. Je považován za jeho „mladšího bratra“. Je znám pod zkratkou LTC, jeho jednotky jsou litecoiny. Autorem je Charlie Lee, který je bývalý zaměstnanec Googlu. Vytvořil Litecoin v roce 2011 tím, že snížil mining difficulty (náročnost těžby) Bitcoinu na 2,5 minuty na block a zvýšil maximální možný počet vytěžených litecoinů na čtyřnásobek, tedy na 84 milionů. (Hosp, 2018)

Díky své rychlosti transakcí a nižším poplatkům se zpočátku Litecoin používal spíše pro mikroplatby. V současné době však mnoho obchodníků berou LTC jako alternativu k BTC. (Stroukal, 2018, s.149)

Následující odstavec je popis Litecoinu z oficiálního webu litecoin.org.

„Litecoin je peer-to-peer internetová měna, která poskytuje okamžité platby komukoliv na světě za téměř nulovou cenu. Litecoin je open source globální platební síť, která je plně decentralizovaná a bez jakýchkoli centrálních autorit. Matematika zabezpečuje síť a umožňuje jednotlivcům kontrolovat své vlastní finance. Litecoin poskytuje rychlejší potvrzení transakcí a vylepšuje efektivitu ukládání oproti vedoucí internetové měně. Se značnou podporou průmyslu, objemu obchodu a likvidity, je Litecoin osvědčený obchodní prostředek, který doplňuje Bitcoin.“ (Litecoin, 2019)

4.2 ETHEREUM

Ethereum je Turingově úplná platforma založená na blockchainu, sloužící ke zpracování takzvaných „chytrých kontraktů“ (smart contracts). Blockchain Etherea se považuje jako

blockchain druhé generace díky svým rozšířeným funkcím. Oproti Bitcoinu, jehož síť je využívána jako distribuce měny, Ethereum využívá svou síť jako globální decentralizovaný virtuální počítač označovaný jako Ethereum Virtual Machine (EVM).

Ethereum vytvořil ruský programátor Vitalik Buterin koncem roku 2013, ve svých devatenácti letech. U zrodu stál nápad využití blockchainu nejen jako měny, ale jako decentralizovaného počítače. (Antonopoulos, 2015, s.229, Hosp, 2018, s.124-126, Stroukal, 2018, s.161)

Ethereum využívá měnu zvanou Ether. Prostřednictvím měny Ether platí uživatelé za těžařům za běh jejich aplikací. Jeho deriváty, tedy menší jednotky jsou pojmenovány podle spoluzakladatelů, a to: attoether = wei (Wei Dai), microether = szabo (Nick Szabo), miliether = finney (Hal Finney). Měna je nekonečně inflační, nemá tedy na rozdíl od Bitcoinu omezené množství. (Stroukal, 2018, s.161)

Na Ethereum Virtual Machine běží řada tokenů. Tyto tokeny v současnosti tvoří hlavní využití EVM. Jsou označovány jako ERC20 (Ethereum Request for Commentc No.20). Definuje je šest funkcí: 1) celkový počet tokenů, 2) kolik tokenů je přiděleno jedné adrese, 3) odkud se tokeny převedou, 4) kam se tokeny převedou, 5) zda je něco dovolené nebo ne, 6) zda je povolena další dodatečná funkce. (Hosp, 2018, s.127)

Mezi nejznámější ERC20 tokeny patří například: Binance Coin (BNB), OmiseGO (OMG), 0x (ZRX), Agur (REP) nebo například Golem (GNT). Celkem je těchto tokenů přes tisíc, to znamená, že téměř polovina měn z coinmarketcap.com jsou ERC20 tokeny. (Eidoo, 2019)

4.3 RIPPLE

Ripple, známý pod zkratkou XRP je spíše real-timový platební a zúčtovací systém než příklad klasické kryptoměny. (Stroukal, 2018, s.146) Cílem bylo vytvořit systém, kde si uživatelé mohou vytvářet a vyměňovat vlastní peníze a dluhy. Transakce se nepotvrzují těžbou, ale shodou důvěryhodných uzlů, tzv. proof-of-correctness. Coiny XRP se netěží, Ripple při svém vzniku vytvořil fixní počet coinů a to 100 miliard XRP. Jednotky XRP jsou dělitelné na šest dekadických řádů. (Stroukal, 2018, s.146) Ripple je využíván hlavně v bankovním sektoru, kde nabízí bankám spolehlivou platformu, s možností plateb v různých měnách. Ripple uvádí, že jejich síť je schopná utáhnout 1500 transakcí za sekundu. (Ripple, 2019)

5 JAK ZÍSKAT KRYPTOMĚNY

Pokud se tedy uživatel rozhodne si nějakou kryptoměnu pořídit, má několik možností. Nejjednodušší cestou k pořízení kryptoměny jsou takzvané bitcoinové bankomaty někdy jsou nazývány zkráceně bitcoinmaty. Uživateli stačí mít mobilní aplikaci nebo vytisknutý QR kód své peněženky, který pak načte v bankomatu. Bankomat pak přečte tuto adresu a zjistí kam coiny poslat. Do bankomatu se pak vloží bankovky, nebo uživatel zaplatí platební kartou, ty se pak následně převedou na danou měnu podle aktuálního kurzu a odešlou na již načtenou adresu. Nevýhodou těchto bankomatů bývá vyšší kurz, než ve skutečnosti je. V praxi to znamená, že pokud uživatel zakoupí coiny za určitou částku, do jeho krypto peněženky mu přijdou coiny v hodnotě nižší v řádech až do desítek procent.

Tyto bankomaty fungují většinou obousměrně. Princip je podobný jako při nakupování. Bankomat vygeneruje QR kód, který uživatel naskenuje svým telefonem a odešle coiny na adresu bankomatu, a ten mu následně vydá peníze v hotovosti. (Stroukal, 2018, s.75-76)

„Předpokladem (podmínkou) nákupu nebo prodeje virtuální měny prostřednictvím služby Bitcoinmat je dosažení věku 18 let Klientem. Provozovatel umožňuje v souladu s platnou legislativou České republiky provedení nákupu nebo prodeje virtuální měny bez nutnosti osobní identifikace za hotovost. Maximální výše nákupu nebo prodeje bez nutnosti osobní identifikace je ke dni vydání těchto Obchodních podmínek 25 000 Kč.“ (WBTCb.cz, 2017)

Z výňatku z obchodních podmínek společnosti wBTCb.cz s.r.o. provozující desítky bitcoinmatů v České republice jasně plyne, že není nutná osobní identifikace při transakci nepřevyšující 25 000Kč. To znamená, že nákup měn přes některé bitcoinové bankomaty mohou být úplně anonymní.

V současné chvíli se v České republice nachází kolem třech desítek bitcoin bankomatů. Nabízejí kromě Bitcoinu také některé atlernativní měny jako je například Litecoin nebo Ethereum. (Coinmap, 2019)

5.1 SMĚNÁRNY

Další možností nákupu jsou internetové směnárny specializující se na kryptoměny. Příkladem takové směnárny může být coinbase.com nebo simplecoin.eu. Tyto směnárny nabízejí uživateli nákup v řádu až desítek různých coinů. Uživatel však musí být registrován a identifikován podle občanského průkazu. Tyto směnárny nabízejí velmi příjemné uživatelské rozhraní. Nákup kryptoměn tam zvládne téměř každý během pár kliknutí. Lze nakupovat coiny i za minimální částky, avšak s malými částkami jsou spojené vysoké poplatky.

Směnárny poskytují ve většině případů možnost platby bankovním převodem nebo platební kartou. Právě platební kartou je transakce dokončena během pár vteřin a uživatel může své coiny okamžitě užívat.

Nevýhodou jsou opět, jako již v předchozích bankomatech, vyšší kurzy měn nebo poplatky spojené s transakcí, na kterých směnárna vydělává. Poplatky s tímto spojené se pohybují kolem 5 %. (Stroukal, 2018, s.77-78)

5.1.1 COINBASE

Coinbase je americká směnárna se sídlem v San Franciscu v Kalifornii, založená v roce 2012. V současné chvíli (březen 2019) nabízí k obchodování deset kryptoměn, které lze měnit za eura, libry, americké dolary a za bitcoin. Se svými dvaceti miliony uživatelských účtů je jednou z největších světových směnáren. Uživatel si může nabít peněžní prostředky pomocí platební karty nebo pomocí bankovního převodu SEPA nebo IBAN. S nákupem coinů pomocí platební karty je však spojen poplatek 3,99 % z celkové částky. Při SEPA a IBAN platbách uživatel odešle fiat peníze na svůj coinbase účet a za ty pak nakoupí kryptoměnu. Nevýhodou však je, že Coinbase nepodporuje platby v CZK. Uživatel si tedy musí zaslat prostředky v směnárnou podporované měně. Rozdíl mezi nákupem a prodejem coinů se pohybuje okolo 1 %.

