MORAVSKÁ VYSOKÁ ŠKOLA OLOMOUC

Ústav informatiky a aplikované matematiky

Faktory ovlivňující práci s vybranými kryptoměnami

Factors which affect operations with selected cryptocurrencies

BAKALÁŘSKÁ PRÁCE

Jméno studenta – Zdeněk Grossmann

Vedoucí práce: PhDr. Jan Lavrinčík, Ph.D.

Olomouc 2019

PROHLÁŠENÍ

Prohlašuji, že bakalářskou práci jsem vypracoval samostatně a s použitím uvedených zdrojů a literatury.

V Olomouce dne 29. 03. 2019 ……..……...…….

Grossmann Zdeněk

PODĚKOVÁNÍ

Otevřeně děkuji panu PhDr. Janu Lavrinčíkovi, Ph.D. za odborné vedení a zejména za cenné rady, které mě navedly správným směrem v mé bakalářské práci. Také bych chtěl poděkovat blízkým osobám, které mě po dobu vypracovávání bakalářské práce podporovaly.

Příloha – Zadání kvalifikační práce

Obsah

Úvod

Kryptoměnové technologie a kryptoměny se staly fenoménem dnešní doby. Obecně, se neklade důraz na nové technologie, které mohou obohatit celou společnost. Kryptoměny mají velký potenciál se touto globálně rozšířenou technologií stát. Trh se plní vizionářskými projekty, které mají usnadnit či zlepšit aktuální stav. Zaměřím se na nejzajímavější kryptoměnové projekty a popíšu jejich technologickou podstatu a jejich účel.

Kryptoměny a technologie blockchainu přinášejí řadu nových technických řešení, která zatím využívají počítačoví „geekové“ a „IT nadšenci“. Nejběžněji řešenými tématy v souvislosti s kryptoměnami je využíti na mikroplatby na internetu, těžba, IT bezpečnost, převody atp. Domníváme se však, že je málo ucelených studií, které by se zabývaly myšlenkou uceleného systému kryptoměnových projektů, které by představovali alternativu ke stávajícím platebním systémům fiat.

O kryptoměnách se stále častěji a přístupněji dozvídá široká veřejnost, čímž přirozeně roste lidská zvědavost a zájem o jejich hlubší pochopení, potažmo další práci s nimi. Díky tomuto trendu krypto-technologie už nejsou jen výhradou specialistů a fanoušků informačních technologií. Běžně se o výhody kryptoměn zajímají jak jednotlivci, tak velké společnosti, které se snaží zvýšit svůj potenciál na trhu.

Kryptoměnový trh je často srovnáván s Forexovým trhem. Mnoho aktivních forexových traderů přešlo ke spekulacím na kryptoměnových burzách, kde je trh mnohem volatilnější a likvidnější než u Forexu, což z něj dělá pro některé typy obchodníků mnohem zajímavější a rychlejší způsob výdělku. S rostoucí volatilitou však narůstá i riziko. Aktuálně se denní objem obchodů ve všech kryptoměnách pohybuje okolo 15 miliard dolarů[1], kdy stále dominuje neznámější a historicky první vyvinutá kryptoměna – Bitcoin.

Jednotlivce může lákat nezávislost vůči tradičnímu systému, anonymita, vidina rychlého výdělku pomocí tradingu či dlouhodobého zhodnocení.

Podnikatelé a firmy mohou využít kryptoměnových technologií pro inovace stávajícího systému nebo postavit na základech blockchainu svůj vlastní projekt. Díky aplikaci nových pracovních nástrojů a technologií mohou získat konkurenční výhodu, stát

[1] *Coinmarketcap* [online]. 2013 [cit. 2019-02-11]. Dostupné z: https://coinmarketcap.com/

se lídrem v oboru a zavádět trendy.

V bakalářské práci jsem se rozhodl soustředit na kryptoměnové technologie, které všeobecně ještě nejsou tolik známé, jako je tomu již u těch ověřených. Potenciál kryptoměn v nynější době není ani zdaleka naplněn – stojíme teprve na začátku. Přínosem této bakalářské práce bude přiblížení základů kryptoměn a jejich technologií jak neodborné, tak i odborné veřejnosti za současné demonstrace jejich využití na několika praktických příkladech.

Hlavní cíl

Hlavním cílem bakalářské práce je analyzovat a navrhnout ucelený systém vybraných kryptoměnových projektů, které by mohly nabídnout alternativu ke standardním platebním systémům.

Zaměřím se na finanční sféru s ohledem na zdokonalení platebních transferů jak pro retailové zákazníky, tak korporátní klientelu.

Výstupem navrženého systému bude na základě důkladné analýzy sestaveno doporučení optimálních technologií – eventuálně kryptoměny – která by mohla v současnosti či budoucnosti nahradit aktuální, méně výhodné řešení.

Dílčí cíle

V teoretické části bakalářské práce se zaměřím na základní faktory ovlivňující problematiku kryptoměn, vysvětlím pojmy související s vybranou tématikou, popíši historii vzniku kryptoměn a jak se vyvinuly z Bitcoinu až do dnešní podoby. V neposlední řadě uvedu rizikové faktory kryptoměn.

1. Prvním dílčím cílem je vysvětlení základních pojmů. Zaměříme se na objasnění pojmů – například, jaký je rozdíl mezi virtuální a digitální měnou. Poté provedu srovnání s tradičním pojetím měn.
2. Druhým dílčím cílem je popis a analýza historického vývoje technologie kryptoměn. Mým cílem je vysvětlit a popsat, co zahrnuje termín blockchain, jeho technologickou podstatu a formy, kterými se definuje, modifikuje a dělí.
3. Dalším cílem je analýza a zohlednění možných rizik konceptu kryptoměn, jejich nevýhody, zneužívání a krádeže. Soupis profilu ověřené, důvěryhodné kryptoměny.

4. Poslední dílčí cíl se zabývá možnostmi, jak přistoupit k softwarové a hardwarové ochraně primárních klíčů.

Teoretická část

1. Základní pojmy a rozdělení typů měn

1.1. Tradiční pojetí měny

První platidlo vzniklo v Sumerské civilizaci (destičky, účtenky) a od té chvíle se rozšiřovalo do dalších kultur, kde však měli pro své měny vlastní ekvivalenty hodnoty, např. délka látky, nádoba s obilím nebo váha v určeném kovu.

Z dochovaných zdrojů máme informace, že první mince byly raženy na území Lydie cca 650 let před naším letopočtem. Ražbou kovových mincí se situace radikálně změnila a dala impulz pro zdokonalení účetnictví a základ pro vznik prvních bank.[2]

V Číně byly papírové peníze zavedeny již v sedmém století našeho letopočtu, do západních zemí se však dostaly až v sedmnáctém století, kdy je jako první začali používat Švédové. Zavedením papírových peněz se obchod značně usnadnil a tím i urychlil. Zejména Evropa tak mohla rychleji ekonomicky růst. Bankovky coby druh papírových peněz spolu s mincemi byly donedávna nejpoužívanější formou platidla, než došlo na vznik digitálních peněz.[3]

1.2. Digitální měna

Digitální měna je dalším stupínkem ve vývoji platidel. Prvním náznakem digitálních měn přišel v roce 1871, kdy společnost Wester Union začala elektronicky zpracovávat transfery hotovosti pomocí telegrafu (EFT).

Digitální měnou chápeme ve své podstatě matematické jednotky interpretující hodnotu vložených hmotných prostředků, jako jsou bankovky, mince či vzácné kovy. V praxi se jedná například o peníze na bankovním účtu, kdy banka přijme vklad v hotovosti a připíše je na účet klienta v digitální měně.

---

[2] BIRCH, David. *BEFORE BABYLON, BEYOND BITCOIN: From Money That We Understand To Money That Understands Us*. London: London Publishing Partnership, 2017. ISBN 978-1-907994-67-8.

[3] WHIPPS, Heather. The Profound History of Coins. *Live Science* [online]. 2004, 16.11.2007 [cit. 2019-03-20]. Dostupné z: https://www.livescience.com/2058-profound-history-coins.htm

Vznikem digitální měny se obchod mnohonásobně zrychlil a ulehčil. Některé státy jako třeba Švédsko dokonce zvažují zrušení hotovosti a přejít tak k plné digitalizaci.

1.3. Virtuální měna

Pojem virtuální měna vydefinovala Evropská Centrální Banka a oficiálně ji popsala v roce 2014. Podle Evropské Centrální Banky je virtuální měna: „Digitální reprezentace ceny, která není stanovena centrální bankou, ani veřejnou autoritou. Virtuální měna nemusí být nutně vázaná na fiat měny, ale je přijímána jako způsob platby osobou fyzickou, ale i právnickou. Virtuální měna může být elektronicky směňována, uchovávána a obchodována.“[4]

Virtuální měny jsou zpravidla založeny na základě matematického, kryptografického výpočtu, který definuje aktuální hodnotu, má vlastní zákonitosti a zabezpečení oproti digitální měně, která je pouze znázorněním číselné hodnoty v minulosti vložených prostředků.[5]

1.4. Kryptoměna

Kryptoměny, často označovány jako platidla budoucnosti, jsou typ virtuálních měn, který se stává fenoménem 21. století. Kryptoměna, virtuální měna, jež je postavena na základech kryptografie pro zašifrování, slouží jako nástroj identifikace a zabezpečení. Díky výše uvedeným faktům, je téměř nemožné ji padělat a velmi obtížné zneužít třetí stranou.

1.5. Základní terminologie z oblasti kryptoměn

Blockchain – Systém, seznam validovaných bloků. Každý z bloků je napojený na svého předchůdce až k bloku původnímu (genesis block).

Genesis block – Původní blok v blockchainu, který byl použit pro spuštění

[4] JUDMAYER, Aljosha, Nicholas STIFTER, Katharina KROMBHOLZ a Edgar WEIPPL. *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms*. Morgan & Claypool Publishers, 2017. ISBN 9781627057165.

[5] HUJOVÁ, Gabriela, ed. *Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti*?: sborník z konference: Praha, 26. března 2014. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. ISBN 978-80-86847-71-9.

kryptoměny.

Hash – Digitální identifikace binárního vstupu.

Miner – Vstup výpočetního výkonu tvořící uzel v síti (network), který na základě konceptu proof – of – work dešifruje hash, tím zprocesuje požadovanou operaci a dostane odměnu.

Poplatky – Poplatky mají dvě strany. Poplatek za transakci – standardně v kryptoměně, ve které je transakce zadána. Poté je odměňována opačná strana, kdy je přiznána odměna těžařům (miners) za dešifrování hashe a dokončení pokynu.

Proof – of – work – Část dat, která potřebují určitý počet výpočetního výkonu k dohledání a vyřešení operace k exekuci úkonu. Výpočetní výkon je určený podle nodů připojených do networku v blockchainu.

Smart contracts – Počítačový kód napsaný tak, aby za každých okolností ctil své zákonitosti a podmínky. Nahrazuje tedy nutnost uzavírání skutečných smluv. Exekuce kontraktu je tak v plné režii systému na základě jeho technické parametrizace.

Adresa – Veřejný klíč – jedná se o řadu (string) písmen a čísel, která reprezentuje konkrétní kryptoměnovou peněženku např. 32tUpMJL2bHWDqhPupYF9vB6W7fqB5vurD. Adresu ve správném tvaru může příjemce sdílet odesílateli, který na danou adresu může provést transakci, jež je pak pomocí blockchainu zpracována.

Transakce – Transfer kryptoměny z jedné adresy na druhou. Transakce jsou zprocesovány dle principů dané kryptoměny např. na principu Proof – of – Work.

Konfirmace – Jakmile se dostane transakce do bloku v blockchainu, má jednu konfirmaci. Poté, co se vytěží další block ve stejném blockchainu, má transakce dvě konfirmace, a tak dále. Pokud má transakce šest a více konfirmací, považuje se za dostatečně ověřené, že transakce nemá být anulována.[6]

Peer – to – peer neboli P2P je všeobecné označení v IT, kdy jsou si v síti všechny

[6] 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.

uzly navzájem rovny a komunikují spolu napřímo bez potřeby centrálního uzlu. Nejčastěji se jedná o počítačovou síť.

Fork – Modifikovaný blockchain, který změní původní pravidla bloků v blockchainu. Jedna část těžící skupiny pozměněný blok příjme a druhá část z nějakého důvodu se změnou nesouhlasí, a tudíž jej neakceptují. Zůstane tedy původní verze, avšak zároveň vznikne i nová – fork. Může však docházet i k tzv. soft forku, kdy se celá komunita shodne na nových změnách a nevznikne tak odštěpená verze, pouze se inovuje ta stávající.[7]

Peněženka – Softwarový nástroj pro uchování kryptoměnových adres a jejich bezpečnostních klíčů. Použitelný pro zadání, přijímaní transakcí a uchování držených kryptoměn.

Soukromý klíč (private key) – Jedná se o neveřejný klíč, který slouží tvůrci peněženky k přístupu, potvrzení operace či k dešifrování jemu určené zprávy.

Whitepaper – dokument, který vydává společnost, vývojový tým za účelem popisu a vysvětlení technických parametrů a záměru celého projektu. Standardně obsahuje časovou osu projektu, jak bude daná kryptoměna distribuována a kdo za projektem stojí.

*Ponziho schéma-„*Ponziho schéma je pojmenováno po Charlesovi Ponzim, který v roce 1920 jako první využil unikátní struktury získávání prostředků od investorů. Investoři, kteří se zapojili do sítě dříve, jsou vyplaceni se ziskem, avšak prostředky na vyplacení poskytli investoři, jež se zapojili později. Jedná se o druh podvodného jednání, kdy poslední investoři ztratí svou investici, protože byla vyplacena jiným investorům jako odměna. Podmínkou pro dlouhodobé trvání takovéto struktury je pravidelný přísun prostředků od nově zapojených investorů“. [8]

[7] NARAYANAN, Arvind. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, [2016]. ISBN 9780691171692.

[8] Ponzi Scheme. *Investor.gov: Types of Fraud* [online]. Washington, DC [cit. 2019-02-11]. Dostupné z: https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme

2. Historie kryptoměn

2.1. Kryptoměny před Bitcoinem

Před Bitcoinem si můžeme všimnout náznaků a pokusů o tvorbu dokonalého a funkčního kryptografického produktu, jenže i když nějaký produkt vznikl, nikdy se nedostal až k veřejnosti, aby se mohl rozrůst do velikosti kryptoměn. Prvním průkopníkem se stal až Bitcoin, který dokázal spojit obecnou kryptografii a elektronické digitální platby tak, aby vznikla funkční decentralizovaná kryptografická měna.

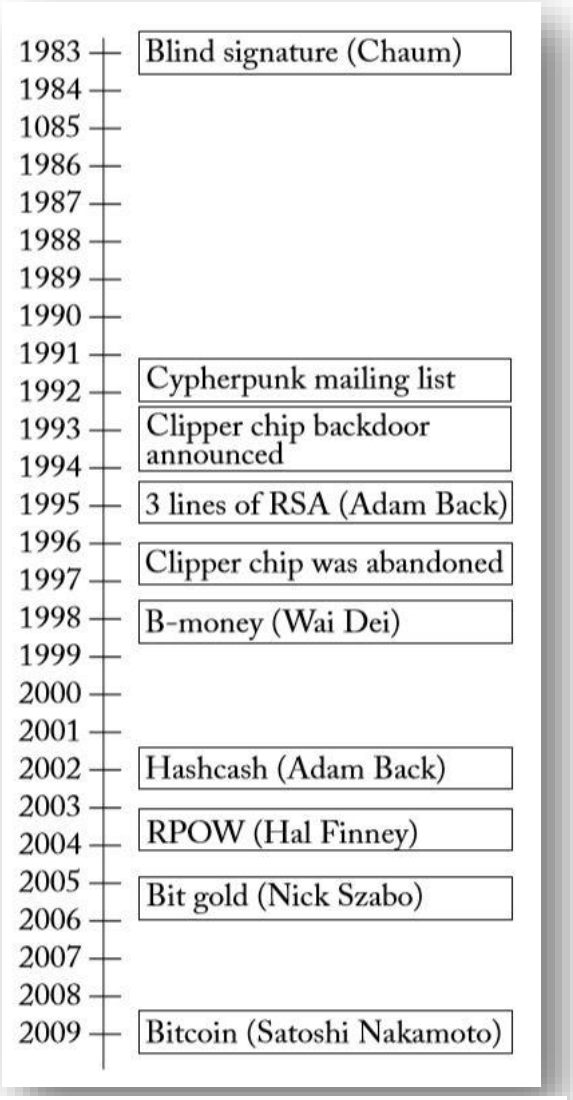
Kryptografie je matematická disciplína zabývající se problematikou šifrování, kdy se záměrně šifruje informace a bez znalosti klíče k dešifrování, nelze informaci přečíst. Kryptografie se dělí na symetrickou a asymetrickou. „Symetrická kryptografie je postavena na znalosti jednoho klíče, který šifruje i dešifruje požadovanou informaci. Při asymetrické kryptografii jsou vytvořeny dva rozdílné klíče – jeden, který zprávu zašifruje, a druhý, který nese logiku pro rozluštění“.[9] Asymetrická kryptografie se používá pro zabezpečení a funkci Bitcoinu.

Vraťme se ale k úplným začátkům moderní kryptografie. Za zmínku stojí David Chaum, kterému je často přisuzováno vyvinutí zabezpečené digitální hotovosti, a to již v osmdesátých letech dvacátého století. Jeho produkt byl v dané době revoluční, nicméně, i když byl marketingově silně podporován, široká veřejnost jej nepřijala za svůj a tím jeho myšlenka upadla v zapomnění.

Projekt Cypherpunk navázal na práci Davida Chauma, dokázal poskytnout kryptograficky zabezpečené technologie rozsáhlejší skupině lidí, kteří využívali Cypherpunku ke komunikaci pomocí zabezpečených e-mailových zpráv. Cypherpunk obsahoval některé klíčové vlastnosti definující nynější podobu kryptoměn, jako jsou např. komunikační diskrétnost a anonymita.

Další projekty se již přibližovaly myšlence dnešních kryptoměnových produktů, nebyly však plně decentralizovány.

[9] Symmetric cryptography. *IBM®: Knowledge Center* [online]. 1994 [cit. 2019-02-11]. Dostupné z: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.15/gtps7/s7symm.html



Obrázek č. 1. Brzké začátky digitálních peněz (Blocks and Chains Introduction to Bitcoin, Cryptocurrencies, and their Consensus Mechanisms)

V roce 1998 se poprvé zapojil Nick Szabo započetím vývoje svého projektu Bit Gold, narazil však na problém s dublováním transakcí. Jeho produkt měl napodobovat chování zlata jakožto komodity, aby tomu zabránil.[10]

Adam Black v roce 2002 představil jeden z prvních a významnějších projektů postavených na konceptu proof – of – work (PoW). Nazýval se Hashcash. Myšlenkou bylo vytvořit hash, jenž půjde jen velmi obtížně dohledat, ale snadné vyřešit. Odesílatel e-mailu tak měl být uchráněn případných spamových útoků. Důležité z hlediska historie je znovu využití PoW v Bitcoin miningu.

Projekt RPOW využil systému PoW a teorie přenositelnosti od Nicka Szaba, kdo zvolil za vzor zlato. Hal Finney, tvůrce RPOW, představil tokenové peníze, které stejně jako v Bit Goldu byly vázány na hodnotu zlata.

Údajně po vzniku Bitcoinu byl Han Finney první osobou, která obdržela transakci v Bitcoinu, a sice přímo od Satoshiho Nakamota.

2.2. Vznik a nástup Bitcoinu

První kryptoměna svého druhu vznikla v roce 2009 a byla pojmenována Bitcoin. Údajně název vznikl ze slovního spojení Bit gold, projektu, za nímž stál Nick Szabo. Byl pomyslným předchůdcem kryptoměn, jaké známe dnes. Druhou část názvu nové jednotky měny tehdy tvůrci vybrali podle mince (z angl. „coin“), tudíž byl název intuitivně zkrácen na Bitcoin.

„Tvůrcem a otcem myšlenky je Satoshi Nakamoto, jehož identita není známa a s největší pravděpodobností se jedná o pseudonym jednoho člověka nebo skupiny více lidí, odborníků na kryptografii, matematiku a informatiku, kteří stojí za celým projektem. Po

[10] SZABO, Nick. Bit Gold. *Satoshi Nakamoto Institute* [online]. 29.12.2005 [cit. 2019-02-12]. Dostupné z: https://nakamotoinstitute.org/bit-gold/

dokončení první publikovatelné verze, na níž Satoshi Nakamoto pracoval mezi lety 2007 a 2009, předal server Bitcoin.org pozdějšímu hlavnímu vývojáři projektu Gavinovi Andersonovi.“[11]

Gavin v práci pokračoval a v roce 2012 založil Bitcoin foundation, která se stará o komunitu sdružující se okolo Bitcoinu a jeho vývoje. Kdo skutečně je Satoshi Nakamoto dodnes s jistotou nevíme. Existuje několik spekulací, avšak žádná z nich nebyla nikdy potvrzena. Nejžhavějšími kandidáty na postavy stojící za pseudonymem Nakamota jsou Vladimír Oksman, Neal King, Charles Bry. Velká část zainteresovaných osob tvrdí, že by Nakamotem mohl být samotný Nick Szabo, který stál za myšlenkou „smart contracts“ a Bit goldu.

[11] 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.

Co je to bitcoin?

Bitcoin historicky první kryptoměna. Bitcoin i většina dalších kryptoměn, stojí na několika základních pilířích, vlastnostech, které je definují a dávají jim smysl, unikátnost, cenu.

Jednou z nejvíce vyzdvihovaných vlastností je decentralizovanost. Decentralizovanost znamená, že neexistuje žádný centrální bod, který by ovlivňoval ostatní, a jsou tak zcela nezávislé, neovlivnitelné, což představuje velkou výhodu oproti centralizovanosti a všeobecně centralizovaným měnám.[12]

Centralizované databáze, kryptoměny, představují pravý opak, jsou přímo závislé na jádru, centru, které je esenciálním bodem celé sítě. Po narušení či kompletní změně tohoto centra ztratí celá síť spojení, nebo to může zapříčinit její zánik. Rizikem centralizace je zneužitelnost díky přílišné moci v rukou jednotlivců.

Samotný Bitcoin stojí na základech distribuované, decentralizované peer-to-peer síti známé jako blockchain. Síť je autonomní, nikdo ji nevlastní, ani ji nemůže ovlivňovat, není vázaná na obrovské datové sklady, nýbrž běží na zařízeních milionů lidí, kteří se dobrovolně do sítě připojili, ať už z důvodu podpory komunity, anebo pro odměnu za umožnění provedení výpočetního úkonu pro vyřešení/dešifrování hashů v blockchainu.[13]

Další důležitou vlastností Bitcoinu je jeho pseudo anonymita. Bitcoin není plně anonymní kryptoměnou jako je např. Monero. Pseudo anonymní znamená, že provedený kontrakt je přímo dohledatelný spolu s adresou a hodnotou transakce, kdo však danou peněženku vlastní nikdo nezjistí.[14]

Důležitými vlastnostmi Bitcoinu, které jej dělají nejdůvěryhodnější kryptoměnou pro uložení svých prostředků jsou: nezávislost z důvodu decentralizace, neregulovanost a pseudo anonymita. Vlastník s nimi nakládá, jakkoli potřebuje, přičemž jeho jednání neregistruje žádná třetí strana.

Vstupem Bitcoinu na světlo světa nevznikla pouze alternativní měna, ale hlavně se uskutečnil další krok kupředu v oblasti IT technologií. Od jeho prvního spuštění se udála

---

[12] TAPANG, Carlos. Will Cryptocurrencies Replace Fiat?. *Medium: Coinmonks* [online]. 06.05.2018 [cit. 2019-03-14]. Dostupné z: https://medium.com/coinmonks/will-cryptocurrencies-replace-fiat-732ca57b751b

[13] ANTONOPOULOS, Andreas M. *Mastering bitcoin*. Sebastopol CA: O'Reilly, 2015. ISBN 9781491902608.

[14] ANTONIA, Cameron. Bitcoin for dummies. Indianapolis, IN: John Wiley, 2016. ISBN 9781119076131.

spousta změn a postupných zdokonalení. Cena Bitcoinu je momentálně znovu na pomyslném úpadku, nicméně po technologické stránce ještě nikdy nebyl Bitcoin tak vyspělý, jako je tomu nyní. Následkem těchto zdokonalení má velký předpoklad nejen se na trhu udržet, nýbrž i zopakovat svůj „raketový růst".

Proč je Bitcoin stále kryptoměnou č. 1.?

Denně se v oběhu zobchoduje okolo 10 miliard dolarů Bitcoinu, i kvůli tomu o Bitcoinu hovoříme jako o nejsilnější a nejstabilnější kryptoměně.[15] Zájem o Bitcoin nijak rapidně neklesá – spíš naopak. Za jeho vývojem stojí silná komunita, která pomocí technologických úprav zdokonaluje Bitcoin jako produkt tak, aby byly provedené transakce co nejrychlejší a poplatky se snižovaly. Co však Bitcoin činí ve světě kryptoměn skutečným lídrem, je nejvyšší tržní kapitalizace a s tím spojena i větší stabilita, což zvyšuje i důvěru investorů v samotný Bitcoin. Z hlediska investice, se tak jeví jako nejméně rizikový. Má největší příslib zhodnocení vložených prostředků, ať už z dlouhodobého hlediska – držení – nebo jako nástroj pro spekulaci na trhu s kryptoměnami.

Bitcoin od svého vzniku v roce 2009 inspiroval mnoho dalších technologických nadšenců a expertů, díky čemuž vznikly tisíce dalších kryptoměnových projektů. Valná většina z nich stojí na základě právě Bitcoinového blockchainu.

[15] *Coinmarketcap* [online]. 2013 [cit. 2019-03-27]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/#charts

3. Blockchain – technologie kryptoměn

3.1. Blockchain jako technologický základ kryptoměn

„Kryptoměny jsou ve své technologické podstatě závislé na dvou typech datových struktur, a to na struktuře transakcí a bloků. Transakce jsou sdružovány do bloků. Bloky jsou propojeny mezi sebou skrze hashe svých předchůdců (mimo Genesis block – úplně první, vstupní blok), čímž se vytváří ověřená datová struktura, tzv. blockchain. Transakce a bloky jsou rozptýleny mezi všechny účastnící se nody, které jsou propojeny na základě škálovatelného protokolu přes peer-to-peer síť."[16]

Blockchain virtuálně ztělesňuje databázi zaknihovaných transakcí, primárně v sobě nese transakční historii, již nelze žádným způsobem přepsat zpět. Každá z transakcí, která je do bloku napevno propsána a veřejně zpřístupněná, musela nejdříve projít procesem zadání virtuální transakce. Transakce proběhne za předpokladu, že debetní strana zná adresu nebo veřejný klíč peněženky kreditní strany. Debetor zvolí konkrétní částku pro zadání. Zadavatel transakci stvrzuje svým privátním klíčem, čímž se propíše jeho digitální podpis, který nese detaily celé transakce – adresa kreditní strany a množství převáděné kryptoměny. Po zadání této transakce však musí dojít k jejímu ověření, aby došlo k finální exekuci a připsání prostředků do peněženky příjemce.[17]

Zajímavé srovnání tradičního systému s technologií blockchainu sepsal William Mougayar: „Tradiční způsob sdílení dat pomocí psaných dokumentů (např. Microsoft Word) je snadné, požádáte druhou osobu o kontrolu a čekáte, než se na to „podívá". Problém spočívá v tom, že než se vám vrátí opravená kopie, nemůžete vidět změny nebo sami nějaké provádět, protože jste zaseknutí v bodě, kdy čekáte na dokončení editace druhou osobou. Na tomto principu fungují databáze v dnešní době. Dva vlastníci dokumentu nemohou zároveň vstupovat do stejného záznamu. Podobně fungují i banky, když připisují transakce na účet a mění tak zůstatek. Dočasně uzamknou přístup pro změny, provedou potřebné operace, změní stav na druhé straně a znovu přístup povolí. Např. aplikace Google Docs dokáže zprostředkovat přístup

[16] JUDMAYER, Aljosha, Nicholas STIFTER, Katharina KROMBHOLZ a Edgar WEIPPL. *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms*. Morgan & Claypool Publishers, 2017. ISBN 9781627057165.

[17] SWAN, Melanie. *Blockchain: blueprint for a new economy*. O´Reilly: Sebastopol, 2015. ISBN 978-1-491-92049-7. The Bitcoin Primer – Risks, Opportunities, And possibilities by David Seaman

jednoho dokumentu, jedné verze více uživatelům najednou a je pro ně vždy viditelná, pokud mají povolený přístup. Je to podobný princip ala zaknihované transakce v blockchainu. Představme si, že by šly takto sdílet všechny dokumenty. Namísto nekonečného přeposílání jednoho dokumentu jeden druhému. Mezitím může dojít ke ztrátě orientace nad aktuální verzí. Proč nejsou všechny business dokumenty sdílené namísto přeposílání tam a zpět?“[18] V těchto případech by se hodilo využít technologie blockchainu.

3.2 Mining

Mining neboli těžení je způsob generování, získání kryptoměn a zprocesování kryptoměnových transakcí, založený na proof–of-work konceptu, kdy přidanou hodnotou je elektrická energie spotřebovaná na výpočetní výkon těžebních strojů. Těžba je výpočetní proces, kdy za pomoci hardwarového výkonu těžební přístroje hledají další bloky pro připojení do sítě blockchainu. Blok může být dohledán pouze, pokud splňuje aktuální podmínky obtížnosti pro jeho vytěžení – tzv. difficulty. Obtížnost je momentální nastavení sítě a vzhled požadavků na potřebné množství výpočetního výkonu, aby byla naplněna podmínka proof-of-work. Parametr obtížnosti se mění rozdílně u každé kryptoměny. Například u Bitcoinu je to každých 2016 bloků, aby docházelo ke zpracování jednoho bloku za deset minut.[19]

Hashovací rychlost (hash rate)

„*Veličina udávající míru výpočetního výkonu uzlu nebo celé bitcoinové sítě. Její jednotkou je h/s – počet spočtených hashů za sekundu. Odvozené jednotky jsou 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). Výkon celé sítě se mezi léty 2009-2013 zvýšil z 1 Mh/s na 10 Ph/s (tj. rozdíl o 10 dekadických řádů)*“ [20]

Typy těžících nástrojů

V úplných začátcích nebyla obtížnost na vyřešení bloků tak vysoká, jako je tomu dnes. Stačily menší výpočetní výkony, tudíž nebyly tolik velké hardwarové nároky.

---

[18] MOUGAYAR, William. *The business blockchain: promise, practice, and application of the next Internet technology*. Hoboken, New Jersey: John Wiley & Sons, [2016].

[19] BARSKI, *Conrad. Bitcoin for the befuddled*. San Francisco, CA: No Starch Press, 2014. ISBN 1593275730.

[20] 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.

První mineři zvládli obstojně těžit na svých desktopových zařízeních a laptopech. Konkrétně se zpočátku využívalo procesorových čipů (CPU), jejichž výkon je však opravdu nízký. Tito uživatelé v prvopočátcích těžili relativně velké objemy za nízkou cenu. V tu dobu však cena jednoho Bitcoinu ani zdaleka nedosahovala cenu jednoho dolaru, tím pádem se jednalo spíše o „anarchistickou" komunitu přidružených fanoušků, jež netěžila s vidinou většího výdělku.

Další metou byla tvorba těžebních sestav, které již nevyužívali výkonu CPU, ale výkonu grafických karet (GPU), nejčastěji pak přirozeně těch výkonnějších určených primárně pro hraní počítačových her (GTX). Toto uzpůsobení časem s rostoucí náročností již na vytěžení bloku nestačilo, tak těžaři začali stavět mining-rigy. Mining-rigem označujeme speciální počítačovou sestavu, která se skládá ze základních počítačových komponentů, ale volí se základní deska s větším počtem socketů, do nichž se vsadí několik grafických karet. Díky popularitě kryptoměn a zvýšenému zájmu o těžbu vznikla komponentní krize, kdy rapidně vzrostla cena herních grafických karet a obecně všichni výrobci nestíhali vyrábět součástky ani pro běžné uživatele.

ASIC miners představují speciálně navržené počítače vyvinuté pouze pro jeden konkrétní účel – těžení kryptoměn. ASIC minery jsou často výkonnější než klasické mining-rigy, mají však jednu nevýhodu, dají se použít jen pro jednu, maximálně dvě konkrétní kryptoměny. Oproti tomu standardní, ručně vytvořený rig lze snadno použít k duálnímu těžení a dojde-li ke změně podmínek těžby původně těžené kryptoměny, lze jej jednoduše upravit a začít s jeho pomocí těžit kryptoměnu úplně jinou.[21]

Mining – pools odkazují na sdružení vícero mining-rigů, ASIC minerů na jednom místě. Pooly vznikají z několika důvodů. Hlavní důvod zní zvýšení celkového výpočetního výkonu, čehož se docílí spojením. Účastníci poolu tak mají mnohem větší šanci, že vyřeší daný hash právě oni, o celkovou odměnu se potom tedy logicky podělí. Dalším – jistě neméně důležitým – faktorem je také cena elektrické energie nutně spotřebované na těžbu. Jakožto větší celek

[21] SWANSON, Tim. *The Anatomy of a Money-like Informational Commodity: A Study of Bitcoin*. San Francisco: Tim Swanson, 2014. ASIN: B00MEAO7XK.

zpravidla vysmlouvají výhodnější tarif za energie.[22] Praktickým příkladem je první Bitcoin mining pool svého druhu, který byl založen již v roce 2010 v České Republice.[23]

Od doby, kdy cena některých kryptoměn spadla pod hranici, pod níž se už jednotlivcům nebo malým skupinám nevyplatí z finančních důvodů těžit, se těžba celoplošně přesouvá k těžařským velmocem. Světové těžbě jednoznačně dominuje Čína, a to hlavně ze dvou důvodů – velmi nízkých nákladů na energie a také lehké dostupnosti potřebných přístrojů, zejména ASIC minerů.