Coinbase nabízí také mobilní aplikaci, díky které může uživatel nakupovat kryptoměny přímo v mobilním telefonu pomocí platební karty. (Coinbase, 2019)

Společnost Coinbase vlastní nejen směnárnu, ale i burzu zvanou Coinbase Pro. Tato burza působí jako ostatní burzy, avšak má omezené množství svých coinů. Celkem obsahuje kolem 20 obchodovatelných párů. Největší výhodou této burzy, že poskytuje limit order, tedy nabídku, kterou zadá prodávající nebo kupující uživatel do order book (lze přeložit jako knihu objednávek), a tato nabídka uživatele nestojí nic. Coinbase Pro tak poskytuje uživateli obchodování s limit order bez jakýchkoliv poplatků. Není však zaručeno, že se tato nabídka vyplní. K tomu je potřeba, aby tuto nabídku nějaký jiný prodávající koupil, popřípadě prodal. Uživatelům jsou také umožněny market buy/sell, které zaručují instantní nákup nebo prodej za cenu mezi poptávkou a nabídkou. Je k tomu však započten manipulační poplatek pohybující se kolem 3 %. (InvestPlus, 2018)

5.1.2 SIMPLECOIN

Směnárna simplecoin.eu, pod společností Simple Coin s.r.o. je česká směnárna kryptoměn působící od roku 2013. Nabízí nákup a prodej BTC, LTC, BCH, ETH a XRP. Simplecoin neobsahuje žádné transakční poplatky, na úkor tomu je kurz méně výhodný. Rozdíl mezi prodejem a nákupem coinů se pohybuje okolo 6 %. Jelikož se jedná o českou směnárnu, podporuje nejen platby v CZK, ale i v EUR nebo PLN.

Minimální velikost transakce na SimpleCoin je 0,03 BTC při nákupu a 0,01 BTC při prodeji.

Směnárna požaduje identifikaci pomocí osobního dokladu při přesáhnutí částky 1000 EUR viz Registrace a verifikace Klienta.

„V. Registrace a verifikace Klienta

1. *Klient může provést objednávku nákupu či prodeje Digitální měny bez registrace nebo s registrací.*
2. *Možnost provedení objednávky bez registrace je limitována souhrnem hodnoty objednávek Klienta, který nesmí překročit částku ve výši 1.000 EUR za období jednoho (1) měsíce.*
3. *Dosáhne-li souhrn hodnoty objednávek Klienta za období jednoho (1) měsíce částku ve výši 1.000 EUR, je Klient oprávněn provést další objednávku pouze s registrací.“* (Simplecoin.cz, 2018)

Při překročení částky 1000 euro je klient povinen prokázat svou totožnost vyplněním formuláře a poskytnutím kopie dokladů totožnosti viz Identifikace Klienta.

„Identifikace Klienta

Identifikace Klienta se provádí v souladu s ustanovením § 8 AMLZ následovně:

při identifikaci Klienta, který je fyzickou osobou, Provozovatel identifikační údaje zaznamená a ověří z průkazu totožnosti, jsou-li v něm uvedeny, a dále zaznamená druh a číslo průkazu totožnosti, stát, popřípadě orgán, který jej vydal, a dobu jeho platnosti; současně ověří shodu podoby s vyobrazením v průkazu totožnosti;“ (Simplecoin.cz, 2018)

5.2 BURZY

Další formou získání kryptoměn jsou specializované internetové burzy. Tyto burzy nabízejí desítky až stovky různých coinů. Příkladem mohou být bitstamp.com, bittrex.com, kraken.com nebo třeba gdax.com. Uživatelské rozhraní těchto burz není zpravidla jednoduché. Jejich weby obsahují stovek kryptoměn v kombinaci s BTC, USD nebo třeba EUR. Poplatky na těchto

burzách jsou většinou za transakci. To znamená, že pokud uživatel nakupuje ETH/BTC, tedy chce koupit měnu ethereum za bitcoin, zaplatí malou částku za transakci burze. Například u burzy bittrex.com jsou to 2 % z transakceTyto směnárny jsou určeny převážně zkušeným traderům. . (Stroukal, 2018, s.78-80)

Příkladem může být burza Binance. Je to jedna z největších kryptoměnových burz současnosti. Byla založena v roce 2017, jejím zakladatelem je Changpeng Zhao a sídlí na Maltě. Binance poskytuje uživatelům obchodování s více jak 150 kryptoměnami. Zatím však neumožňuje směnu kryptoměn s fiat penězi. (Binance, 2019) Rozhraní Binance se může zdát ne příliš uživatelsky přívětivé, jelikož se na jejich platformě vyskytuje obrovské množství coinů a jednotlivých párů, které lze zobchodovat. Burza Binance rovněž podporuje většinu operačních systémů jako je macOS, Windows, Android, iOS, pro které má vyvinutý software, na kterém může uživatel obchodovat. Lze ale obchodovat i přes webový prohlížeč. (Binance, 2019)

Burza také vydala svůj vlastní token nazývaný Binance coin (BNB). Jedná se o token, který běží na blockchainu Etherea, je to tedy jeden z ERC20 tokenů. V současné chvíli se drží na sedmé pozici v celkové market kapitalizaci s přibližně 2,8 mld USD. (Binance coin, 2019)

5.3 TĚŽBA

Existuje však další způsob, jak získat kryptoměny, a tím je těžba. Může nás napadnout otázka, proč kupovat drahé kryptoměny za dolary či eura, když jdou „jednoduše“ vytěžit. Avšak není to tak jednoduché, jak se na první pohled může zdát. S tím je spojena řada pojmů, o kterých bude řeč dále.

Při těžbě kryptoměn nevzniká kryptoměna samotná, i přes to, že se navyšuje money supply (celková zásoba) měny, jak si většina lidí může myslet. Těžba kryptoměny je postup, při kterém v decentralizovaném systému vzniká konsenzus.

Konsenzus znamená souhlas o tom, co se stalo a co nestalo v decentralizovaném systému. Právě v decentralizovaném systému o konsensu rozhoduje komunita, na rozdíl od systému centralizovaného, kde rozhoduje centrální instituce. (Hosp, 2018, s. 52)

Těžaři potvrzují nové transakce a zaznamenávají je na global ledger, zjednodušeně je zapisují do fronty čekající na potvrzení. Transakce se potvrdí tím, že bude součástí vytěženého blocku, který bude zapsán na blockchain. (Antonopoulos, 2015, s.173)

Block je datová struktura blockchainu. Obsahuje množinu transakcí, které při svém obsažení potvrzuje. Právě jedna z transakcí obsažená v blocku je generující a tímto vznikají nové coiny. (Stroukal, 2018, s.37)

Existují většinou tři typy účastníků, a těmi jsou, uživatelé, uzly a těžaři.

Uživatelé (Users) se nestarají o nic jiného než o přijímání a odesílání transakcí. Do této skupiny patří většina účastníků. Tito uživatelé platí poplatek za těžbu známý jako mining-fee.

Uzly dostávají informace od ostatních uživatelů a uzlů, které kontrolují a zasílají dále. Navíc ukládají celý blockchain, aby zaručili plnou decentralizaci.

Těžaři kontrolují a ověřují transakce, realizované uživateli a vytvářejí konsensus. (Hosp, 2018, s. 52-53)

Těžbu coinů si lze představit jako řešení složitých matematických operací. Avšak záleží na tom, kolik coinů je v oběhu a kolik těžařů se snaží operace řešit. Princip funguje tak, že čím více coinů je vytěženo a čím více těžařů těží, tím menší odměnu uživatel dostane. Toto se značí jako náročnost sítě. Zpočátku nebyla náročnost téměř žádná. Sám Nakamoto vytěžil prvních 50 bitcoinů téměř okamžitě, ale to bylo z toho důvodu, že byl na síti sám, náročnost sítě tedy nebyla žádná, a bitcoinů bylo vytěženo nula. Postupem času se však náročnost sítě zvyšovala natolik, že bylo téměř nemožné vytěžit nějaké coiny na osobním počítači. (Stroukal, 2018, s.82-83) Prakticky by to tedy možné bylo. Těžit kryptoměny lze dnes téměř na všech zařízeních, bylo by to ale velmi neefektivní v porovnáním se spotřebou energie. (Antonopoulos, 2015, s.207, Stroukal, 2018, s.85).

Těžba na osobním počítači přes klasický počítačový procesor, nazývaná jako CPU těžba, se v současnosti nevyplácí vůbec. Osobní počítač dosáhne hodnoty hash rate kolem 1-3 milionů za sekundu, tedy 1-3 MH/s. (Hosp, 2018, s.65)

Trochu efektivnější je pak těžba pomocí grafických karet, tedy GPU těžba, které dosahují hash rate kolem 3-5 MH/s. Tato těžba se využívá například u Etherea. Těžení Bitcoinu by stále nebylo efektivní. (Hosp, 2018, s.65-66)

Z toho důvodu začaly vznikat počítače specializované na těžbu kryptoměn. Říká se tomu ASIC těžba. Tyto počítače dokáží vyvinout výkon v řádech giga až tera hashů. Příkladem společnosti, která vyrábí specializované počítače je společnost Bitmain. Je to čínská firma sídlící v Pekingu, založená v roce 2013. Specializuje se na výrobu technologií podporující těžení kryptoměn, blockchainu a umělé inteligence. (Bitmain, 2019)

Společnost Bitmain byla dlouho na světové špičce ve výrobě zařízeních určených na těžbu kryptoměn Antminer. Mezi jejich první produkty patřil Antminer S1 z roku 2013, určený pro těžbu Bitcoinu, s Hash rate 180 GH/s. V současné době je na trhu nejvýkonnější Antminer S15,

který má Hats rate 28 TH/s. Za šest let se tedy výkon Antmineru zvýšil více než 150x. (Bitmain, 2019)

A nevznikaly jen počítače, ale celé pooly. Pool se nazývá specializované místo, kde jsou soustředěny stovky až tisíce počítačů určené k těžení kryptoměn. Uživatel si tedy může zakoupit určitý počet výpočetního výkonu. Stačí mu jen se zaregistrovat u daného provozovatele, zaslat kryptoměnu do své peněženky, a za ty potom zakoupí již zmíněný výpočetní výkon. Tato služba s sebou nese však značná rizika. Jedním z nich je riziko stále se zvyšující náročnosti těžby. Návratnost zakoupených hashů se může tedy s časem snižovat v důsledku nových technologií, či většímu počtu těžařů. Značným rizikem je také výnosnost z pohledu ceny kryptoměny. Jak jsme si ukázali již dříve, cena kryptoměn je velice volatilní. Může se tedy stát, že uživatel nakoupí výpočetní výkon a vytěžené coiny nebudou mít po uplynutí času pronájmu ani hodnotu, za kterou uživatel nakupoval. (Stroukal, 2018, s.104)

Mezi nejznámější pooly patří BTC.com nebo AntPool, které mimo jiné vlastní již zmíněná společnost Bitmain. (Antonopoulos, 2015, s.207)

5.3.1 PROOF OF WORK

Proof of work je nejstarší a nejpoužívanější algoritmus, který využívá většina kryptoměn, mezi které patří Bitcoin nebo Litecoin. Podle posledních testů se jeví jako nejodolnější z ostatních algoritmů. Při tomto konsensu se dokazuje, že byla vykonaná určitá práce.

Těžaři neustále sledují síť a vyhledávají transakce, které je potřebné zrealizovat. Pokud nějakou takovouto transakci najdou, přidají ji ke svým nepotvrzeným transakcím (pool of unconfirmed transactions) a pokračují dál. Zároveň vykonají práci, která se nazývá zpětné řetězení kryptografického kódu (reverse engineering). Tento proces se dá přirovnat ke skládání puzzlí. Každý těžař sbírá své puzzle, a ten co to zvládne jako první, vyhrává. Získá block. U Bitcoinu se jedná o přibližně 4200 transakcí na block.

Když těžař nalezne řešení, odešle block ostatním uživatelům a těžařům, kteří block zkontrolují a předají dál. Těžař, který block vytěžil dostává odměnu za uskutečněné transakce, které block obsahuje a zároveň dměnu za vytěžený block. V případě Bitcoinu je to v současné době 12,5 bitcoinu. (Hosp, 2018, s.58-60)

6 LEGISLATIVA V ČR A VE SVĚTĚ

V České republice v současné době není platný zákon, který by reguloval kryptoměny. Viceguvernér České národní banky Mojmír Hampl se ve svém vyjádření z roku 2018 zmínil o postoji ČNB ke kryptoměnám, ve kterém ČNB nahlíží na kryptoměny spíše jako na komoditu než na měnu. Zmínil, že nechtějí nijak regulovat a bránit v jejich rozvoji, ale také nechtějí aktivně pomáhat nebo propagovat. Investice do kryptoměn je čistě svobodnou volbou a je přirovnána se sázkou v kasinu, kdy je sázející připraven na ztrátu celé své sázky. (Regulation of Cryptocurrency Around the World, 2019a)

Některé legislativní úpravy jsou obsaženy v Zákonu č. 253/2008 Sb., (Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu), které se vztahují na osoby poskytující služby související s virtuálními měnami.

Evropská unie hledí na kryptoměny rovněž jako na komoditu. EU v roce 2016 definovala kryptoměny jako digitální reprezentaci hodnoty, která není vydávána centrální bankou nebo veřejným orgánem, ani nutně spojena s fiat měnou, ale je akceptována fyzickými nebo právnickými osobami jako platební prostředky, které mohou být převedeny, uloženy nebo obchodovány elektronicky. (Regulation of Cryptocurrency Around the World, 2019b)

Soudní dvůr Evropské komise v roce 2015 došel k důležitému závěru. Směna tradiční měny za bitcoin a jiné kryptoměny a naopak, nepředstavují poskytování služeb, tudíž spadají pod výjimku, ze které se neodvádí daň z přidané hodnoty.

Ve světě mimo Evropu je to velmi podobné. Jsou však státy, které zakazují jakékoliv aktivity spojené s kryptoměnani, a těmi jsou Alžírsko, Bolívie, Maroko, Nepál, Pákistán a Vietnam. (Regulation of Cryptocurrency Around the World, 2019b, Stroukal, 2018, s.105-105)

7 BEZPEČNOST

Když už se člověk rozhodně pořídit si nějakou kryptoměnu ať už za účelem možnosti plateb, investičním potenciálem nebo čistě jen ze zvědavosti, měl by zvážit veškerá rizika a bezpečnostní hrozby, které jsou v dnešním světě na denním pořádku. Ať se to nezdá, kryptoměny mají hodnotu stejně jako peníze používané v běžném životě, jako jsou koruny, eura nebo třeba dolary. Jediný rozdíl je, že si je nemůžeme reálně osahat, jelikož jsou virtuální. S tímto je spojena řada rizik v kyberprostoru, na které vlastník kryptoměny musí myslet. Ať už to jsou hackerské útoky na osobní počítač, útoky na virtuální burzy a mnoho jiných.

Bezpečnostní prvky blockchainu jsou takřka neprolomitelné. Kdyby bylo možné hacknout blockchain, jednalo by se o hacknutí kryptografického algoritmu, jako je například SHA256. Toto by teoreticky šlo pomocí kvantového počítače. Takovéto hacknutí by zcela jistě ovlivnilo celý svět jelikož na kryptografii nestojí jen blockchain, ale i celý internet, jelikož je z velké části založen na kryptografii. Pokud by však došlo k prolomení kódu a informace by se dostala na veřejnost, cena kryptoměn by nejspíše prudce klesla, následovala by úprava protokolu a všechno by se s velkou pravděpodobností vrátilo do starých kolejí. (Hosp, 2018, s.104) Takže pokud se v médiích vyskytne zpráva, že došlo k hacknutí kryptoměn, velmi pravděpodobně spíše došlo k hacku nějaké burzy nebo k útoku na konkrétního uživatele. (Hosp, 2018, s.91)

Útočník může do počítače vlastníka kryptoměny nainstalovat škodlivý kód, pomocí kterému mu může kryptoměny odcizit. Tento kód se nazývá malware. Pokud je nainstalován do zařízení oběti, ať už přes email nebo například nějakým nedůvěryhodným programem, může uživatel přijít takřka o všechno.