Jak přistupovat do blockchainu?

Do blockchainu jsou tři možnosti připojení – plným klientem (taktéž tlustým klientem), tenkým klientem a webovým přístupem.

Plný klient neboli „full client“, také známý jako “full node“ klient, je připojení přímo ke zdroji transakční knihovny v blockchainu. Obsahuje tak každou transakci ze strany všech uživatelů, kteří do daného blockchainu kdy vstoupili. Jedná se tedy o napojení napřímo bez zprostředkování třetí stranou.

Tenký klient, „lightweight client“, závisí na třetí straně, která obstarává interface pro vstup do kryptoměnové sítě. Tenký klient v sobě neuchovává kompletní historii transakcí, jako je tomu u plného klienta. Transakce nejsou zpracovávány napřímo, validace v tomto případě probíhá ve spolupráci s třetí stranou.

Webový klient slouží k přístupu do kryptoměnové peněženky zprostředkované třetí stranou přes aplikaci ve webovém prohlížeči.

Výběr provedený uživatelem v rámci široké škály veškerých přístupů čistě závisí na tom, do jaké míry uživatel potřebuje kontrolovat své prostředky. Plný klient zajišťuje největší kontrolu, nicméně zároveň vyžaduje největší technickou zdatnost a zvyšuje se riziko chyby při tvorbě zálohy. Nejjednodušší přístup i prvotní nastavení jde přes webového klienta, zde opět vzrůstá riziko z důvodu znalosti přihlašovacích údajů provozovatelem aplikace. Pokud by se někdo do aplikace naboural hrozí ztráta všech prostředků.

[22] LEE, David. *Handbook of digital currency: bitcoin, innovation, financial instruments, and big data*. Amsterdam: Elsevier/ AP, [2015]. ISBN 9780128021170.

[23] *Slushpool* [online]. 2010 [cit. 2019-03-20]. Dostupné z: https://slushpool.com/home/

4. Rizika kryptoměn a jejich zneužití

4.1. Rizika kryptoměn

Kryptoměny od svého vzniku zažily mnoho nadějných růstů a dramatických pádů. Řídí se stejnými zákonitostmi jako každý jiný trh, jen se jeho role v tomto světě ještě neustálila, a tak jsou výkyvy mnohem častější, než se děje u již dlouho živoucích ekonomik.

Z hlediska investičních příležitostí jsou kryptoměny považovány za jedny z těch nejrizikovějších. Proč tomu tak vlastně je?

Kryptoměny se vyznačují vysokou volatilitou, trend trhu je ovlivňován velkými subjekty, které vědomě ovlivňují křivku vývoje trhu a tím jí zvednout strmě nahoru, ale i do extrémně nižších hodnot. Z takového dna už se jednou nemusí zvednout a celý projekt „umře“. Velkým rizikem pro „spekulanty“ na trhu je také pozdní nastoupení, což znamená, že koupí kryptoměnu o velké hodnotě, která jest z dlouhodobého hlediska neudržitelná, a při poklesu mohou být rázem ve velké ztrátě. Prostředky obětované tímto nákupem se již nemusí nikdy zvrátit.

Samotným rizikem je také logika exekuce transakcí v blockchainu. String sice nese poslední znaky, které kontrolují součet (zabezpečení proti zadání nevalidní adresy z důvodu špatného opsání/zkopírování) v rámci bezpečnostní prověrky, jenomže pokud zadá odesílatel validní adresu, která však nepatří požadovanému příjemci, nelze platbu zvrátit, ani vrátit.

Riziko týkající se kryptoměn se dotýká také samotných těžařů, kteří investují obrovské množství financí do těžebních přístrojů, jejichž návratnost a ziskovost je přímo závislá na vývoji trhu těžené kryptoměny. Změna podmínek pro těžbu daného bloku může přirozeně velice ovlivnit výhodnost těžení. V současné době se potýká mnoho minérů s nevýhodnými podmínkami a zvažují, zda podnikání ukončit, pokračovat dál ve ztrátě, či investovat do nového hardwaru.

Velkým rizikem, které se již několika jednotlivcům draze nevyplatilo, je ztráta přístupových údajů do svých peněženek či zapomenutá existence v minulosti získaných kryptoměn, např. vytěžením, ponechané na harddisku, který nebyl uschován nebo jej již nemá.

Obrovským rizikem se vyznačují nedůvěryhodné projekty nepodložené existujícím produktem nebo nezaštítěné realistickým business plánem a kompetentním vývojovým týmem. Na vytvoření profilu důvěryhodné kryptoměny se zaměřím v praktické části bakalářské práce.

Risk může být zisk, co se kryptoměn týká, zdá se to však být čím dál těžší díky obrovskému nárůstu nových projektů a ICOs.

ICO

Initial Coin Offerings – jsou začínající projekty, určitá forma startupu v kryptoměnách. Tvůrci nových projektů pomocí ICO vybírají peníze na realizaci své myšlenky, vývoj technologie nebo úplně nového produktu. Standardně fungují ICOs formou vygenerování určitého počtu mincí, kterým určí cenu dle období, ve kterém se zrovna projekt realizuje. První prodejní dávka je takto učiněna nejvýhodnější a s přibližujícím se časem vypuštění do produkce se cena dále zvyšuje.[24]

Problém projektů stojících na podpoře ICO tkví zejména v neregulovanosti a nulové záruce. Často se tak stává, že podvodníci operují se zkázonosným záměrem vybrat prostředky od důvěřivých investorů a potom celý projekt sabotují, nebo jej úplně zruší. Investoři tím ztrácí své vložené prostředky, které často bývají zaplaceny v již ověřených měnách, nejčastěji pak v Bitcoinu nebo Ethereu.

Není vždy pravidlem, že ICO projekty jsou tzv. „Scam" podvodný projekt, bez reálných úmyslů funkčního provozu. Ve skutečnosti jsou ICO projekty zajímavou příležitostí nejvyšších a rychlých výdělků, bohužel 90% ICOs se do produkce nikdy nedostanou a většina z nich zanikne.

4.2. Zneužívání kryptoměn

Zneužití anonymity kryptoměn

Díky specifickým vlastnostem, především tedy jejich pseudo anonymitě a kompletní anonymitě, se staly kryptoměny novým nástrojem na praní špinavých peněz, k ukrývání nezdaněných příjmů, ale také k nákupu nelegálních látek a předmětů na černém trhu.

Výhodou pro zločinné organizace je právě tolikrát zdůrazňovaná anonymita. Jejich účty jsou skryté pod pseudonymem a je velmi obtížné skutečného vlastníka dohledat, až se to stává úplně nemožným úkolem. Tím, že v oběhu je obrovské množství transakcí, je o to těžší

[24] Glossary: Cryptocurrency and Blockchain Glossary: A-Z. *CrushCrypto* [online]. [cit. 2019-03-20]. Dostupné z: https://crushcrypto.com/glossary/

podezřelou transakci zachytit. Kde však lidé tyto zločiny a nekalé praktiky osnují? Na odvrácené straně internetu – Darknetu.[25]

Darknet vznikl v 80. letech 20. století. Je to prostor, kde se schází podsvětí z různých koutů světa a s různými záměry. Na Darknetu se obchoduje např. se zakázanými látkami, jako jsou ty dopingové, drogy, nebo také s odcizeným zbožím, uměním, zbraněmi a uživatelskými daty. Velmi žádanými se stále častěji stávají osobní data a přihlašovací údaje, hesla nebo čísla platebních karet s PIN kódy.

Na Darknetu se setkávají také hackeři, kteří zde sdílí své zkušenosti nebo se nechávají najímat na konkrétní zakázky. Obrovské oblibě, která stále narůstá, je platba za nelegální činnost v kryptoměně, často je zmiňován samotný Bitcoin, nebo potom větev kryptoměn s důrazem na anonymitu, jako je např. Monero nebo Zcash.[26]

Hackeři

Kryptoměnový hackeři nebo také kryptozloději jsou většinou technicky velmi zdatní jedinci, kteří znají architekturu kryptoměn a zneužívají toho k vlastnímu či cizímu obohacení. K získání nedostatečně zabezpečených prostředků používají různé metody.

Nejméně závažným způsobem je podstrčení těžícího softwaru hostiteli. Uživatel si nevědomě nainstaluje aplikaci, která na pozadí krade jeho výpočetní výkon pro těžbu, vytěžené mince jsou pak odesílány do peněženek. Zajímavou alternativou je napadení webové stránky v prohlížeči. Webová stránka obsahuje v javascriptové knihovně zakódovanou informaci s příkazem k využití CPU návštěvníka, ten pak po dobu návštěvy stránky poskytuje svůj výpočetní výkon.

Jako velké riziko obecně vidíme přihlašování se na nezabezpečených veřejných sítích, kde je každý připojený uživatel vystaven riziku připojení cizí entity a instalaci škodlivého softwaru.

Ransomware – Vyšším stupněm získání kontroly nad uživatelskými daty je využití cryptovirů, jako jsou ransomware, malware. Pokud se vám do systému dostane virus typu ransomware, často dojde k zašifrování souborů, které bez potřebného klíče neodemknete.

[25] MALIK, Nikita. How Criminals And Terrorists Use Cryptocurrency: And How To Stop It. *Forbes* [online]. 31.08.2018 [cit. 2019-02-18]. Dostupné z: https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#7ec5f0923990

[26] BUNTINX, JP. The Role of Cryptocurrency in Crime – Darknet Activity Soars. *Null TX* [online]. 2014, 08.06.2018 [cit. 2019-03-20]. Dostupné z: https://nulltx.com/the-role-of-cryptocurrency-in-crime-darknet-activity-soars/

Takovýto útok je často proveden s vidinou výkupného za odemčení dat. Některé malwary vás však mají za úkol pouze sledovat a zasílat data útočníkovi. Ten se pak s potřebnými údaji, jako jsou přihlašovací údaje, hesla nebo dokonce privátní klíče, může dostat k vaším prostředkům a odcizit je.

Virové útoky jsou mířeny i na jednotlivce, hlavním cílem však nejčastěji bývají velké kryptoměnové směnárny, burzy a peněženky. Za zmínku stojí několik známých případů, kdy došlo ke ztrátě prostředků klientů z důvodu prolomení ochrany poskytovatele služby.

1. Mt. Gox

Hackerský útok na Japonskou Bitcoinovou směnárnu byl proveden 19. června 2011. Útočníci se nabourali do celého systému a zcizili 2609 BTC. Zajímavé na kauze Mt. Gox je to, že byli napadeni znovu v roce 2014, kdy hackeři tentokrát ukradli zůstatky uživatelů, které skýtaly více než 750,000 BTC, a společnost zbankrotovala.[27]

2. Bitfinex

Druhým největším útokem z hlediska ztráty financí bylo hacknutí kryptoměnové burzy Bitfinex. Hackeři odcizili sumu o hodnotě 120,000 BTC. Bitfinex však útok ustál a většinu prostředků svým klientům refundoval.

Útoky s popularitou a rozmachem kryptoměn stále rostou a jsou čím dál tím důmyslnější, dokonalejší. Věnujte zvýšenou pozornost zabezpečení, kvůli útokům, je potřeba provádět preventivní opatření, aby vaše prostředky nebyly dosažitelné a naprosto zranitelné.

[27] KHATWANI, Sudhir. Top 5 Biggest Bitcoin Hacks Ever. *Coinsutra* [online]. 2017, 13.10.2018 [cit. 2019-03-20]. Dostupné z: https://coinsutra.com/biggest-bitcoin-hacks/

Praktická část

5. Prevence odcizení kryptoměny

Základem prevence ztráty vašich kryptoměnových prostředků je jejich kvalitní zabezpečení. Aby nedošlo ke ztrátě vašich údajů, vždy si vytvořte vlastní „Backup“ klíč, díky němuž později případně znovuobnovíte přístup ke svým financím.

Nejdůležitější prevencí je bezpečné uložení vašeho soukromého klíče. Způsob uložení soukromého klíče se dělí na dva typy, tzv. „Cold“ a „Hot“.

„Hot“ metoda uložení soukromého klíče je forma, při níž je klíč uložený na zařízení s přístupem na internet. Výhodou je přístupnost a pohodlnost při zadávání transakcí.

„Cold“ metoda zálohy klíče naopak bez přístup na internet, a tudíž je mnohem bezpečnější.

5.1. Držení na kryptoměnových směnárnách a burzách

Obecně se nedoporučuje držet dlouhodobě větší objemy prostředků, uložených na kryptoměnových burzách a směnárnách, a to hned z několika důvodů. Jedná se v podstatě o ekvivalent banky v kryptoměnovém světě, kdy záměrně centralizujete své vklady a zabezpečení necháváte na třetí straně. Zpravidla se jedná o webové klienty v prohlížeči, tím pádem už jen díky tomuto faktu jsou vaše prostředky zranitelnější. Pokud však chcete jít touto cestou, je vhodné mít k tomuto přístupu vyhrazen zvlášť prohlížeč, který na nic jiného nepoužíváte. Osobně doporučuji prohlížeč Brave, za kterým stojí vývojářský tým kryptoměny BAT (Basic attention token), který je mimořádně dobře zabezpečený. Nezapomeňte na dvoufaktorové zabezpečení (2FA). Např. pomocí přihlašovacího jména s heslem a zasláním kódu pro potvrzení na ověřené zařízení prostřednictvím aplikace Google Authenticator. Dvoufaktorové zabezpečení zajišťuje mnohonásobně vyšší ochranu před odcizením vašich prostředků. Bohužel v dnešní době již hackeři umí prolomit i tento druh obrany.

5.2. Online kryptoměnová peněženka

Lepším způsobem zabezpečení je vytvoření vlastní kryptoměnové peněženky. Zde už se jedná o decentralizovaný způsob, kdy však rozhraní pro správu vaší peněženky vám zprostředkovává třetí strana. Pro vytvoření vlastní peněženky slouží mnoho webových i mobilních aplikací, některé kryptoměnové peněženky však mají i svého tlustého klienta.

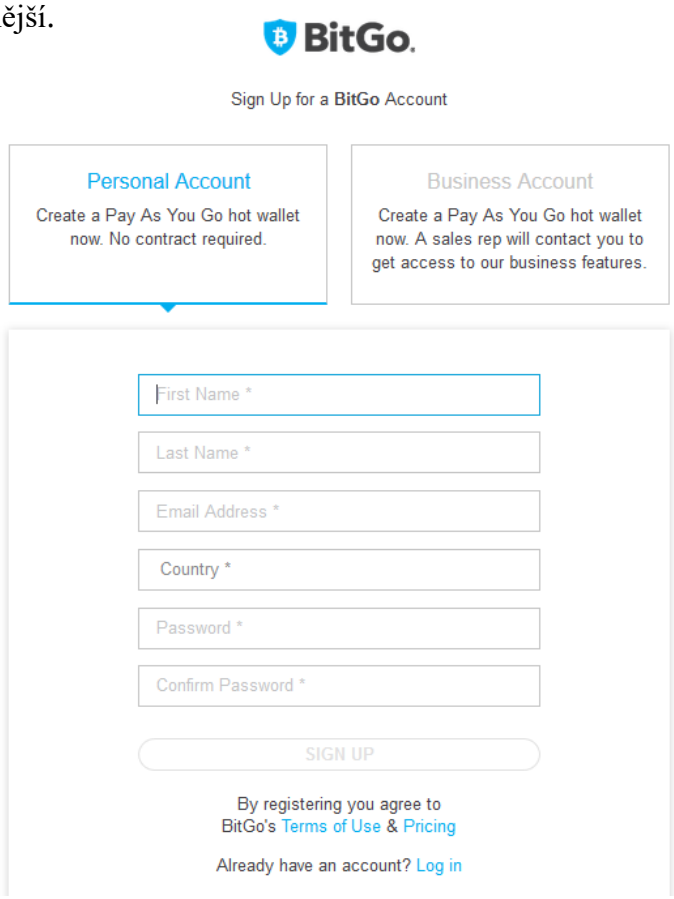
Vytvoření online kryptoměnové peněženky je velice snadné. Stačí si vybrat jednu z desítek dostupných peněženek, vytvořit si uživatelský účet stejně jako v případě kteréhokoliv tenkého klienta. Vybírejte peněženky dle ověřenosti, zabezpečení a také podporovaných kryptoměn. Pomocí přihlašovacích údajů a hesla se pak přihlásíte do uživatelského rozhraní. Doporučuji nastavit 2FA způsob přihlášení, některé aplikace to přímo vyžadují pro okamžité zvýšení bezpečnosti.

Pro podrobný návod, jak vytvořit online kryptoměnovou peněžneku jsem vybral aplikaci BitGo.com.