Příkladem může být software, díky kterému útočník může ovládat počítač oběti a následně si pak převede kryptoměny na svou adresu. Objevily se i případy, kdy škodlivý kód nahradí při kopírování adresy příjemce, adresou jinou. To následně způsobí, že uživatel dobrovolně odešle kryptoměnu zloději, aniž by cokoliv tušil. (Stroukal, 2018, s.88)

Mezi nejčastější útoky však patří monitorování uživatelských účtů a hesel oběti pomocí programů zvaných keylogger. Keylogger je škodlivý počítačový program, který bez vědomí uživatele monitoruje stisky klávesnice a odesílá je přímo zloději. (Hub, 2013, s.34)

7.1 PENĚŽENKY

Pro skladování a přechovávání kryptoměn se využívají takzvané peněženky. Avšak nejedná se přímo o skladování kryptoměn, nýbrž jejich soukromých klíčů. Jejich soukromý klíč pak vede k adrese, na které je v blockchainu zapsáno kolik coinů se na ní nachází. Peněženka funguje tedy spíše jako správce hesla, ve kterém jsou uložena různá hesla (soukromé klíče) k různým kryptoměnám. (Hosp, 2018, s.83)

7.1.1 PAPÍROVÁ PENĚŽENKA

Papírové peněženky jsou jednou z nejjednodušších a nejdostupnějších možností, jak uchovávat kryptoměny. Jsou zde již od počátku Bitcoinu, kdy se první vygenerované soukromé klíče zapsaly na papír a problém byl vyřešen. K takovéto peněžence se nelze dostat přes digitální média, a tím je zaručena její vysoká bezpečnost.

Takovéto peněženky se využívají převážně k většímu množství coinů, se kterými nemá uživatel v plánu více manipulovat, z důvodu horší dostupnosti.

Papírová peněženka lze vytvořit velmi snadno. K tomu nám pomůže webová stránka bitcoinpaperwallet.com, která nám vygeneruje Bitcoinovou papírovou peněženku. Nejbezpečnější před začátkem generování peněženky, je načtení stránky a odpojení počítače od internetového připojení, což zredukuje další potenciální hrozby. Pro úplnou bezpečnost by bylo nejlepší generovat peněženku na počítači, který nebyl nikdy předtím připojen k internetu a nemohl být do něj instalován jakýkoliv škodlivý kód, a tisknutí na tiskárně, která taktéž nemá přístup k internetu, potažmo ke škodlivému kódu. Prvním krokem je vygenerování náhodných znaků generátorem. Generování probíhá snímáním pohybů myši, aby byly znaky zcela náhodné. (Bitcoinpaperwallet, 2019, Hosp, 2018, s.84-85, Stroukal, 2018, s.92-93)

Následuje vygenerování přední strany peněženky, která je zobrazena na obrázku 2. (Bitcoinpaperwallet, 2019)

Obrázek 2 Generování papírové peněženky *Zdroj: Bitcoinpaperwallet.com*

Můžeme si všimnout dvou QR kódů a dvou adres. Adresa vlevo, je adresa veřejná (public address). Tu používá uživatel k přijímání coinů. Public address je veřejná, mohou ji tedy znát všichni. V našem případě se jedná o adresu 13qFqrUPZ3BvEJnKuxrXcXzkjvSR8RrD7k, která má délku 34 znaků.

V pravé části se nachází private key, což je soukromý klíč, který se užívá k vybírání a manipulaci s coiny. Tuto adresu nesmí uživatel zveřejnit, jinak by mohl přijít o všechny coiny uložené v peněžence. Private key se obecně doporučuje přepsat na papír a uložit ho někam, kde k němu nebude mít nikdo přístup, z důvodu možné ztráty papírové peněženky.

Dalším bodem je vytisknutí zadní strany peněženky, vystřižení a následné poskládání, aby nebyl vidět soukromý klíč, jako je to zobrazeno na obrázku 3. (Bitcoinpaperwallet, 2019)

Obrázek 3 Papírová peněženka *Zdroj: Bitcoinpaperwallet.com*

Nedoporučuje se dělat jakékoliv digitální kopie peněženky, jelikož potom ztrácí význam cold storage, tedy offline archivování. Digitální kopie, ať už je to například fotografie nebo naskenovaný obrázek může být terčem hackerských útoků.

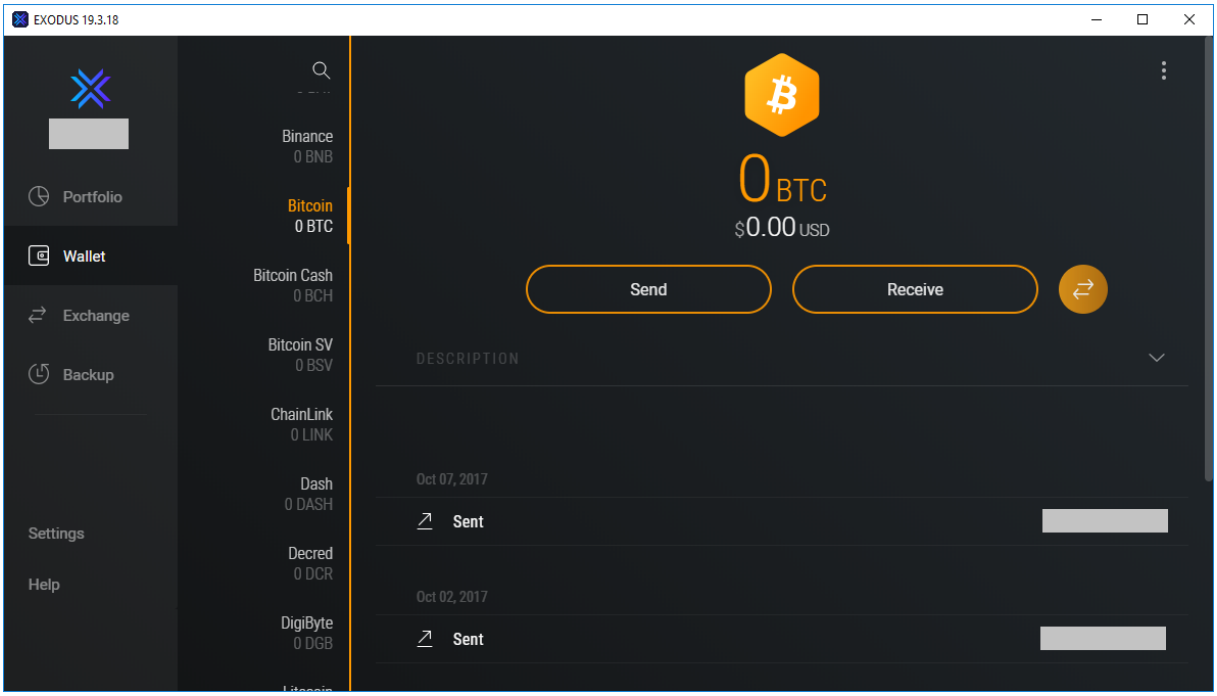
7.1.2 SOFTWAROVÉ PENĚŽENKY

Další možností skladování kryptoměn jsou takzvané softwarové peněženky. Jedná se o počítačový program, který si uživatel stáhne a nainstaluje do svého zařízení. Důležité je, aby uživatel věděl, kam se bude soubor instalovat a kam se tedy jeho soukromé klíče budou ukládat. Tento software by si měl uživatel pečlivě zálohovat. Zálohování by však mělo počítat s tím, že se jedná o soukromé klíče, ke kterým by neměla mít většina lidí přístup. Lze si to představit jako klíč do internetového bankovnictví, bez jehož hesla bude účet s veškerým obsahem, tedy všemi penězi, nenávratně ztracen. Bezpečnou možností je software nainstalovat na flash disk, který bude mít uživatel odpojen od počítače a bude ho mít fyzicky uschován. Avšak bude mít také horší přístup ke coinům v peněžence.

Při instalaci si uživatel zvolí heslo, kterým bude do programu vstupovat. Program pak zobrazí určitý počet slov, která budou sloužit při obnově peněženky v případě poruchy zařízení. Při poruše zařízení uživatel jednoduše nainstaluje peněženku na nové zařízení a zadá daná slova a peněženka bude obnovena. (Hosp, 2018, s.86-87, Stroukal, 2018, s.69-70)

Konkrétním příkladem takovéto softwarové peněženky může být Exodus Wallet. Je to softwarová peněženka, kterou lze nainstalovat nejen na osobní počítače Windows, Mac, Linux, ale i do mobilních zařízení v Androidem a iOS. V současné chvíli nabízí uschování pro 96 různých coinů. Exodus umožňuje nejen přijímat a zasílat coiny během pár kliknutí, ale nabízí také službu Exchange, kde má uživatel možnost vyměnit coiny za jiné, avšak s lehce vyšším kurzem. (Exodus, 2019)

Na obrázku 5 je zobrazeno uživatelské rozhraní Exodus Wallet, které je určeno pro co nejširší okruh uživatelů, takže je velmi jednoduché a snadno využitelné.



Obrázek 4 Exodus wallet *Zdroj: vlastní zpracování*

Přijímání a odesílání coinů je v Exodus Wallet také velmi jednoduché. Pokud chce uživatel přijímat coiny, stačí kliknout u konkrétního coinu, který chce obdržet, na Recieve (Obr. 4) a zobrazí se mu jeho veřejná adresa s QR kódem (Obr. 5), který lze naskenovat mobilním telefonem, nebo adresu zkopíruje, vytiskne nebo odešle emailem. Poslední možnost na Obr. 4 je zobrazení adresy na blockchainu,

Obrázek 5 Exodus address *Zdroj: vlastní zpracování*

7.1.3 HARDWAROVÁ PENĚŽENKA

Hardwarová peněženka, jak už lze poznat z názvu, je nějaký kus hardwaru, do který slouží k uschování veřejného klíče. Zařízení bývá zpravidla velké jako USB flash disk nebo třeba klíče od auta. A v něm se nachází malý jednoúčelový počítač, který slouží k uschování kryptoměn.

Přístup a manipulace s coiny je o něco málo složitější než u již zmíněných softwarových peněženek, avšak z hlediska bezpečnosti je tomu naopak.

Konkrétním příkladem může být TREZOR. Je to společnost, která vyvíjí hardwarové peněženky, o jejíž vznik se zasloužil český startup SatoshiLabs. (Stroukal, 2018, s.88) Nabízí několik modelů hardwarových peněženek, v tomto případě si představíme TREZOR Model T.

TREZOR Model T je hardwarová peněženka podporující více než sedm set coinů, která funguje na dvou jednoduchých principech, a to izolace soukromých klíčů a nutnost fyzické manipulace a potvrzení uživatelem. Tento model, tedy Model T má oproti ostatním modelům dotykovou obrazovku. U předchozích a u levnějších modelů se dotyková obrazovka nevyskytuje, obsahují tedy hardwarová tlačítka, pomocí kterých se potvrzují transakce. Cena tohoto modelu se pohybuje kolem 180 eur. Nejedná se tedy o malou investici do bezpečnosti, v porovnáním s ostatními papírovými a softwarovými, které jsou zdarma, avšak bezpečnost je několikanásobně vyšší. (TREZOR, 2019, Stroukal, 2018, s.88-91)

Při pořízení takovéto peněženky je třeba dbát zvýšené opatrnosti a kupovat hardwarové peněženky přímo od výrobce nebo od oficiálních prodejců. Peněženky, které se prodávají na internetových tržištích jako je například ebay, jsou velmi nevěrohodné v důsledku cizího předchozího majitele, který do peněženky mohl nainstalovat škodlivý kód.

V případě TREZOR Model T je tento problém vyřešen ochrannou známkou, která je přilepena přes připojovací USB port. Pokud je tedy tato známka poškozena, peněženka se stává nevěrohodnou a uživatel by ji neměl z hlediska bezpečnosti používat. Na tuto skutečnost společnost TREZOR několikrát upozorňuje, ať už přímo v krabici produktu, tak na svých webových stránkách.

Pokud je ochranná známka po nákupu tam kde má být, uživatel ji odstraní a připojí ke svému osobnímu počítači. Peněženka se pak přes stránku trezor.io nastaví a aktivuje. Uživatel si vygeneruje svých dvanáct back-up slov (pro obnovu stejně jako u softwarových peněženek) a zvolí si PIN kód, pomocí kterého bude potvrzovat transakce.

7.1.4 SMĚNÁRNY A BURZY

Mezi nejpohodlnější, ale zároveň nejméně bezpečné varianty patří přechovávání coinů ve směnárnách nebo burzách. Uživatel, který má zde „ukryté“ coiny, nemá přístup k soukromým klíčům a tím spoléhá na provozovatele, který za ně zodpovídá. Uživatelsky příjemné rozhraní je vykompenzováno nízkou bezpečností.

Burza či směnárna tak musí klást na bezpečnost velký důraz, jelikož jsou pod neustálými útoky hackerů, kteří mají pro útoky pádný důvod. Na burze nebo směnárně je koncentrováno velké množství uživatelů a tím pádem velké množství soukromých klíčů k peněženkám, které vedou k obrovskému množství coinů.

Jedním z konkrétních příkladů obrovské ztráty coinů z burzy je krach burzy Mt. Gox. Burza Mt. Gox byla ve své době jednou z největších burz obchodující s Bitcoinem. Byla založena v roce 2010 a sídlila v Japonsku. Problémy nastaly v červnu 2013, kdy burza pomalu přestávala vyplácet peníze nebo transakce trvaly týdny až měsíce. Nakonec pak v únoru 2014 burza pozastavila i vyplácení bitcoinu.

Uživatelé mohli na burze stále obchodovat za prostředky, které měli na účtech k dispozici, avšak cena byla v porovnání s ostatními burzami několikrát nižší. Uživatelé si pak nedávali nejmenší šance, že své peníze vůbec někdy uvidí. Nakonec tedy 24. února 2014 burza Mt. Gox uzavřela své stránky a o čtyři dny později oznámila krach. (Stroukal, 2018, s.58-59)

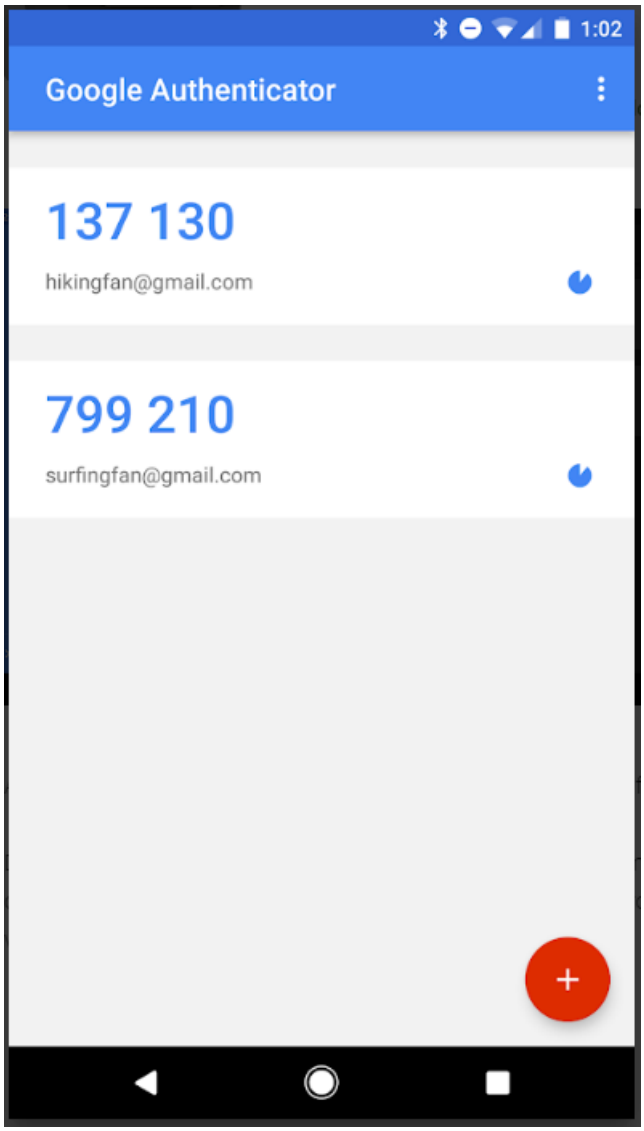
Jelikož se jednalo o jednu z největších burz v té době, cena Bitcoinu tuto událost nesla velmi špatně. Z ceny kolem tisíce amerických dolarů spadla až přibližně ke čtyřem stům. (Coinmarketcap, 2019)

7.2 BEZPEČNOSTNÍ MECHANISMY A OVĚŘENÍ

Existuje několik bezpečnostních mechanismů, které zaručují vyšší bezpečnost k přístupu ať už k účtům nebo peněženkám. S takovým mechanismem se běžně setkává uživatel, kterému nabízí banka SMS potvrzení platby se zadáním určitého kódu. Tato ochrana se nazývá dvoufaktorové ověření, překládána jako Two-factor authentication nebo může být navýšena na několika faktorové ověření, tedy Multi-factor authentication.