BitGo peněženka se zobrazuje ve dvou rozlišných formách – ve formě podnikatelského účtu a osobního. Rozdíl je v dodaných funkcích a nutnosti v podnikatelském módu uzavřít smlouvu.

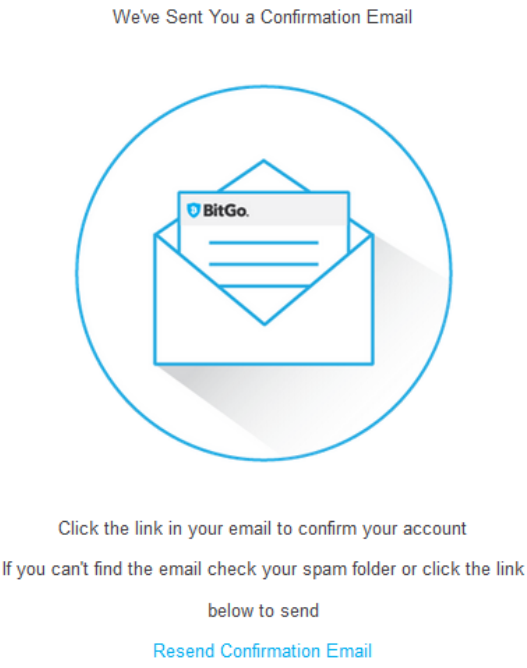
Jak si založit kryptoměnovou peněženku online?

Vyplňte všechny povinné údaje a nezapomeňte si zvolit velmi silné heslo. Doporučuji použít velká a malá písmena v různém pořadí, dále nezapomeňte na číslice a speciální znaky, jako jsou např. &, #, @. Čím delší heslo bude, tím bude obtížnější pro potenciální útočníky prolomit a tedy bezpečnější.



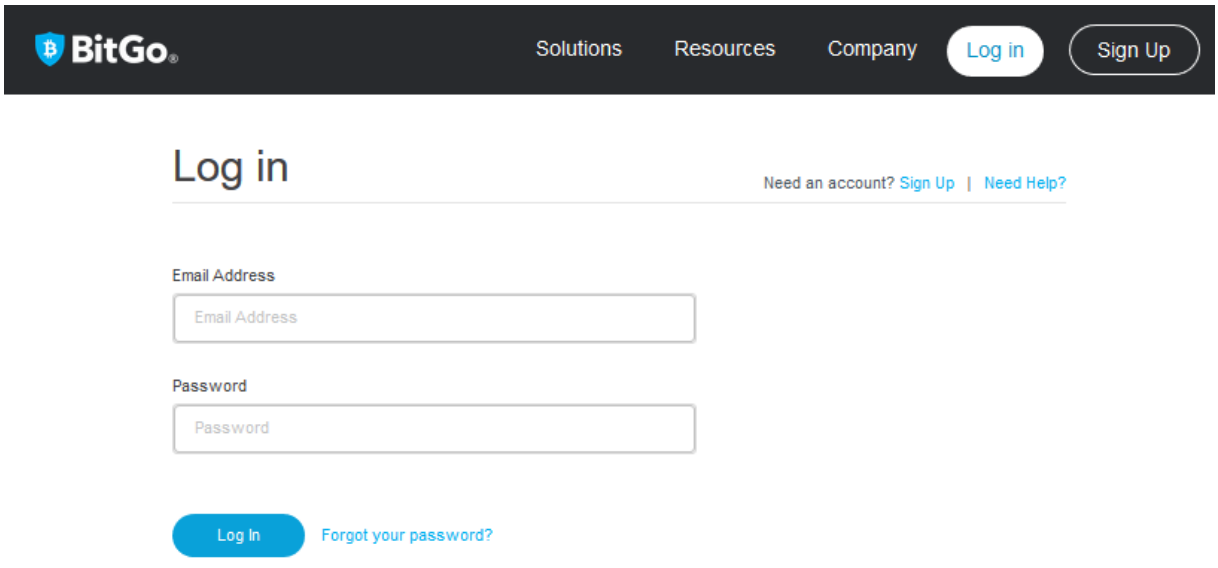
Obrázek č. 2 - https://www.bitgo.com/info/signup

BitGo vám zašle aktivační, autorizační zprávu na předem zvolenou e-mailovou adresu.



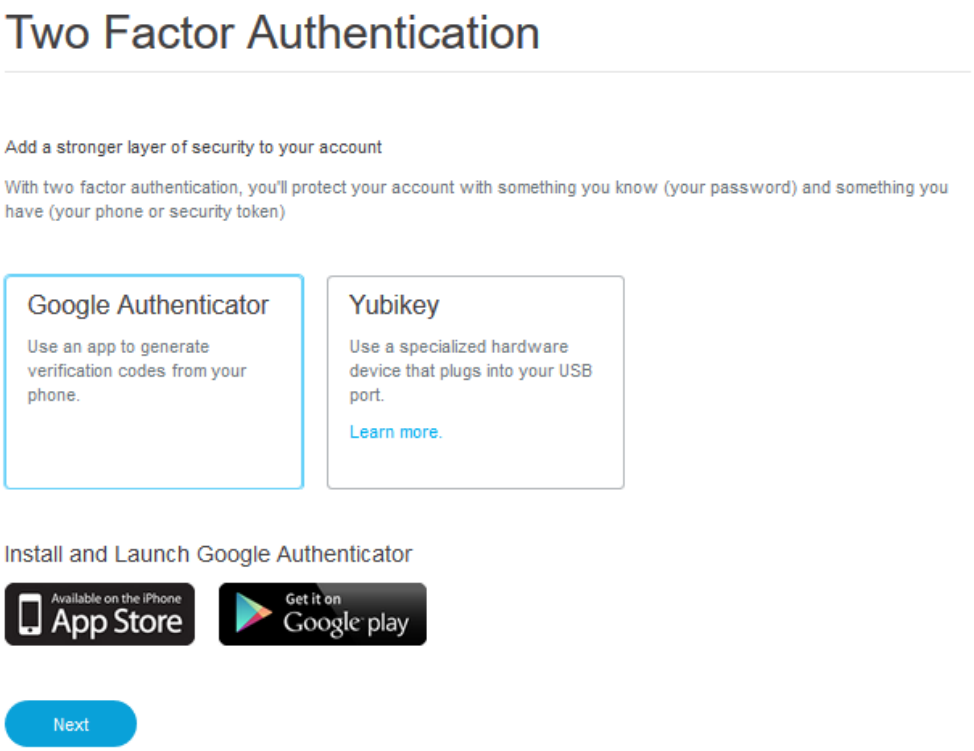
Obrázek č. 3 - https://www.bitgo.com/info/signup

Po provedení aktivace budete přesměrování zpět na server BitGo pro přihlášení pomocí vašich údajů zadaných v prvotní registraci.



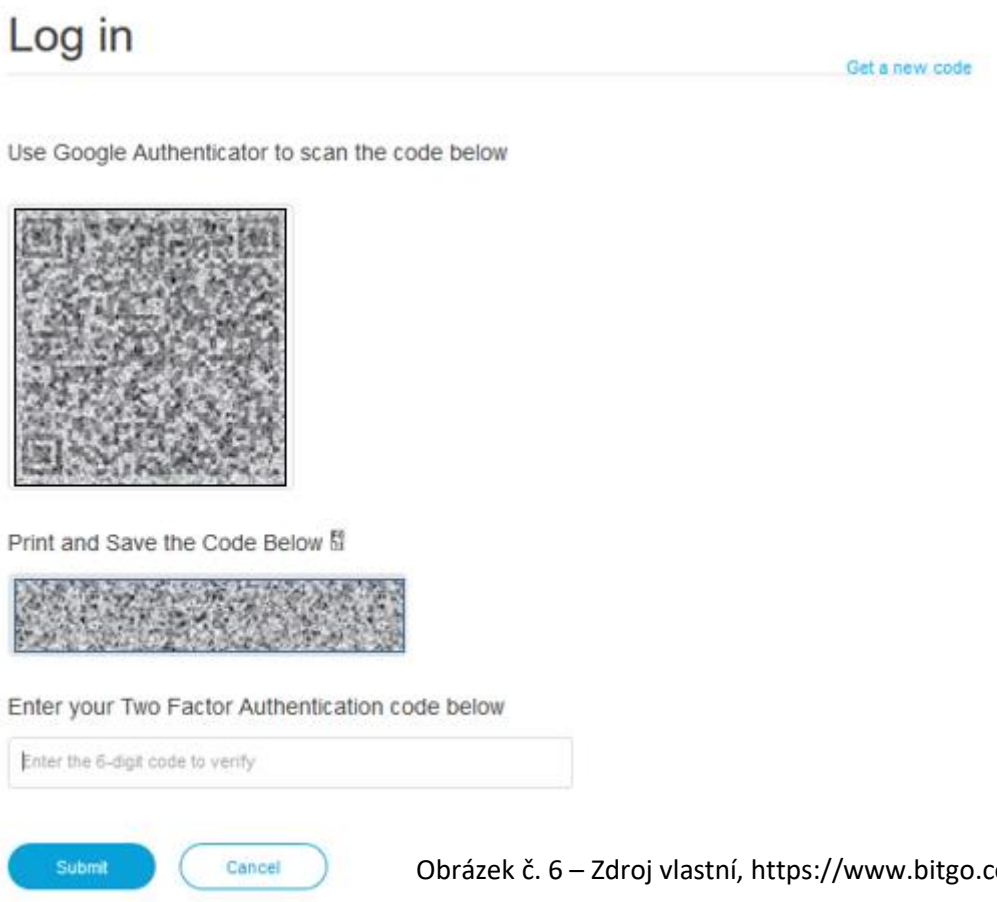
Obrázek č. 4 - https://www.bitgo.com/login

Po přihlášení budete vyzváni ke zvolení druhého faktoru pro přihlašování. U BitGo nemáte jinou možnost, bez 2FA to nepůjde. Výběr máte hned ze dvou možností. Mezi aplikací Google Authenticator, která je běžně používanou metodou i u jiných aplikací. Aplikace Google Authenticator funguje na principu spárování druhého zařízení s uživatelským účtem, kdy při každém pokusu o přihlášení, autorizaci je vygenerován jednorázový kód s platností jedné minuty. Yubikey je hardwarovou alternativou autorizace, kdy při každé vyžádané autorizaci vložíte Yubikey do USB portu, potvrdíte stisknutím tlačítka na daném zařízení, a tak dojde k validaci. Yubikey je často kombinován s password managerem a považujeme jej za nejvyšší stupeň zabezpečení pro online přihlašování. Pro založení nové peněženky využiji častějšího a jednoduššího způsobu přes Google Authenticator.



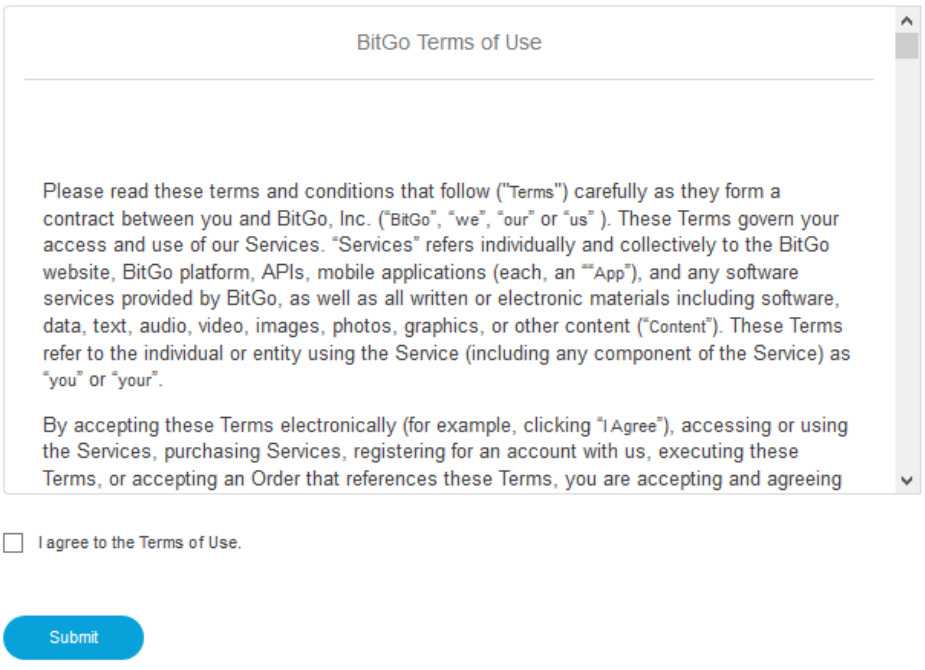
Obrázek č. 5 – Zdroj vlastní, https://www.bitgo.com

Pro absolvování dalšího kroku je podmínkou mít staženou a nainstalovanou aplikaci z Google Play (Android) nebo App Store (iOS). Poté vstoupíte do aplikace Google Authenticator a provedete propojení s BitGO. Nejjednodušší způsob zahrnuje oskenovat QR kód, nebo můžete provést aktivaci přepsáním kódu z registrace. Po propojení je vám již systémem vygenerován první kód pro dokončení spárování.



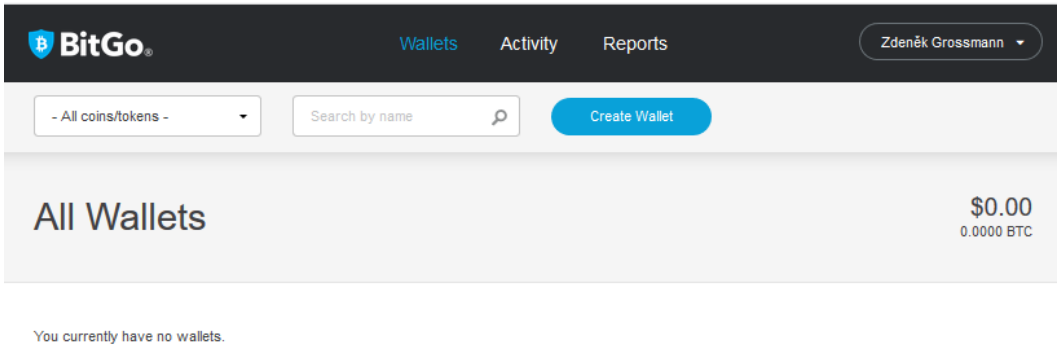
Obrázek č. 6 – Zdroj vlastní, https://www.bitgo.com

Po spárování už stačí jen potvrdit podmínky užití aplikace a váš uživatelský účet je vytvořen.



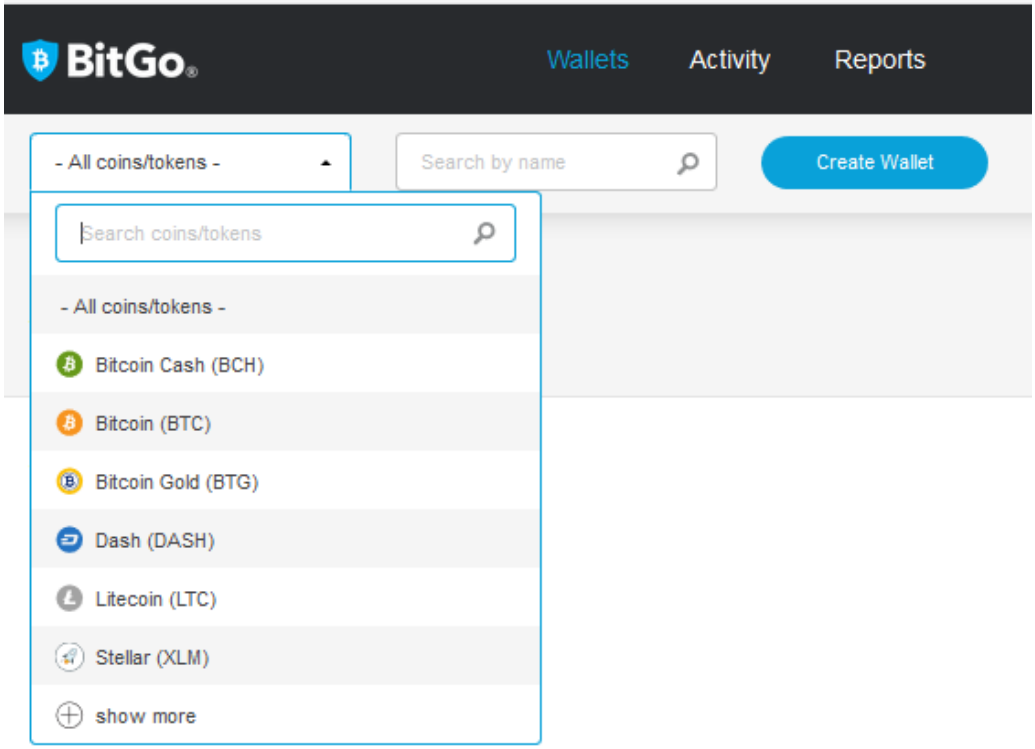
Obrázek č. 7 – Zdroj vlastní, https://www.bitgo.com

První, co se vám zobrazí, je přehledová stránka, kde naleznete přehled nad všemi svými peněženkami, dále uživatelské funkce pro sledování aktivity a reportů.