Jedním z příkladů může být dvoufaktorové oveření společnosti Apple. Nabízí ověření přihlášení k účtu iCloud pomocí důvěryhodného zařízení společnosti Apple. Toto ověření se zobrazí po zadání přihlašovacích údajů. Nejprve je zobrazena poloha přihlašujícího se zařízení. Uživatel tedy potvrdí, že se jedná právě o něj a následně se zobrazí šesticiferný kód, kterým potvrdí přihlášení.

Společnost Google se s tímto vypořádala podobně pomocí Google Authenticator. Toto dvoufázové ověření zajišťuje vyšší zabezpečení použitím bezpečnostního kódu, který je zobrazován v aplikaci Google Authenticator. Uživatel pak musí znát nejen přihlašovací údaje, jako jsou přihlašovací jméno a heslo, ale musí zadat daný kód z aplikace. (Google Authenticator, 2019) Tento kód se pak mění každých třicet vteřin. Google Authenticator se využívá nejen k přihlášení účtů Google, ale i k řadě směnáren a burz obchodující s kryptoměnami, jako jsou například Binance, Bittrex nebo Coinbase. (Google Authenticator, 2019)



Obrázek 4 Ověření pomocí Google Authenticator *Zdroj: (Google Authenticator, 2019)*

Jednou z dalších možností potvrzení nové IP adresy. Toto ověření využívá například burza Bittrex spolu s Google Authnticator. Princip spočívá v tom, že ke každému účtu má uživatel whitelist IP adres, který obsahuje již ověřené adresy, ze kterých se uživatel již připojil. Pokud se tedy uživatel připojí z adresy jiné, je vyžadováno ověření pomocí Google Authenticator, díky kterému uživatel přidá adresu do svého whitelistu.

8 DEEPWEB A ILEGÁLNÍ AKTIVITY

Jako deepweb se označuje taková část internetu, která není dohledatelné pomocí běžných internetových prohlížečů, jako jsou například Google, Yahoo nebo třeba Bing. Naopak dohledatelné webové stránky pomocí těchto běžných webových prohlížečů se nazývají surface web, někdy také clearnet, neboli viditelný internet. Tyto viditelné stránky však tvoří přibližně 4 % celkové velikosti internetu. Často je internet přirovnáván k ledovci, kdy je viditelná pouze špička ledovce, zatímco mnohem větší část se nachází pod hladinou. (DarkWebLinks, 2019)

Zbylých 96 % tvoří deepweb, neboli hluboký internet, ke kterému patří ještě darkweb, který by se dal přeložit jako temný internet.

Deepweb obsahuje stránky, které internetové prohlížeče neindexují nebo je k nim omezený přístup. Příkladem mohou být univerzitní systémy, ke kterým má uživatel přístup pouze s přihlašovacím jménem a heslem. Dále deepweb obsahuje například soukromé weby, které by šly zaindexovat, avšak majitel si to nepřeje, bankovní data apod.

Avšak hlavní složka, kvůli je deepweb zmiňován, je darkweb. Darkweb je součástí hlubokého webu, ke kterému je potřeba speciální software. Tímto softwarem je například prohlížeč Tor, který využívá stejnojmennou síť. Pomocí Toru se uživatel připojí anonymně, přes P2P síť, do darkwebu. Webové stránky na darkwebu jsou zašifrované a mají příponu: onion. Tyto stránky obsahují většinou ilegální obsah, který by byl ve viditelném internetu cenzurován nebo smazán. Příkladem tohoto obsahu může být prodej drog, zbraní, pornografie, falešných dokladů a mnoho dalších. (DarkWebLinks, 2019)

Právě velkou částí darkwebu jsou ilegální tržiště. Jedná se o weby velmi podobným těm viditelným, jako jsou například Aukro nebo ebay, avšak s ilegálním obsahem. Nejčastějšími položkami na těchto tržištích je prodej drog (přibližně tři čtvrtiny) a platby probíhají v kryptoměnách. (Stroukal, 2018, s.52)

Kryptoměny, zpočátku tedy Bitcoin se staly pro ilegální tržiště dokonalým nástrojem díky své anonymitě.

Mezi první ilegální tržiště se řadil server Silk Road, který byl založen v roce 2011. Nabízel kolem deseti tisíc různých produktů. Stvořitelem a provozovatel tohoto webu byl Ross Ulbricht, známý na Silk Road pod přezdívkou Dread Pirate Roberts, avšak tento účet užívalo nejspíše více uživatelů. (Stroukal, 2018, s.52) Ross Ulbricht vytvořil Silk Road jako experiment, který by umožňoval uživatelům spolu obchodovat a komunikovat s absolutní svobodou a anonymitou. Existovala tedy také fóra, kde komunita sdílela názory a myšlenky.

Ross Ulbricht byl dopaden 1. října roku 2013 v internetové kavárně v San Franciscu. A server Silk Road byl okamžitě uzavřen. Po uzavření se cena BTC propadla z 139 dolarů na 109, avšak díky mediálnímu vlivu se cena rychle vrátila zpět. (Stroukal, 2018, s.53) Při jeho zatčení byly zabaveny jeho Bitcoinové adresy. Jednou z nich byla adresa 1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55 (TheOpenLedger, 2015), kde se nacházelo 26 tisíc BTC. Později však mluvčí FBI uvedl, že se zabavilo celkem 144 tisíc BTC v celkové hodnotě kolem 20 milionů amerických dolarů.

V roce 2015 byl odsouzen na doživotí za trestné činy praní špinavých peněz, obchod s drogami, obchodování s falešnými identifikačními dokumenty a počítačového hackerství. (FreeRoss, 2018)

Po uzavření Silk Road netrvalo dlouho a objevila se řada dalších podobných serverů, nabízející podobné služby jako jsou například Atlantis, Black Market Reloaded nebo třeba Sheep marketplace. (Stroukal, 2018, s.53)

Tyto markety však neměly dlouhého trvání. Většinou skončily podvodem na své uživatele. Právě autor již zmíněného Sheep Marketplace utekl s 96 tisíci bitcoiny, což se v tehdejší době rovnalo přibližně 1,5 miliardy Kč. (Stroukal, 2018, s.53) Kořeny tohoto autora sahaly do České republiky, a to konkrétně k Tomáši Jiřikovskému, který byl odsouzen za obchodování s drogami, krádež a nedovolené ozbrojování na děvět let vězení. (Novinky, 2017)

V současné době se mezi největší markety řadí Dream market nebo Wall Street Market, který na svém webu uvádí, že se na jejich serveru nachází 4,8 tisíc prodejců a 1,05 milionu zákazníků. (DeepDotWeb, 2019, WallStreetMarket)

9 ANONYMITA A TRANSPARENTNOST

Kryptoměny se na první pohled mohou zdát anonymní, avšak u většiny to není úplná pravda. Většinu transakcí a peněženek je schopné dohledat například se spoluprací orgánů činných v trestním řízení s internetovým poskytovatelem. (Stroukal, 2018, s.108)

Uživatel může být anonymní, musí však projít ne příliš jednoduchým procesem a musí být velmi opatrný. Příkladem může být využívání internetového prohlížeče Tor, o kterém již byla zmínka. Připojí se tedy před vzdálené proxy servery, a právě toto připojení je téměř nevystopovatelné.

Jak již bylo uvedeno většina burz a směnáren požadují ověření identifikačním dokladem, ž jen z toho důvodu, aby nedocházelo k ilegálním aktivitám. Navíc pak všechny transakce, které putují z bankovního účtu rovněž nemohou být anonymní, když onen bankovní účet nemůže být anonymní. (Stroukal, 2018, s.108)

Jedinou možností je tedy využití bitcoinového bankomatu, avšak po překročení určité částky může uživatel jednat v rozporu se zákonem č. 253/2008 Sb., zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. (Zákon č. 253/2008 Sb.)