Obrázek č. 8 – Zdroj vlastní, https://www.bitgo.com/enterprise/personal/walletsListings

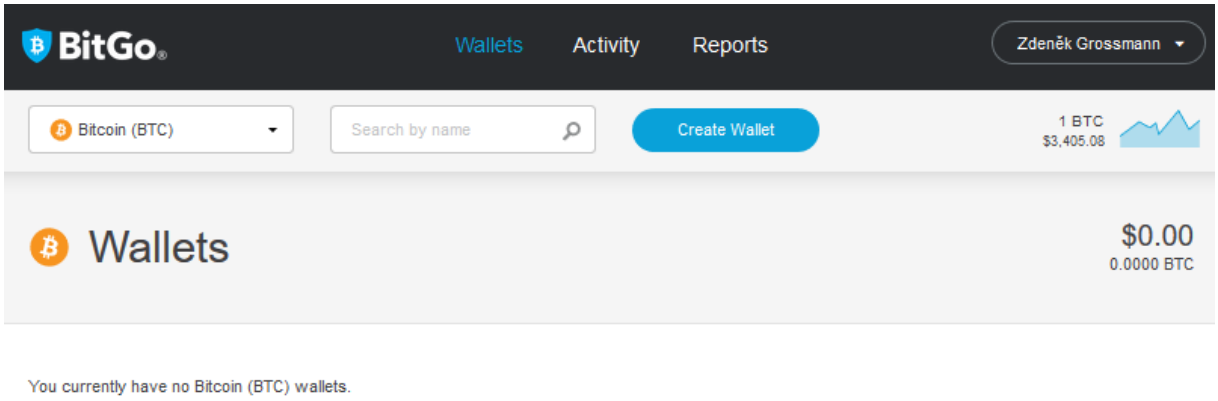
V textovém poli „All coins/tokens“ zvolíte do kontextu dle vašeho zájmu libovolnou kryptoměnu z nabídky. Tento výběr slouží jak pro přehled zůstatků, tak pro vybrání kryptoměny do kontextu, abyste si mohli vytvořit svou první kryptoměnovou peněženku.



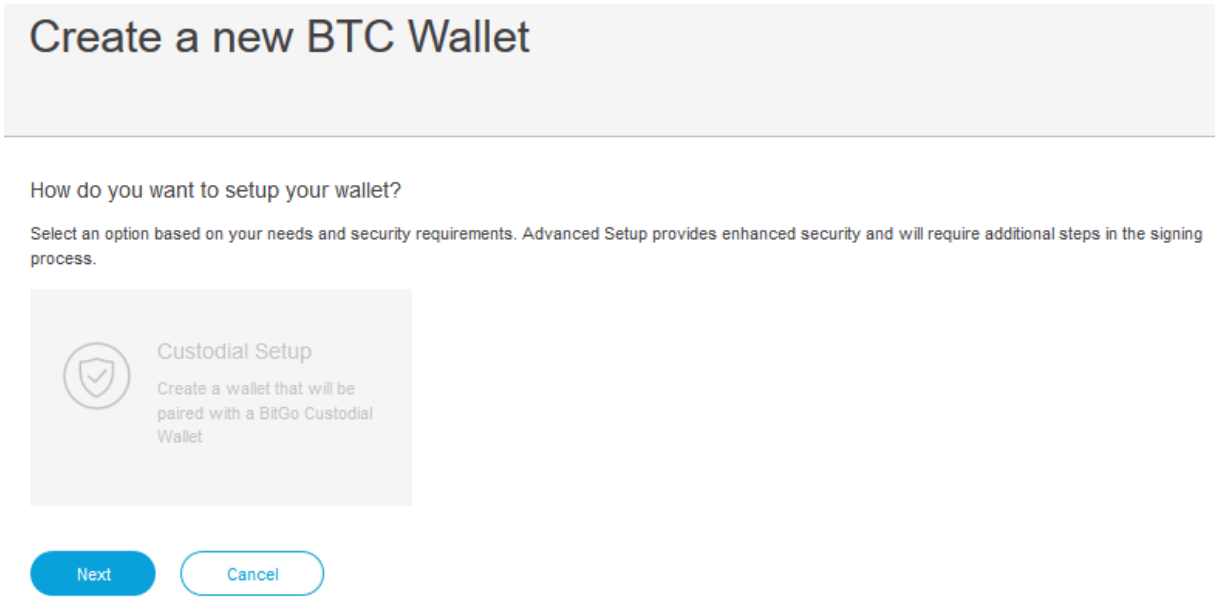
Obrázek č. 9 – Zdroj vlastní,https://www.bitgo.com/enterprise/personal/walletsListings

Pro demonstraci jsem si vybral Bitcoin. Po vybrání kryptoměny už stačí kliknout jen na tlačítko „Create Wallet“, což spustí proces založení nové krypto-peněženky. Během procesu hned v prvním kroku akceptujete fakt, že zprostředkovatelem peněženky je třetí strana –

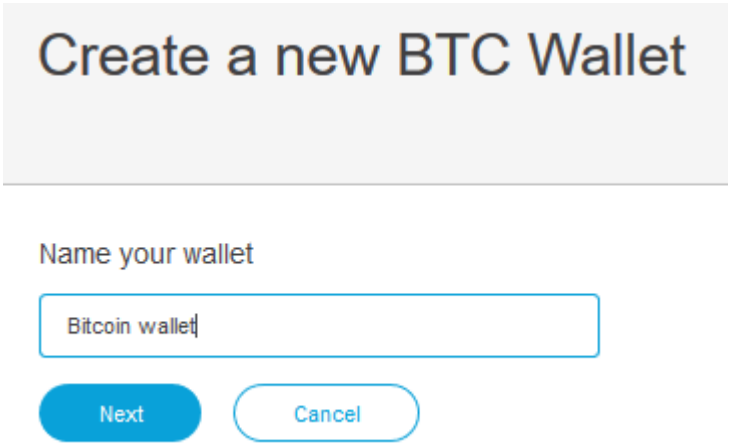
v našem případě společnost BitGo. Libovolně si pojmenujte svou peněženku a zvolte způsob zabezpečení pro autorizaci vašich transakcí. Bezpečnějším způsobem rozhodně volíme rozdílné heslo pro přihlášení do peněženky a pro autorizaci.



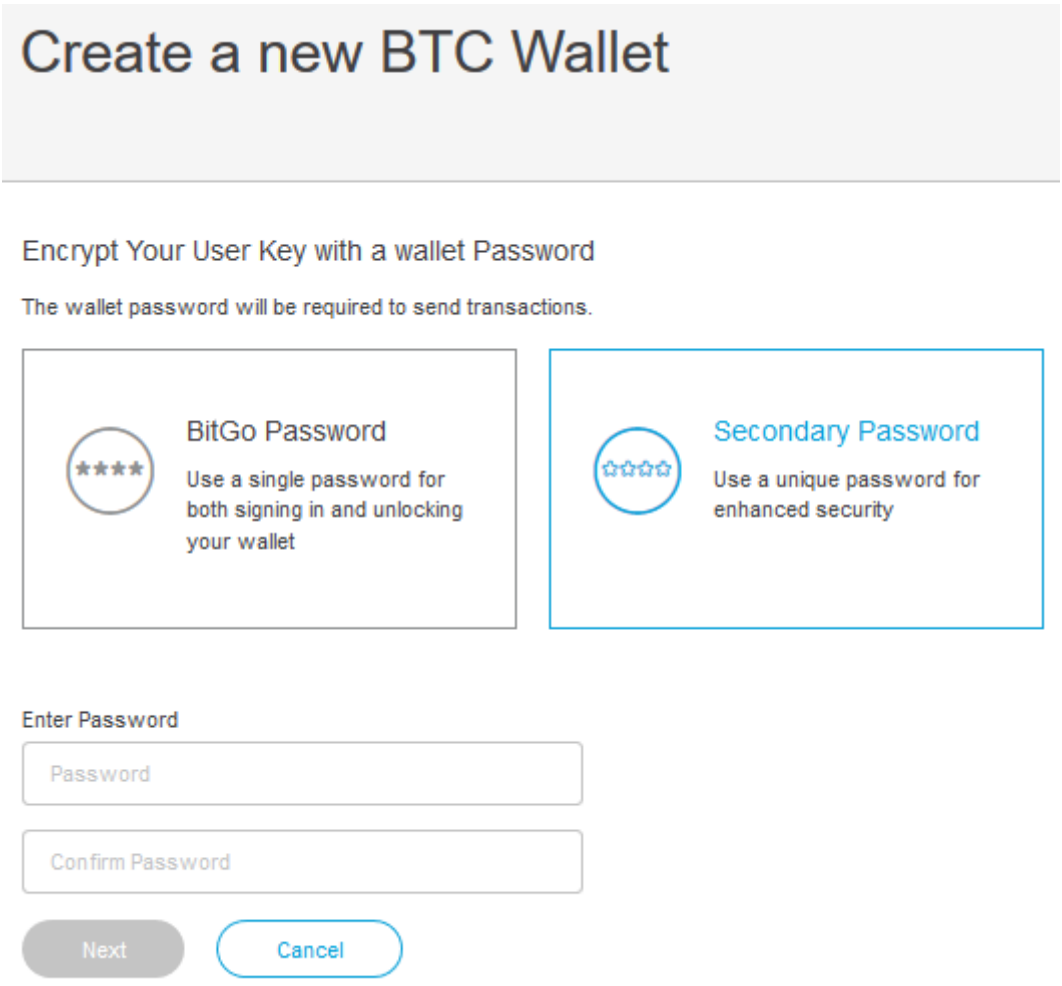
Obrázek č. 10 – Zdroj vlastní, https://www.bitgo.com/enterprise/personal/walletsListings



Obrázek č. 11 – Zdroj vlastní, https://www.bitgo.com/enterprise/personal/coin/btc/create/landing

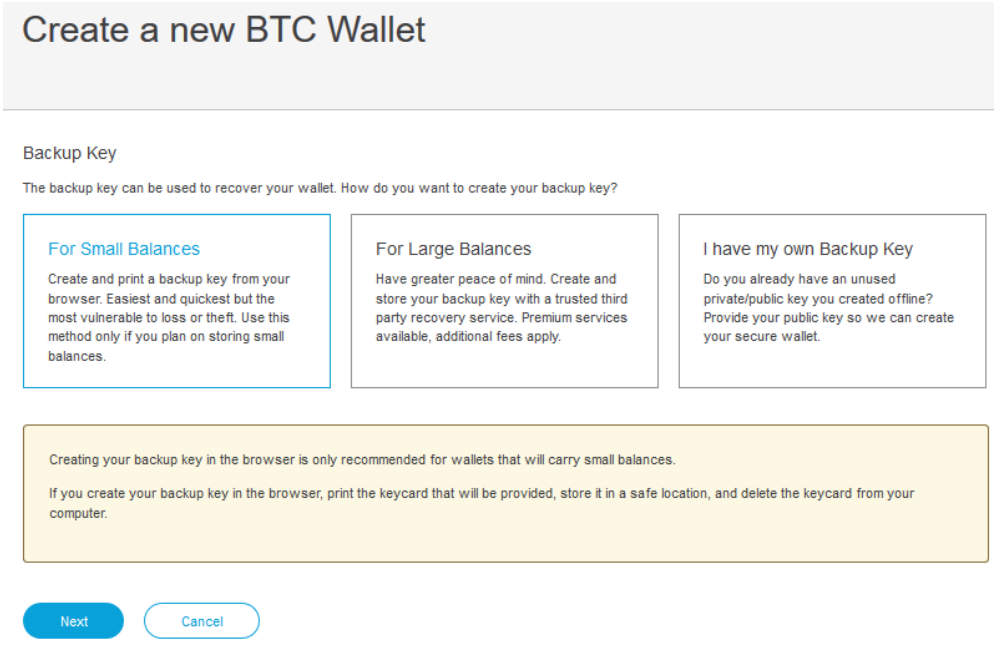


Obrázek č. 12 – Zdroj vlastní, https://www.bitgo.com/enterprise/personal/coin/btc/create/label



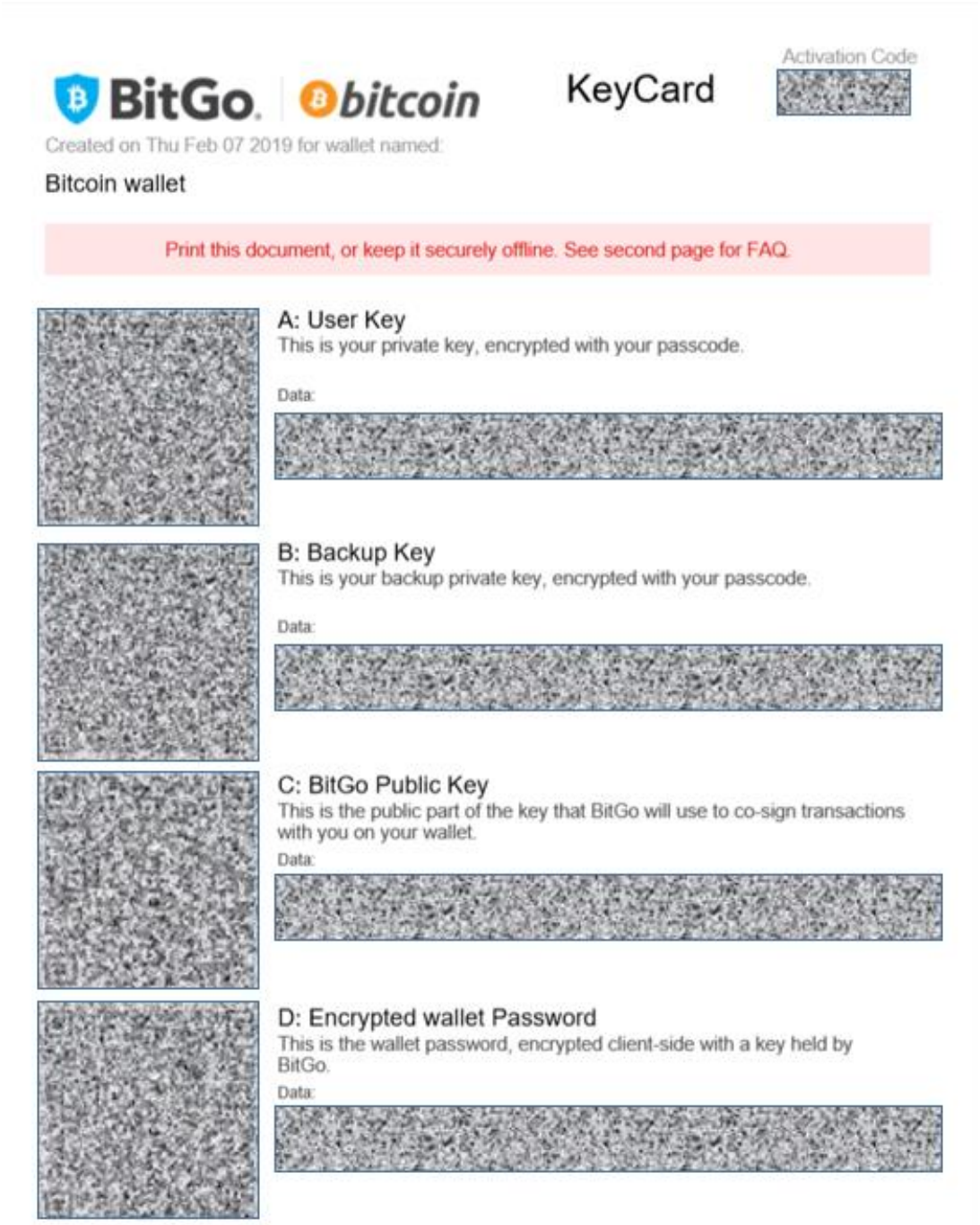
Obrázek č. 13 – Zdroj vlastní, https://www.bitgo.com/enterprise/personal/coin/btc/create/userKey

Velmi důležitou část představuje vytvoření záložního klíče. V BitGo máte hned tři možnosti. Vygenerování záložního klíče přes webový prohlížeč, což je nejrychlejší, nejsnadnější, ale také nejvíce náchylné k odcizení. Druhá varianta je vytvoření „backup“ klíče přes důvěryhodnou aplikaci třetí strany, tato forma je však zpoplatněna, stojí 99 dolarů. Třetí možností je využití již existujícího záložního klíče, tudíž nemusíte vytvářet nový. Pro ukázku jsem zvolil nejjednodušší variantu, která je doporučená jen, pokud plánujete v peněžence držet menší obnosy prostředků.