Jedním z kroků ke zvýšení anonymity je změna přijímací adresy. To se hodí v případě, kdy příjemce nechce, aby ostatní viděli, kolik coinů přes adresu prošlo. Některé peněženky tuto funkci nabízejí. (Stroukal, 2018, s. 109)

Existují však kryptoměny, které si na anonymitě zakládají. Nazývají se privacy coins a příkladem může být kryptoměna Monero (XMR), která zvyšuje anonymitu díky rozdílnému typu podepisování transakcí, což činí transakce téměř nevystopovatelné.

Kryptoměny jsou jak anonymní, tak ale zároveň úplně transparentní, díky technologii blockchainu. Někdy není možné vystopovat vlastníka adresy, avšak na blockchainu je zaznamenaná kompletní historie transakcí, které kdy na něm proběhly. Toto šlo využít na již zmiňovaném příkladu Rosse Ulbrichta, kde bylo možné dohledat kompletní seznam transakcí, které prošly jeho peněženkami.

10 SHRNUTÍ A DOPORUČENÍ

V této části práce bych chtěl shrnout, jak by se uživatelé, kteří mají v plánu nakoupit kryptoměny, chovat. Bude se však jednat o čistě osobní názor a doporučení, jelikož nejsou k dispozici jakákoliv statistická data.

Když už se člověk rozhodne nakupovat, měl by zvážit základní bezpečnostní rizika. Nejdůležitějším faktorem je objem transakce, za kterou chce nakupovat. Jinak se bude uživatel chovat při nákupu za stovky a tisíce než ti, kteří nakoupí za statisíce a miliony.

Pokud se tedy uživatel rozhodně nakoupit v řádu stovek až tisíců korun, doporučil bych mu papírovou nebo softwarovou peněženku, popřípadě nechat coiny ležet v dané směnárně či burze. Jedná se nejlevnější řešení a při takto malých objemech by jiná řešení postrádala smysl z důvodu vysokých nákladů.

Pokud se bude jednat o částky v řádech desítek tisíc korun, je stále možné nechat coiny ve směnárně či burze. Doporučil bych ale použití dvoufaktorového ověření. Na zvážení už přichází také TREZOR, či jiné hardwarové peněženky, které jsou ovšem dražší na pořízení. Jedná se však o jednu z nejbezpečnějších alternativ.

Na částky vyšší než sto tisíc bych rozhodně nedoporučoval směnárny ani burzy. V tomto případě připadá v úvahu papírová nebo hardwarová peněženka.

Dalším důležitým faktorem je, jak často bude uživatel coiny transferovat či prodávat. Ať už nakupuje za jakýmkoliv účelem, některé z možností jsou pohodlnější a některé méně. V tu chvíli stojí za zvážení, zda podstoupit riziko za účelem většího pohodlí. Coiny ve směnárně či burze jsou dostupné takřka kdykoliv a kdekoliv s přístupem na internet. Lze tedy s nimi okamžitě manipulovat, popřípadě nakoupit či prodat.

Papírové a hardwarové peněženky musí mít uživatel fyzicky u sebe. Pokud tedy chce s coiny jakkoliv manipulovat, musí podstoupit složitější proces.

O trochu lépe jsou na tom softwarové peněženky, jelikož se většinou nachází na zařízení, jako je například osobní počítač nebo mobilní telefon, které má uživatel k dispozici denně.

Jedním z dalších faktorů může být, jak je osoba zběhlá v informačních technologiích. Můžeme si určit tři základní kategorie, osoba IT neznalá, IT znalá a osoba s vysokou znalostí v IT. A k těmto kategoriím shrnu, jak by měly jednotlivé skupiny jednat při nákupu kryptoměn.

První kategorii, osoba s nízkou znalostí IT, si můžeme definovat jako osobu, která nemá příliš mnoho vědomostí z oblasti IT. Ovládá základní funkce jako je třeba internetový prohlížeč a email. Pokud má tedy zájem nakoupit kryptoměnu, za jakýmkoliv účelem, doporučil bych poradit se s odborníkem. Kdyby by osoba s takto nízkou znalostí nakupovala kryptoměny na vlastní pěst, mohlo by to mít fatální následky. Veškeré manipulace by měl na starosti odborník, který by posílal pravidelné reporty o tom, jak si coiny vedou.

Další kategorií jsou osoby se střední znalostí IT. Ti se dají definovat jako běžní uživatelé internetu s pokročilou znalostí v informačních technologiích, samy si třeba dokáží spravovat osobní počítač, nainstalují si antivirus a počítač pravidelně kontrolují apod. Těmto uživatelům bych s klidem doporučil použití jakýkoliv peněženek v kombinaci s některým z dvoufaktorových ověřeních. Při větších objemech pak rozložit coiny do více různých peněženek, aby se snížilo riziko ztráty všech coinů najednou.

Poslední kategorií jsou osoby s vysokou znalostí IT. Může se jednat o IT experty, kteří vědí o rizikách, která na ně v informačních technologiích číhají. Příkladem můžou být programátoři, správci sítí nebo třeba bezpečnostní experti. Tito uživatelé například apelují na aktuální antivirus či operační systém, využívají dostatečně silné heslo a toto heslo nikdy nevyužívají pro více služeb najednou, vyhýbají se podezřelým stránkám nebo třeba pravidelně zálohují důležitá data. Tyto osoby by nejspíše nedůvěřovaly jednotlivým burzám a směnárnám a chtěly by si coiny ochránit samy. Můžu jim tedy vřele doporučit softwarovou peněženku, jelikož pravděpodobnost, že se v jejich počítači bude vyskytovat nějaký škodlivý kód je velmi malá. Záleží však vždy na objemu transakcí. Pokud se jedná o velké objemy, vždy bych raději doporučil hardwarovou peněženku.

11 ZÁVĚR

V závěru své práce bych rád shrnul, o čem práce pojednává a podělil se o pár myšlenek s kryptoměnami a bezpečnosti s nimi spjatými.

Kryptoměny jsou tedy virtuální tokeny, fungující ve veřejné pokladní knize zvané blockchain. Díky tomu, že blockchain je decentralizovaný, nespravuje jej žádná centrální instituce. Tokeny nebo coiny samy o sobě nejsou nositeli žádné hodnoty. Jde pouze o číslo, které je zapsané kdesi v pokladní knize. Nesmírnou hodnotu má však ona technologie a systém samotný. Přirovnat to zle například k sociální síti Facebook. Jedná se o systém, který poskytuje uživatelům sdílet obsah na internetu, který má velmi vysokou hodnotu, avšak bez aktivních uživatelských účtů by systém byl k ničemu, a to platí i v opačném případě. Jednotlivé uživatelské účty nemají žádnou hodnotu bez dané sítě.

U kryptoměn je tato hodnota navíc umocněna tím, že ji nikdo nedokáže ovlivnit, nikdo ji nespravuje a nikdo ji nemůže zakázat.

V současné době existuje velké množství kryptoměn, avšak pouze některé mají vyhlídky do budoucnosti. V práci zmiňuji jen pár takových, které by se svou současnou market kapitalizací v budoucnu mohly obstát, avšak v oblasti kryptoměn není nikdy nic jisté.

Míst kde nakoupit kryptoměny je dostatek, není tedy pro kohokoliv problém si o kryptoměnách něco zjistit a případě si nějaký coin pořídit. V práci jsou uvedeny jedny z největších směnáren a burz, které v krypto-světě v současnosti působí. Jednou z možností, jak získat coiny je vytěžit si vlastní, ať už s pomocí svého osobního počítače nebo speciálního hardwaru.

Z pohledu legislativy je evidentní, že stále nevíme, na čem jsme. Podle současné právní úpravy v České republice jsou kryptoměny považovány jako komodity a měla by se na ně při jejich nákupu či prodeji vztahovat daň z přidané hodnoty, avšak toto je v rozporu s rozhodnutím Soudního dvoru Evropské komise, který hovoří, že Bitcoin a jiné kryptoměny, a jejich prodej či nákup za fiat peníze je osvobozen od value-added-tax, tedy od daně z přidané hodnoty. A toto rozhodnutí by měly respektovat všechny členské státy EU.

Velmi důležitá je ochrana zakoupených coinů. K tomuto ve své práci věnuji značnou pozornost. Bezpečnost musí být vždy na prvním místě a v případě kryptoměn je nesmírně důležité dodržovat bezpečnostní pravidla a využívat bezpečnostní mechanismy.