Obrázek č. 14 – Zdroj vlastní https://www.bitgo.com/enterprise/personal/coin/btc/create/backupKey

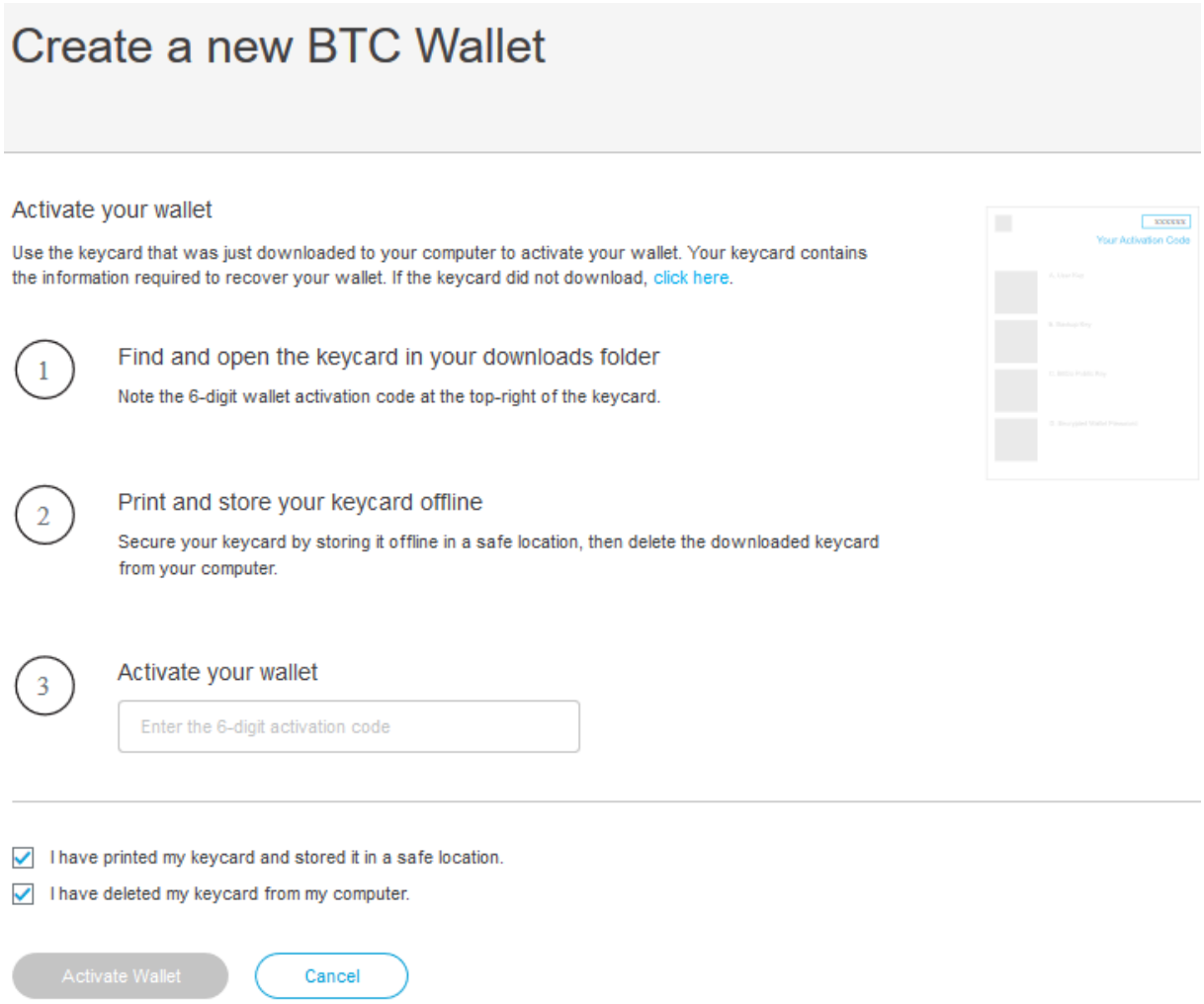
Ihned, jakmile zvolíte metodu pro vytvoření karty s klíči, se vám přes internetový prohlížeč začne stahovat soubor ve formátu pdf. Po otevření dokumentu a jeho následném prostudování, v něm naleznete hned několik důležitých údajů. Tím prvním je aktivační kód, který potřebujete pro dokončení vaší kryptoměnové peněženky. Dalším esenciálním údajem bude vaše heslo zašifrované do soukromého klíče. Dále zde obdržíte již zmiňovaný backup klíč. BitGo public key je údajem, kterým zprostředkovatel schvaluje vaše transakce, aby byly zprocesovány. Posledním klíčem je zašifrované heslo do vaší peněženky společně s částí, kterou u sebe drží třetí strana. Všechny tyto údaje mají své specifické QR kódy, díky kterým můžete provádět autorizace rychleji. Důležitým krokem u těchto vygenerovaných souborů s jednotlivými hesly je jejich zálohování na bezpečné místo. V ideálním případě si je vytiskněte a poté trvale smažte, případně uložte na zařízení bez přístupu na internet.



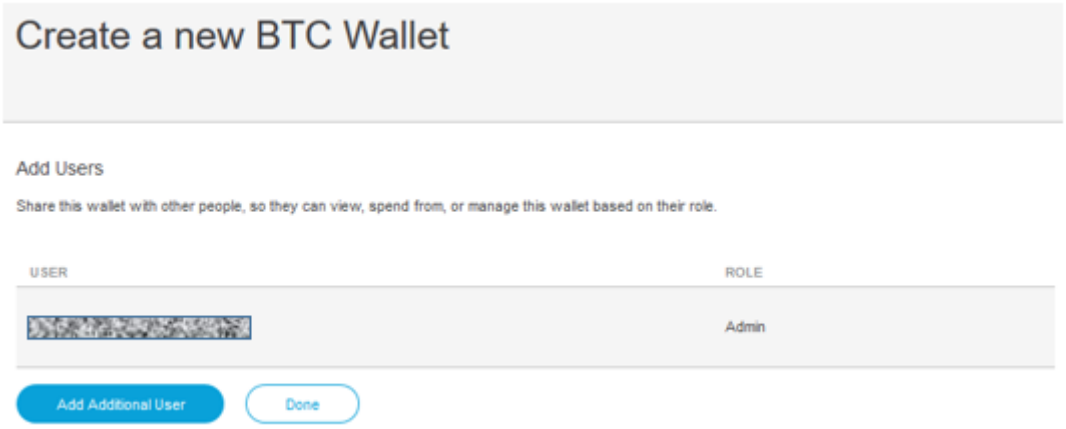
Obrázek č. 15 – Zdroj vlastní, BitGo KeyCard

Pro dokončení žádosti musíte znát aktivační kód ze souboru s klíči. Daný kód vepíšete do pole pro aktivaci vaší nové kryptoměnové peněženky. Poté už jen potvrdíte checkboxy s poučením o správném zacházení s privátními klíči a vaše první kryptoměnová peněženka je hotová.

V posledním kroku můžete spravovat rozdělení dispozic k peněžence a definovat role.

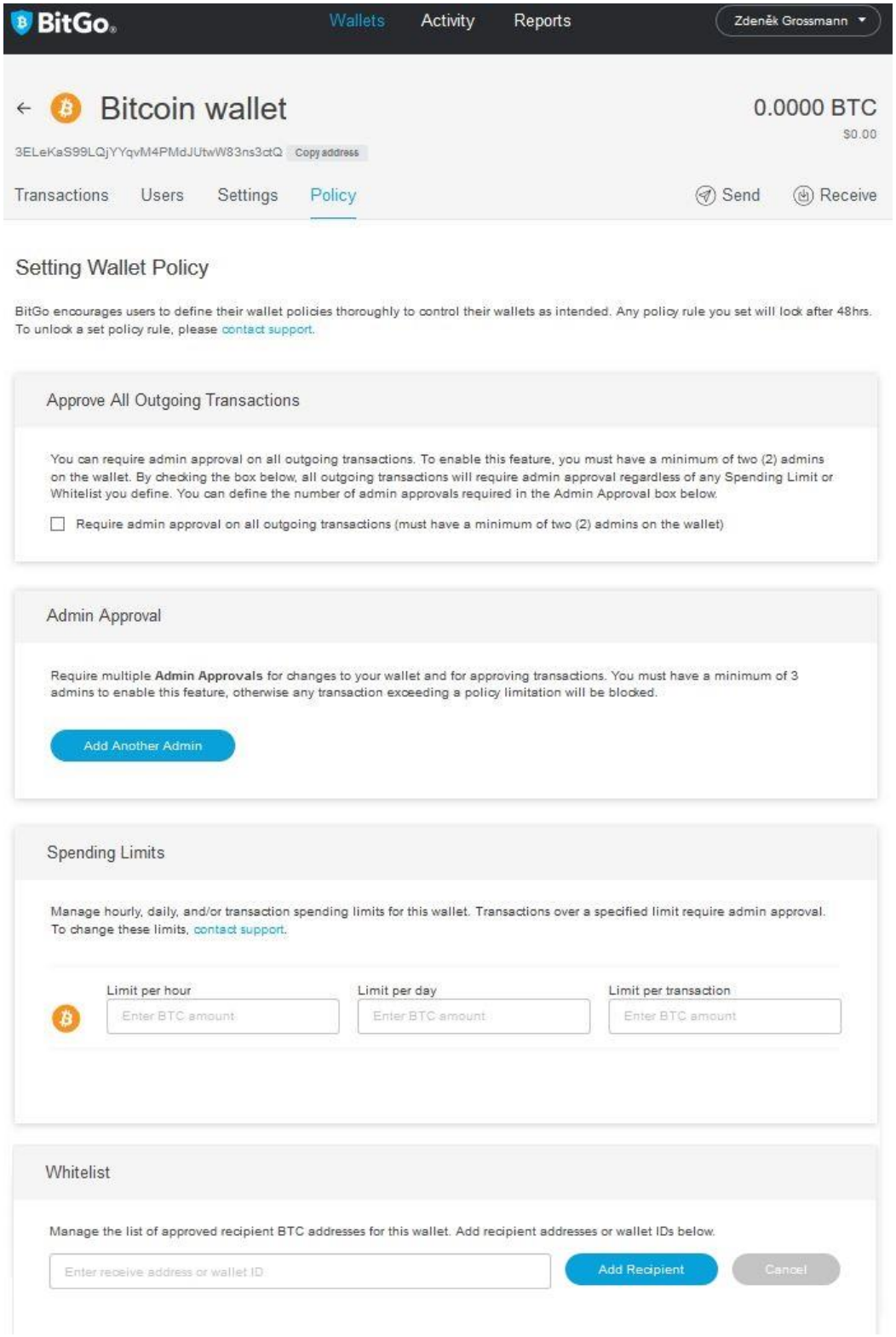


Obrázek č. 16 – Zdroj vlastní, https://www.bitgo.com



Obrázek č. 17 – Zdroj vlastní, https://www.bitgo.com

Po dokončení celého procesu vytvoření vaší peněženky je připravena k plnému užívání. V dodatečném nastavení ovládáte prvky, jako jsou podmínky pro autorizace transakcí disponentem, nastavení limitů, a hlavně pak příjem a odesílání kryptoměnových transakcí.



Obrázek č. 18 – Zdroj vlastní, https://www.bitgo.com/enterprise/personal/walletsListings

BitGo.com jsem vybral z důvodu míry jeho rozšíření a nízké náročnosti pro založení první kryptoměnové peněženky. Na trhu se však setkáváme s mnoha obdobnými aplikacemi, každá se něčím odlišuje, díky čemuž může více vyhovovat potřebám určitého klienta.

Další příklady ověřených online peněženek:

Electrum - https://electrum.org/

Exodus - https://www.exodus.io/

Pro mobilní zařízení např. https://edge.app/

Další formou ještě silněji zabezpečených prostředků jsou papírové peněženky.

5.3. Papírová kryptoměnová peněženka

„Papírové kryptoměnové peněženky (anglicky „Paper Wallets“) jsou jedním ze způsobů „Cold“ zálohovaných privátních klíčů. Papírové peněženky se zakládají na offline zařízeních, kde se vytvoří adresa i privátní klíč, avšak tyto informace se nikdy se neukládají, vlastník si údaje opíše k sobě na papír. Zejména privátní klíč by si měl každý účastník uložit na bezpečné místo. Nic pak nebrání tomu, aby vám byly zasílány prostředky na vaši kryptoměnovou adresu. Komplikace nastávají v momentě, kdy chcete provést transakci z vaší strany. Buď musíte vzít svůj privátní klíč a použít jej online, což aplikace umožňují, tím se však zruší váš statut „Cold“ a změní se na „Hot“, přičemž se z vaší papírové peněženky stává online peněženka. Pokud se však jedná o nárazovou akci, jakmile je zdárně ukončena, můžete vytvořit novou papírovou peněženku a prostředky z původní (teď již online) peněženky na ni přeposlat.“[28]

Nejvyšší stupeň zabezpečení skýtají hardwarové krypto-peněženky.

5.4. Trezor & Ledger

Hardwarové peněženky jsou malá zařízení zpravidla podobná USB flash disku. Jejich úloha však spočívá zejména v ochraně vašich privátních klíčů. Hardwarové peněženky jsou navržené tak, i kdyby se nepovolaná osoba zmocnila zařízení, k vašim prostředkům se nedostane.

Hardwarové peněženky mohou být používány jak v offline módu, tak i online. V offline módu je připojíte k offline počítači a importujete informaci o transakci do vaší

[28] BARSKI, Conrad. Bitcoin for the befuddled. San Francisco, CA: No Starch Press, 2014. ISBN 1593275730.

hardwarové peněženky. Po připojení online můžete provádět transakce stejně snadno jako v online peněženkách, avšak transakce potvrzujete manuálně na hardwarové peněžence. Díky tomuto faktu vaše prostředky nejsou v nebezpečí, protože lidský faktor nedokáže nikdo nahradit.[29]

Aktuálně jsou na trhu dvě varianty hardwarových peněženek. Český produkt Trezor, který vyvinula společnost SatoshiLabs s.r.o., a konkurenční produkt dokonce od stejnojmenné firmy Ledger. Výhodou těchto produktů je jejich schopnost obnovení dat na novém zařízení, potom, když se vám poškodí, či ztratíte to původní.

[29] KALISKÝ, Boris. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. Praha: IFP Publishing, 2018. ISBN 978-80-87383-71-1.

6. Profil ověřené kryptoměny

Základem pro start úspěšných investicí na kryptoměnovém trhu je výběr správného projektu. Na začátku určitě musíme prostudovat ekosystém kryptoměn a pozorovat aktuální trendy. Na trh každý den vstupují desítky – možná stovky – nových projektů, ale jen mizivé množství má potenciál dostat se mezi prvních 100 nejobchodovanějších měn a dlouhodobě se udržet.

Některé projekty vznikají jen s vidinou rychlého výdělku pro první zasvěcené, či šťastlivce, u kterých ještě dojde k vyplacení z investovaných prostředků pozdějších přistupujících – tyto projekty fungují na základech Ponziho schématu a opravdu nedoporučuji zkoušet své štěstí u těchto pochybných metod investování.

Za nejdůležitější faktor značící dlouhodobou udržitelnost, životaschopnost a také důvěryhodnost projektu, považujeme revoluční myšlenku s přiloženou zevrubnou analýzou toho daného projektu sepsanou v oficiálním whitepaperu s fungujícími webovými stránkami.

Než se rozhodnete investovat do nového projektu, je zapotřebí si zjistit, zda podobný či úplně stejný projekt a technologie již neexistují. Tento faktor nám hodně napoví, protože pokud na trhu figuruje stejná myšlenka, proč vytvářet její klon a jako investor podobné jednání podporovat?

Sledujte kryptoměnová fóra, influencery a významné osobnosti z pole kryptoměn. Můžete se dozvědět, zda je o danou technologii či projekt vůbec zájem z řad široké veřejnosti. Pokud je myšlenka utopistická až nereálná, nemá vývoj potenciál, tudíž bychom považovali za velmi rizikové vkládat, byť dočasně, své prostředky pouze s vidinou spekulace.

Vývojový tým zosobňuje jeden z nejdůležitějších faktorů. Pokud za myšlenkou stojí veřejně známá osoba, specialista a odborník na danou problematiku, který má za sebou portfolio úspěšných a dlouhotrvajících projektů, přispívá to k celkové důvěryhodnosti projektu a s velkou pravděpodobností disponuje potenciálem prosadit se i mezi silnou konkurencí. Transparentnost a dostupnost dokumentů na oficiálních webových stránkách, kde je technický popis a kvalitně vypracovaný SMART business plán by měly být nedílnou součástí.

Zalistování kryptoměny k obchodování na velkých kryptoměnových burzách a zařazení do portfolia kryptoměnových směnáren. Vytvoří-li kryptoměnové směnárny přímý směnný pár s fiat, znamená to, že kryptoměna má dlouhodobější potenciál a je všeobecně důvěryhodná.

U takových měn si můžete být téměř jisti, že se nejedná o podvod a v tu chvíli se s vývojem počítá i do budoucna.

Přidání konkrétní kryptoměny mezi portfolio podporovaných kryptoměn hardwarovými peněženkami (Trezor, Ledger Nano).

Žebříček z hlediska kapitalizace vkladů, tzv. „marketcap“. Obecně kryptoměny s vysokou hodnotou marketcap a slušným denním objemem obchodů (obratem) jsou považovány za méně rizikové a stabilnější v smyslu životnosti. Likvidita je z pohledu obchodníka to nejdůležitější, a proto se vždy dívejte na faktory zájmů ostatních investorů.

Při rozhodování, do jaké kryptoměny investovat, se zaměřte také na fakt, zda se jedná o „coin“ nebo „token“. „Coins“ jsou samostatné produkty opírající se o svou vlastní architekturu zpravidla postavenou na principu blockchainu, jenž je většinou modifikován pro specifický účel té jisté kryptoměny. Tokeny stojí na základech jiných platforem již existujících kryptoměn. Nejčastěji jsou tokeny navázány na technologii Etherea. Nevýhodou tokenů je závislost na coinu, ke kterému jsou přidruženy. Jsou tak přirozeně limitovány požadavky a změnami ze strany coinu.

Existující funkční produkt je důkazem, že vývojový tým plní své business cíle, projekt se neustále vyvíjí a hodlá ve svém růstu pokračovat.

Poslední znak slibného projektu, ambice a vize fungující i do budoucna přinášejí spolupráce s velkými a známými korporacemi. V některých případech se přímo zapojují do vývoje, jindy kryptoměnu podporují, v rámci toho ji někdy i veřejně propagují.

Ať už mají kryptoměny jakýkoliv účel, je nutností si před odstartovanou investicí řádně projít všechny získané vstupní informace, ztotožnit se s myšlenkou (daný projekt by vám měl dávat smysl) a v neposlední řadě se ujistit, že v jeho poslání věříte.

7. Vybrané kryptoměny

V této části bakalářské práce se zaměřím na výběr zajímavých kryptoměnových projektů, které mají přínos pro širokou veřejnost a jejichž technologie by bylo vhodné přenést do sfér, které jimi ještě nebyly obohaceny.

První kryptoměnu, Bitcoin, jsem již představil. Mnoho dalších však vzniklo po jeho vzoru, souhrnně jsou pak tedy označovány jako tzv. altcoiny neboli kryptoměny druhé generace.

7.1. Litecoin

V roce 2011 vznikl jeden z prvních altcoinů – Litecoin. Litecoin stvořil Charlie Lee, osoba veřejně známá v kryptoměnových kruzích. Litecoin se odštěpil vytvořením forku z Bitcoinu, když byla upravena logika těžebního algoritmu (Scrypt), a nastala tak další vylepšení oproti původnímu Bitcoinu. Litecoin cílil z počátku na těžaře bez ASIC přístrojů, kteří díky změně konceptu proof – of – work zajistili budoucnost těžbě pomocí GPU. Tím získali z počátku velký výpočetní výkon od přístrojů, které byly pro těžbu Bitcoinu ve větším měřítku nevýhodné a nedostatečné.

Litecoin je označovaný jako vylepšený Bitcoin hned z mnoha důvodů. Jeho jednoznačná výhoda spočívá v rychlejším ověřování transakcí, jež u Litecoinu činí dvě a půl minuty. Oproti Bitcoinu, kdy ověření proběhne po vytěžení jednoho bloku, tedy každých deset minut, jde o značný technologický posun. Díky tomuto faktu je pro běžného člověka mnohem výhodnější měnou pro standardní transakce, po nichž není vyžadováno mimořádné zabezpečení, delší zprávy pro příjemce či okamžité provedení. Poplatky za provedení plateb jsou nižší než u Bitcoinu a v porovnání s běžnými platebními poplatky jsou transakční poplatky u použití Litecoinu mizivé.

Další sympatickou vlastností Litecoinu je jeho historie. Od jeho vzniku uběhlo již mnoho let a vývoj se stále dere kupředu, přívrženců přibývá, což je jasná známka důvěryhodnosti a potenciálu pro existenci v budoucnosti. Díky právě jeho potenciálu jej zařazují kryptoměnové směnárny do jejich portfolia k přímé směně s fiat měnami, čímž se radikálně zvýšila jeho likvidita a popularita.

Litecoin je jen jednou z mála kryptoměn rozšířených u obchodníků, u kterých lze touto formou provést platbu. Často můžete vidět Bitcoin spolu s Litecoinem jako přijímané

alternativy k platbě ve vybraných obchodech a e-shopech. „Litecoinem lze v České Republice platit u několika obchodníků, platbu Litecoinem např. přijímá e-shop Alza.cz a kavárna Paralelní Polis“.[30] Obchodníků, kteří přijímají, jako alternativu k placení kryptoměny stále přibývá a Litecoin je spolu s Bitcoinem těmi nejčastěji přijímanými.

Dle mého názoru Litecoin převzal za svou myšlenku běžného placení v kryptoměnách a plně se na toto poslání zaměřil. Bitcoin vnímám spíše jako alternativu k tradiční komoditě, např. zlatu.

Z Litecoinu vznikla i protestní kryptoměna Dogecoin, která se už mnoho let drží v žebříčku kryptoměn na jedné předních pozic. Dogecoin nás zaujme ještě rychlejším ověřením transakcí. Samotná kryptoměna však byla vytvořena jako vtip, tudíž bych jí nepřikládal velký význam do budoucnosti.

7.2. Ethereum

Ethereum je velmi specifickou kryptoměnou, která zaujala roli živné půdy pro nový technologický směr poskytnutím chytrých kontraktů („Smart contracts“) v praxi. Smart contract je softwarově řízený úkon pro uzavření smlouvy mezi více stranami. V praxi to znamená, že v blockchainu se nese předprogramovaná informace, co se má stát, když druhá strana kontrakt uzavře, ale také, co se má stát, pokud k uzavření dohody nedojde. Nemusí se vždy jednat o převod peněžních prostředků. Tyto akce jsou umožněny díky speciálně vyvinutému programovacímu jazyku nazvanému Solidity. Solidity ve své podstatě pracuje na jednoduchých příkazech typu: IF (jedna strana kontraktu) a THEN (druhá strana kontraktu). Uskuteční-li se něco na jedné straně, vyvolá to takový efekt na straně druhé. Chytrý kontrakt se tak postará o všechny potřebné náležitosti kontraktu, jako je vynucení, výpočetní proces a exekuce příkazu. Za celým projektem stojí ruský programátor Vitalik Buterin, který představil světu Ethereum na konci roku 2014, to bylo později 30. 06. 2015 spuštěno do produkce.

Ethereum tak není jen platební alternativou k ostatním kryptoměnám, jeho role by mohla mít daleko širší dopad, a to např. v centralizaci legislativních dokumentů a smluv. Stejně jako ostatní decentralizované kryptoměny si i Ethereum zakládá na bezpečnosti a neměnnosti, tudíž by vše bylo podpořeno předem stanovenou logikou EVM (Ethereum Virtual Machine), kterou ze své podstaty nelze zneužít.

[30] VÁVRA, Aleš. Po Bitcoinu se Českem šíří Litecoin. Podívejte se, jak se platí appkou v mobilu. *Mobilmania.cz* [online]. 2008, 26.06.2017 [cit. 2019-03-27]. Dostupné z: https://www.mobilmania.cz/bleskovky/po-bitcoinu-se-ceskem-siri-litecoin-podivejte-se-jak-se-plati-appkou-v-mobilu/sc-4-a-1338873/default.aspx

Na promyšlené infrastruktuře Etherea by se teoreticky dalo začít vytvářet nové projekty, které by mohly být použity pro specifické operace, jako nákup cenných papírů, aukce, nákup nemovitostí či dokonce při kandidátských volbách. Této příležitosti se chopilo mnoho ICOs, takže vzniklo mnoho nových projektů stojících na platformě Etherea, které navíc vyprodukovaly své vlastní tokeny.

Měnová jednotka Etherea – Ether – je vázána na EVM, čímž je zajištěna budoucnost celého projektu, jelikož každá nová aplikace využívající prostředí Etherea se stane na existenci původní kryptoměny přímo závislá.

7.3. NEO

Velmi zajímavý, první ryze Čínský kryptoměnový projekt s původním názvem AntShares, byl představen v roce 2014. Ke změně brandu projektu, došlo v červnu 2017 a s novým názvem NEO započala jeho nová éra. NEO vychází z Etherea a jeho plaformy se systémem chytrých kontraktů. Zároveň je však NEO kryptoměnou s proof – of – stake konceptem, kdy je každý uživatel NEA odměňován za fakt, že drží NEO token ve své peněžence, což z něj činí tzv. stakeholdera. Stakeholderovi je pak dle % držených tokenů NEO přepočítána jejich hodnota oproti aktuálnímu množství v oběhu. Přepočítaná hodnota je mu pak vyplacena jako odměna za držení NEO tokenu. Držitel má nárok na svou odměnu, pokud má své NEO tokeny uloženy v prostředích umožňující vyplácení odměn.[31]

NEO přišlo s velmi zajímavým řešením poplatků za služby poskytovaných v rámci projektu. Vývojáři vytvořili druhý token, který se jmenuje GAS a je přímo vázán na NEO, ale jeho prostřednictvím je právě ohlídáno splacení poplatků za dokončené kontrakty. GAS lze získávat stejným způsobem jako ostatní kryptoměny, tedy jako odměnu za zpracování operace. Získání odměny tedy nedocílíme těžbou, nýbrž zprocesováním transakce nodekeeperem, který si předem zvolí hodnotu své odměny v GAS. Další varianta je nakoupit GAS přímo na kryptoměnových burzách. GAS však opět slouží jako již dříve zmiňovaná odměna za držení NEA (proof – of – stake).

Obrovskou výhodou pro vývojáře nebo společnosti, které by se chtěly domluvit na přímé spolupráci s NEEM, je fakt, že NEO je postavené na zaběhnutých programovacích

[31] BAJPAI, Prableen. The 10 Most Important Cryptocurrencies Other Than Bitcoin. *Investopedia* [online]. 1999, 09.02.2019 [cit. 2019-03-18]. Dostupné z: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

jazycích, jako je např. Java, JavaScript, php, C++, python a další. Díky technické dostupnosti není nijak složité vytvořit nový chytrý kontrakt. Do budoucna se pro práci s chytrými kontrakty vybuduje uživatelská platforma, kdy zadavatel smart contractu nebude muset znát žádný programovací jazyk, čímž se stane NEO uživatelsky mnohem atraktivnější než samotné Ethereum, ze kterého NEO vzniklo a je jeho hlavním konkurentem.

7.4. Ripple

Další kryptoměna, která se odštěpila z Bitcoinu a zároveň odlišila od jeho ostatních klonů a vydala se vlastní cestou. Ripple stojí na základech blockchainu jako valná většina ostatních kryptoměn. Co ji však odlišuje, je vlastnictví konkrétní společností a také její již existující produkty se souvisejícími technologickými obměnami.

Ripple má svou vlastní kryptoměnovou síť zvanou XRP ledger, což je obdoba blockchainu. Ripple zastupuje z mála měn, která není těžena. Nestojí klasicky na základech proof – of – work, nýbrž proof – of – stake. Logika pro potvrzování transakcí tak není postavena na výpočetním výkonu, ale na shodně všech účastníků přihlášených do XRP ledgeru, že transakce byla provedena. Transakce pak může být následně zapsána. Opatření v logice potvrzování transakcí byla učiněna zejména pro použitelnost v obchodních a finančních sférách. Do XRP ledgeru se tak mohou přihlásit jak jednotlivci, tak i společnosti. Samotné ověřovací subjekty, které jsou považovány za ověřené a důvěryhodné, se evidují na tzv. UNL – Unique Node List.

Ripple byl vystavěn na opačné logice, než je tomu u těžených kryptoměn, a při jeho spuštění v roce 2012 bylo vytvořeno konečných sto miliard XRP. „Z původních sto miliard XRP bylo věnováno 60 % Ripplu, společnosti, která za projektem a kryptoměnou stojí. 60 % v tomto případě činí 60 miliard XRP. Koncem roku 2017 Ripple uzamkl 55 miliard ze zmíněných 60i do escrow. Escrow jsou časované kontrakty v síti XRP Ledger, které každý měsíc uvolňují právě jednu miliardu XRP. Společnost Ripple Labs Inc. z každé miliardy každý měsíc použije část na podporu XRP ekosystému a zbytek uzamkne na dalších 55 měsíců do escrow.“[32] Díky této skutečnosti je Ripple daleko za myšlenkou kryptoanarchismu, protože je

[32] SCHWARTZ, David. An Explanation of Ripple’s XRP Escrow. *Ripple* [online]. 2012, 15.12.2017 [cit. 2019-03-13]. Dostupné z: https://ripple.com/dev-blog/explanation-ripples-xrp-escrow/

sám ve velké míře centralizován XRP (měna Ripple) drženými přímo organizací Ripple Labs Inc. – tvůrcem celého projektu. [33]

Velkým tématem je jeho spolupráce s finančními a státními subjekty, což naprosto odporuje myšlence decentralizace. Ripple přímo na svých oficiálních stránkách www.ripple.com/xrp/ uvádí, že nabízí nové možnosti pro banky a poskytovatele finančních služeb. Některé firmy již spolupráci navázaly a využívají výhod Ripplu – např. MoneyGram, společnost, která implementovala technologii Ripplu (xRapid) do svého platebního systému. Významnou spolupráci navázala Saudskoarabská centrální banka, která spustila v roce 2018 pilotní provoz Ripple technologie pro zdokonalení systému zasílání zahraničních plateb.

Ripple aktuálně stojí na špičce aktuálního světa kryptoměn, a to hned z mnoha důvodů, ačkoli tím hlavním jsou jeho funkční produkty. Ripple jako jeden z mála projektů má už spuštěné i své produkty v praxi a fungují spolehlivě. Jedním z nich je xRapid. xRapid zprostředkovává transakci fiat měny přes XRP do stejné, nebo jiné fiat měny. Doručení transakcí probíhá zpravidla do pěti vteřin a poplatky jsou v porovnání se standardními bankovními poplatky zanedbatelné. Dalším produktem je xCurrent. Do xCurrent není podmínkou vlastnictví XRP měny. xCurrent využívá infrastruktury Ripplu pro přenos informací – například interní zprávy mezi jednotlivými společnostmi podílejícími se na projektu, výměna dat či validace provedení/neprovedení transakce. xCurrent je vyvinut jakožto inovativní řešení komunikace pro podniky díky možnosti implementace ILP Ledgeru do jiných databází.

7.5. Stellar Lumens

Kryptoměna Stellar Lumens vznikla hardforkem z Ripplu, kdy bývalý člen vývojového týmu Ripplu Jeb McCaleb zastával jiné názory, tak si vytvořil vlastní projekt. Za celým Stellarem stojí vývojová skupina nesoucí název Stellar Development foundation (SDF). Následováním vzoru Ripplu vytvořila vlastní protokol – Stellar consensus protocol – a tím se od něj kompletně oprostila.

Hlavní vizí Stellaru je zrychlení a zlevnění transakcí po celém světě, a to jak pro jednotlivce, tak pro finanční subjekty. Jeho dalšími benefity by za užití technologie a sítě

[33] BROWN, Mike. Ripple vs. Bitcoin: The 5 Biggest Differences Between the Cryptocurrencies. *Inverse* [online]. 2015, 05.01.2018 [cit. 2019-02-16]. Dostupné z: https://www.inverse.com/article/39947-ripple-vs-bitcoin-5-biggest-differences-between-the-cryptocurrencies

Stellaru měly být propojení mobilních platebních služeb, tvorba mobilních bankovních poboček a remitence.

Stellar Lumens a jeho kryptoměna XLM (lumeny) vstoupila na trh v roce 2014, avšak za rok prošla razantní proměnou, kdy z původního Ripple protokolu a tehdejší měny STR se vytvořil protokol nový. Celkově již při samotném vzniku bylo vytvořeno 100 miliard stellarů, později přejmenovaných na lumeny. Každý rok se zvyšuje inflace o 1%, čímž se vytváří další lumeny. Přejmenování měny bylo provedeno hlavně z důvodu rozlišení projektu a jeho technologie od samotné měnové jednotky. Stellar Lumens je tak jeden z dalších zástupců inflačních kryptoměn. Stellar Lumens nefunguje jako většina známých kryptoměn na technologii blockchainu, má vlastní záznam, historii transakcí zvanou ledger, jež zastává funkci ověření integrity údajů.

Samotná měna, lumeny, slouží jako mezičlánek pro směnu hlavně fiat měn, ale také jako antispamové opatření ve formě poplatku za provedenou transakci v XLM.

Myšlenka a koncept decentralizovanosti zaujaly mnoho významných společností a technologických lídrů, kteří se Stellarem navázali partnerství. Tím vůbec nejvýznamnějším je bezesporu technologický gigant IBM. Dalším velmi cenným partnerstvím je konzultační firma Deloitte, která má pobočky po celém světě a zaměřuje se na poradenství v mnoha oborech, např. IT, bezpečnost a právní služby. Do budoucna se Stellar se svým lumen tokenem bude snažit prosadit v mezinárodním bankovnictví a stát se tak přímou konkurencí Ripplu.