Existuje několik možností, jak skladovat kryptoměny, ať už to jsou papírové peněženky, softwarové peněženky nebo hardwarové peněženky. Všechny pracují na stejném principu, a to ochrana soukromého klíče uživatele. Následně je na uživateli, jak bude danou peněženku

chránit. Koneckonců jedná se o peněženku, ve které je ukryta nějaká hodnota, a je jedno jestli ve formě fiat peněz nebo kryptoměn. Peněženku by měl uživatel chránit tak jako tak.

K bezpečnosti kryptoměnových peněženek přispívají bezpečnostní mechanismy s dvoufaktorovým ověřením, jako je například Google Authenticator. Tyto mechanismy zásadně zvyšují bezpečnost peněženek.

Kryptoměny, konkrétně bitcoin, jsou velmi často spojovány s ilegálními aktivitami, podvody apod. Není se čemu divit, většina médií se ke kryptoměnám staví spíše skepticky. Velkou roli v tom hrají obchody s drogami přes internet, o což se ve velké míře zasloužil server Silk Road v čele s Rossem Ulbrichtem a v současné době to jsou obrovské markety jako je například WallStreetMarket. Avšak, když se na to podíváme z druhé strany, zpočátku šlo jen o myšlenku vytvořit svobodný trh, bez jakékoliv regulace a kryptoměny k tomu byly pouze prostředkem k realizaci díky své rychlosti transakcí a relativní anonymitě.

Bitcoin a jiné kryptoměny se naopak pro ilegální aktivity hrubě nehodí z důvodu své transparentnosti. Na blockchainu se zaznamenává veškerá aktivita a pohyb z peněženky a do peněženky. Pro ilegální aktivity se daleko víc hodí peníze v hotovosti. Ty je takřka nemožné vystopovat a nikdo přesně neví kolik, kudy a kam putují.

V závěru jsem si dovolil malé doporučení pro ty, kteří by si chtěli pořídit nějaké kryptoměny. Mezi nejdůležitější faktory patří objemy transakcí, jak často chtějí s coiny manipulovat a velmi důležitý faktor, jak jsou zběhlí v IT. Je nezbytné zvážit alespoň tyto faktory před nákupem, aby nedošlo k nějaké pohromě.

Budoucnost kryptoměn je velmi nejasná, ve světě se vyskytuje plno krypto skeptiků, kteří jsou přesvědčeni, že kryptoměny co nevidět zaniknou, ale i krypto snílků, kteří například věří, že kryptoměny nahradí centralizované fiat měny.

12 ZDROJE

ANTONOPOULOS, Andreas M., 2015. *Mastering bitcoin*. Sebastopol CA: O'Reilly. ISBN 978-1-449-37404-4.

Apple Support, 2019. *Apple.com* [online]. [cit. 2019-04-01]. Dostupné z: https://support.apple.com/cs-cz/HT204915

Binance: About Binance [online], 2019. [cit. 2019-04-17]. Dostupné z: https://www.binance.com/aboutUs.html

Binance coin, 2019. *Binance.com* [online]. [cit. 2019-04-17]. Dostupné z: https://info.binance.com/en/currencies/binance-coin

Bitcoinpaperwallet, 2019. *Bitcoinpaperwallet.com* [online]. [cit. 2019-03-26]. Dostupné z: https://bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html#

Bitmain, 2019. *Https://www.bitmain.com/about?lang=en-US* [online]. Beijing [cit. 2019-03-25]. Dostupné z: https://www.bitmain.com/about?lang=en-US

Coinbase: ABOUT COINBASE [online], 2019. [cit. 2019-03-13]. Dostupné z: https://www.coinbase.com/about

Coinmap [online], 2019. SatoshiLabs [cit. 2019-03-13]. Dostupné z: coinmap.org

Coinmarketcap [online], [cit. 2019-03-12]. Dostupné z: https://coinmarketcap.com/

DarkWebLinks: What is the Deep Web? [online], 2019. [cit. 2019-04-03]. Dostupné z: https://www.thedarkweblinks.com/what-is-the-deep-web/

DeepDotWeb: Top Markets! [online], 2019. [cit. 2019-04-03]. Dostupné z: https://www.deepdotweb.com/marketplace-directory/categories/top-markets/

Eidoo: ERC20 Tokens list [online], [cit. 2019-04-17]. Dostupné z: https://eidoo.io/erc20-tokens-list/

Exodus, 2019. *Exodus* [online]. [cit. 2019-03-26]. Dostupné z: https://www.exodus.io/status/

FreeRoss: Timeline of the Silk Road Case [online], 2018. [cit. 2019-04-03]. Dostupné z: https://freeross.org/case-timeline/

Google Authenticator, 2019. *Google Play* [online]. [cit. 2019-04-01]. Dostupné z: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=cs

HOSP, Julian, 2018. *Kryptomeny*. Bratislava: TATRAN. ISBN 978-80-222-0945-8.

HUB, Miloslav, 2013. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice: Univerzita Pardubice. ISBN 978-80-7395-701-8.

InvestPlus: Klady a zápory SimpleCoin – recenze, zkušenosti, návod, poplatky, diskuze, 2018. *InvestPlus* [online]. [cit. 2019-03-18]. Dostupné z: https://investplus.cz/investice/klady-a-zapory-simplecoin-recenze-zkusenosti-navod-poplatky-diskuze/

Kurzy.cz: Bitcoin - aktuální a historické ceny kryptoměny Bitcoin, graf vývoje ceny kryptoměny Bitcoin - 2 roky - měna USD [online], [cit. 2019-03-11]. Dostupné z: https://www.kurzy.cz/komodity/bitcoin-graf-vyvoje-ceny/usd-2-roky

Litecoin: Co je Litecoin?, *Litecoin.org* [online]. 2011-2019 [cit. 2019-03-12]. Dostupné z: https://litecoin.org/cs/

NAKAMOTO, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*. Dostupné také z: https://bitcoin.org/bitcoin.pdf

Novinky: Programátor stvořil drogovou tržnici a ukradl bitcoiny za 16 miliónů, dostal devět let [online], 2017. [cit. 2019-04-03]. Dostupné z: https://www.novinky.cz/krimi/451367-programator-stvoril-drogovou-trznici-a-ukradl-bitcoiny-za-16-milionu-dostal-devet-let.html

Regulation of Cryptocurrency Around the World: European Union [online], 2019b. [cit. 2019-04-17]. Dostupné z: https://www.loc.gov/law/help/cryptocurrency/world-survey.php#eu%20members

Regulation of Cryptocurrency Around the World: Czech Republic [online], 2019a. [cit. 2019-04-17]. Dostupné z: https://www.loc.gov/law/help/cryptocurrency/world-survey.php#czech

Ripple: XRP The Digital Asset for Payments [online], 2019. [cit. 2019-04-03]. Dostupné z: https://ripple.com/xrp/

Simplecoin: Všeobecné obchodní podmínky, 2018. *Simple Coin s.r.o.* [online]. Praha 7: Simple Coin [cit. 2019-03-13]. Dostupné z: https://exchange.simplecoin.eu/post/tos

STROUKAL, Dominik a Jan SKALICKÝ, 2018. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 2., rozšířené vydání. Praha: Grada Publishing. Finance pro každého. ISBN 978-80-271-0742-1.

TheOpenLedger: 9 Infamous Bitcoin Addresses, 2015. *TheOpenLedger* [online]. [cit. 2019-03-20]. Dostupné z: http://www.theopenledger.com/9-most-famous-bitcoin-addresses/

TREZOR: TREZOR Model T [online], 2019. [cit. 2019-03-26]. Dostupné z: https://shop.trezor.io/product/trezor-model-t

VIGNA, Paul a Michael CASEY, 2015. *The age of cryptocurrency: how bitcoin and digital money are challenging the global economic order*. New York: St. Martin's Press. ISBN 978-1-250-06563-6.

WallStreetMarket [online], [cit. 2019-04-03]. Dostupné z: http://wallst4qihu6lvsa.onion/

WBTCb.cz, 2017. In: *Obchodní podmínky služby Bitcoinmat* [online]. wBTCb.cz [cit. 2019-03-13]. Dostupné z: https://www.wbtcb.com/frontend/webroot/uploads/files/2014/05/obchodni_podminky_BTM.pdf

Zákon č. 253/2008 Sb.: Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu [online], [cit. 2019-04-05]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-253

13 SEZNAM OBRÁZKŮ