7.6. NANO

NANO bylo ukázáno světu v roce 2015, v té době však ještě pod původním názvem RaiBlocks. K jeho změně došlo až na začátku roku 2018. NANO přišlo na trh s jasným cílem, a to nahradit tradiční fiat měny a stát se tak hlavním platebním nástrojem. S touto vizí se NANO zaměřuje výhradně na platby a faktory s nimi spojenými. NANO se snaží poučit z nedostatků ostatních kryptoměnových projektů a často se porovnává s Bitcoinem.[34]

NANO klade důraz na instantní zpracování transakcí s nulovými poplatky, což je ve světě kryptoměn unikátní. Aby této vize docílili, museli vyvinout vlastní podobu blockchainu, kterou nazvali block-lattice. Block-lattice je zvláštní typ blockchainu, který má strukturu přímého acyklického grafu podobnou jako u standardní DAG struktury. Díky této unikátní

[34] Nano price prediction 2019. *Finder* [online]. 2006, 03.01.2019 [cit. 2019-03-15]. Dostupné z: https://www.finder.com/nano-xrb-price-prediction

struktuře není zapotřebí pro zpracování jedné transakce provolávat celou síť, stačí pouze kontakt odesílatele a příjemce. Zadáním platby se vytvoří nový blok, který nahradí ten předchozí, v němž se uživatel nacházel před zadáním transakce, čímž se zjistí zůstatek před zprocesováním. Příjemce potvrdí, že k transakci došlo, a i na jeho pólu nový blok nahradí ten starý, což vyvolá vyrovnání zůstatků na obou stranách. Ve své podstatě tak každý uživatel má svůj vlastní blockchain a jeho transakční historie se váže pouze a jen k němu.

Díky struktuře block-lattice slibuje okamžité zpracování zadaných transakcí, a to bez poplatků a zvyšujících se nároků na výpočetní výkon. Díky své neomezené škálovatelnosti. Škálovatelnost je v případě NANA velmi důležitá pro kompetici s jinými těženými měnami, u nichž v budoucnu predikujeme právě vlivem omezené škálovatelnosti vznik jistých potíží.[35]

NANO navázalo velmi zajímavé partnerství s aktuálně nejpopulárnější platformou pro živé vysílání Twitch.tv. Twitch přidal NANO mezi podporované měny pro podporu umělců, kteří na Twitch.tv vysílají. Twitch.tv denně navštíví okolo deseti milionů uživatelů[36]. Touto spoluprací se NANO velmi dobře dostalo do povědomí veřejnosti, která dříve s kryptoměnami nepřišla do styku.

7.7. IOTA

IOTA je jedna z mála kryptoměn, které stojí na základu, nevyužívající technologii blockchain. Běží na bázi své vlastní unikátní platformy, kterou tvůrci pojmenovali „tangle“. Logika zpracování transakcí v tanglu je rozdílná, a to zejména kvůli faktu, že nevyužívá ledgeru s bloky, které jsou zpracovány na principu proof – of – work. V tangle se transakce propojují mezi sebou a tím je zajištěna nejen jejich historie, ale i zpracování, protože zadáním jedné transakce se současně potvrzují dvě další. Tím pádem není potřeba mít složité těžící přístroje a velmi vysoký výpočetní výkon. Proof – of – work je v procesu zpracování transakce dodržen ve velmi zjednodušené podobě, aby se zabránilo spamování sítě.

Zpracování transakcí je tak bezkonkurenčně nejintenzivnější, co se týká počtu zpracovaných plateb za jednotku času. Je to způsobeno faktem, že transakce zpracovává jiný uživatel zapojený do sítě – tangle. Sám zadává transakci, jen přitom ještě ověřuje další dvě,

[35] What is Nano (NANO)?: Future of NANO Cryptocurrency and know how to buy NANO. *CoinSwitch* [online]. [cit. 2019-03-11]. Dostupné z: https://coinswitch.co/info/nano/what-is-nano

[36] MURRAY, David. Twitch Streamers Can Now Accept Nano (XRB) Donations. *BlockExplorer: News* [online]. 24.02.2018 [cit. 2019-02-18]. Dostupné z: https://blockexplorer.com/news/twitch-streamers-can-now-accept-nano-xrb-donations/

díky čemuž počet zpracovaných transakcí není limitován a je zbaven jakýchkoliv poplatků. Rychlost zpracovávání transakcí je tak přímo úměrná počtu uživatelů.

Hlavní účel IOTY a její měny MIOTY je vytvoření kryptoměny pro placení v síti internet of things. Internet věcí je technologickým výdobytkem příštích let, kdy chytré přístroje, veškerá elektronika budou navzájem propojeny a budou mezi sebou neustále komunikovat. Předpoklad zní, že pomocí IOTY by tyto přístroje mohly mezi sebou provádět mikrotransakce, např. za přeprodání přebytečné energie přístroji, který jí má nedostatek.

8. Komparace vybraných kryptoměn

8.1. Srovnání vybraných kryptoměn

V této části bakalářské práce provedu srovnání kryptoměn, které jsem výše vyjmenoval, definoval a popsal. Vybrané projekty jsem vybíral na základě technologických odlišností oproti kryptoměnám jako celku. Zaměřil jsem se na projekty, které jsou stabilní, zalistované na velkých burzách a některé jsou již dokonce uváděny jako přímý směnný pár k fiat měnám, což je znakem dlouhodobého trvání celého projektu a jeho vysoké důvěryhodnosti. Nejdůležitějším faktorem pro výběr však zůstává účel kryptoměnového projektu, zda již v současnosti funguje nebo jaký v budoucnu přinese prospěch i pro laickou veřejnost.

Věnoval jsem se zejména nabízeným platebním službám a technologii zpracování, která stojí v úzké souvislosti s rychlostí a náklady na zpracování transakce. Pro přehledné srovnání jsem vytvořil tabulku s parametry, kde lze jednoznačně rozlišit výhody a nedostatky jednotlivých kryptoměnových projektů a zvýraznit výsledná zjištění.

Jako první z vybraných faktorů uvádím škálovatelnost. Parametr škálovatelnosti definuje míru vytváření, rozšíření nových mincí, tokenů dané kryptoměny. Pro vysokou škálovatelnost kryptoměny je tak mimo jiné možné rychleji autorizovat a exekuovat transakce než u kryptoměn s nízkou mírou škálovatelnosti. Škálovatelnost se u decentralizovaných kryptoměn stává důležitým faktorem pro svižnost a dostupnost. Pro projekty s nízkou škálovatelností může být velkou překážkou a ohrozit tak jejich budoucí vývoj. Dost možná způsobí jejich útlum až zánik.[37]

Druhým parametrem je doba dokončení jednoho bloku. Tato doba souvisí s dobou zpracování nových transakcí, vytváření a vypouštění nových mincí do oběhu, pokud je tento jev přímo závislý na vytěžení právě jednoho bloku, což také zaujímá část posledního zkoumaného parametru u vybraných kryptoměn.

Třetím faktorem je rychlost provedených transakcí za určitou jednotku času. Jedná se o maximální počet transakcí, které je možné zprocesovat za jednu vteřinu.

[37] LUDWICK, Ibrahim. 10 Cryptocurrencies Hoping to Be the New Cash. *Invest In Blockchain* [online]. 2017, 16.09.2018 [cit. 2019-02-18]. Dostupné z: https://www.investinblockchain.com/cryptocurrencies-replace-cash/

Dále nás zajímají průměrné transakční poplatky. Tato hodnota je orientační, protože hodnoty se mění se zadanou částkou. Jedná se tak zejména o částky při zadání minimální možné hodnoty v dané kryptoměně přepočtené vůči aktuálnímu kurzu USD v únoru 2019.

Další zkoumanou veličinou je maximální počet vydaných mincí/tokenů. Tento parametr nám může nastínit budoucí vývoj ceny měn. U kryptoměn, u nichž dosažení finální hodnoty dojde v budoucnosti a nároky na jejich získání se tím budou přirozeně zvyšovat, je tendence růstu ceny s ohledem na obtížnost získání nových mincí. Naopak ty, které nemají stanovenou konečnou hranici, mohou nést riziko vysoké inflace v budoucnosti, kdy může dojít k přesycení trhu.

Poslední bod souvisí s tvorbou a uvolňováním nových mincí do oběhu. U těžených měn souvisí tento proces s dobou dokončení jednoho bloku, což je zkoumaný parametr č. 2. U inflačních měn se jedná o inflační opatření zajišťující určitou stabilitu – bezproblémové, souvislé řazení nových mincí do oběhu tak, aby nedošlo k inflační krizi dané kryptoměny.

Tabulka č. 1: Srovnání vybraných kryptoměn

Kryptoměna	Měnová jednotka	Míra škálovatelnosti	Doba dokončení jednoho bloku	Rychlost transakcí za vteřinu	Průměrné transakční poplatky v $	Maximální počet v mil.	Inflační/těžební uvolnění nových mincí
Bitcoin	BTC	Nízká	10 min	7	1.184	21	12,5/blok
Litecoin	LTC	Střední	2,30 min	56	0.198	84	25/blok
Ethereum	ETH	Nízká	15 sec	20	0.347	Není limitován	3/blok
NEO	NEO	Střední	15 sec	1000	0,01	100	Do 1mil/rok
Ripple	XRP	Vysoká	instantní	1500	0.0037	100000	1 bilion/měsíc
Stellar	XLM	Vysoká	5 sec	1000	0,0000009	Není limitován	Do 1% inflace/rok
IOTA	MIOTA	Nejvyšší	instantní	1000	0	2778	Všechny v oběhu
NANO	XRB	Nejvyšší	instantní	7000	0	133	Všechny v oběhu

Zdroj: Vlastní

8.2. Vyhodnocení s důrazem na využitelnost v bankovnictví a finančních institucích

V této části práce provedu srovnání vybraných kryptoměn na základě vyhodnocení faktorů jako celku a vyberu dle svého názoru nejvhodnější kryptoměnové projekty pro využití ve finančních institucích a bankovnictví, se schopností zdokonalit tradiční systém.

Paradoxně jako nejméně vhodný se jeví z mnoha důvodů samotný Bitcoin. Bitcoin má oproti ostatním zmíněným kryptoměnám nejnižší míru škálovatelnosti, s tím souvisí

i maximální náročnost na vytvoření nových mincí a zprocesování transakcí. Bitcoin je ze všech vybraných kryptoměn nejpomalejší, co se týká zpracování transakcí, a požaduje nejvyšší transakční poplatky. Čímž se stal nevhodným kandidátem pro mikrotransakce. Na druhou stranu jej považujeme za nejdůvěryhodnější kryptoměnu, velmi bezpečnou a představuje vhodného uchovatele prostředků pro delší časové období. Díky jeho vlastnostem jej vnímám spíše jako komoditu než prostředek pro denní využití – mám na mysli platby u obchodníků či převody mezi institucemi. Mohl by však do budoucna mít roli povinného depozita banky národní či nadnárodní.

Litecoin je vylepšenou obdobou Bitcoinu. Původně se z něj odloučil, a momentálně se snaží poučit z jeho chyb. Litecoin má obrovský potenciál pro uchování hodnoty i levné a relativně rychlé přechody mezi jednotlivými uživateli. Důležitým faktorem je jeho zabezpečení a důvěryhodnost ze strany uživatelů. Nevýhoda pro jeho globální využití jakožto standardního platidla vyvstává v otázce rychlosti. Litecoin zvládne maximálně 56 transakcí za vteřinu. Pokud se na základě stálého usilovného vývoje nedostane na násobky této hodnoty, pak nemůže konkurovat ostatním ani kryptoměnám ani tradičnímu systému.

Velmi slušný potenciál jeví kryptoměny založené na blockchainu, zároveň využívající koncept chytrých kontraktů. Co se týká transakčních vlastností, tak se rozhodně nejedná ani o ty nejrychlejší ani nejlevnější. Oplývají jinou výhodou, a sice neměnností zadaného příkazu, což s sebou přináší vysoké zabezpečení proti manipulaci prostředky třetí (nezvanou) stranou nebo jinému zneužití dokumentů. Nejznámější kryptoměnou tohoto typu je Ethereum, první svého druhu. Ethereum a NEO jsou velmi podobné projekty, zároveň by oba mohly výrazně přispět pro zlepšení stávajícího, tradičního systému, a to zejména v oblasti uzavírání smluv nebo zprostředkování nejrůznější dokumentace. NEO se však zdá být při své aktuální technické zdatnosti z pohledu užitečnosti přeci jen zajímavější. Ethereum má však obrovskou podporu z řad následovatelů a každým měsícem jej vylepšuje a optimalizuje výborný tým specialistů. Ethereum a NEO mají z vyčtených kryptoměnových projektů jednoznačně největší potenciál zapojení se do nejen finančních a bankovních struktur, ale také do realitních a legislativních záležitostí.

Internet věcí bude v následujících letech velkým tématem a s tím souvisí i kryptoměna IOTA, ta má rozhodně co nabídnout, a to hlavně díky jeho unikátní technologické struktuře zvané Tangle. Tangle s narůstajícím počtem uživatelů přibývá na rychlosti a účinnosti. Transakce jsou zpracovány instantně, a přitom za nulové poplatky. Pro běžného člověka by

v budoucnosti mohlo jít o nejvhodnější variantu placení nejen jednotlivcům, ale i hromadně. Internet věcí bude pravděpodobně v blízké budoucnosti standardem, na který si lidé jistě rychle zvyknou, a je možné, že právě IOTA se stane zvoleným nástrojem pro tuto komunikaci. Pro banky a finanční domy však aktuálně není zajímavá, protože by je osoby zapojené do sítě tanglu již nepotřebovaly.

Další dvojicí kryptoměnových projektů, které jsou svým základem a myšlenkou podobné, je Ripple a Stellar s jeho lumeny. Ripple a Stellar přímo cílí na finanční instituce s jasným úkolem, nechat se implementovat do jejich systému tak, aby využívaly jejich nabídek a produktů. Z hlediska technologií a připravenosti pro tyto účely jsou velmi vhodnou alternativou, a dokonce některé spolupráce se už staly realitou. Ripple přináší pro oficiální využití výhodu v produktech, které jsou diferenciované pro konkrétní segmenty a cílí opravdu na velké finanční internacionální instituce. Stellar je naopak vhodnější alternativou pro nově vznikající subjekty, které ještě nemají vyřešené expresní, či instantní platby nebo vhodnou alternativu pro konverzi fiat měn v reálném čase za minimální poplatky. Velkou neznámou však zůstává fakt, že u Ripplu je maximální počet stanovený a je jasně stanoveno kolik mincí se vydá do oběhu v měsíčně opakujících se periodách. Naopak Stellar nemá určený maximální objem, a tudíž je vývoj jeho ceny značně nepředvídatelný, což zase může být jeho značná nevýhoda pro korporátní využití jako mezičlánku pro směnu cizích měn.

Jako nejlepší platidlo v rámci všech zkoumaných kritérií vychází kryptoměnový projekt NANO. Jednoznačně největší výhodou je jeho unikátní technologie a zvláštní typ Ledgeru, kdy jsou transakce zpracovány instantně a s nulovým poplatkem. Velkou výhodou je možnost zadání platby, kdy druhá strana není online. Jednoduše je provedena, jakmile se příjemce připojí a platbu potvrdí. Tím, že je transakční historie vázána pouze k samotnému uživateli, stává se tak i velice bezpečnou variantou, která je dokonale přenosná, pokud zná uživatel své přihlašovací údaje sloužící jako soukromý klíč. Kryptoměna – NANO, se může stát jedním z průkopníků možnosti placení kryptoměnami v budoucnu, míníme-li v masovém měřítku. Pokud tento trend nastane, začnou vznikat fintechové aplikace, které částečně nahradí bankovní platební systémy nebo budou alternativou, konkurencí k tradičnímu systému.

Pro samotné finanční instituce a banky se tak největším přínosem stávají samotné kryptoměnové technologie, na kterých mohou stavět své vlastní procesy. Možností je nad blockchainovou technologií s chytrými kontrakty vystavět vlastní produkty, protože jen tak si udrží nad děním ve finančním světě kontrolu. Ten postup však je nejen velice nákladný, ale

využití fintechů často odporuje samotné legislativě, jelikož koncept kryptoměn je postaven na úplně opačném principu, a to nebýt sledován, kontrolován nikým kromě účastníků. Mít finanční volnost, pracovat bez prostředníka, nezávisle na bance a zajišťovat transakce napřímo P2P. Jedním z mála projektů, který splňuje nároky finančních domů a zároveň není úplně v rukou samotných uživatelů, je Ripple. Ripple tak je jako jediný produkt vhodný i pro velké nadnárodní ústavy a na tyto organizace také přímo svými produkty cílí.

Domnívám se, že do budoucna se role bank a finančních institucí radikálně změní. Banky budou mít spíše roli důvěryhodné instituce poskytující zejména svá licenční práva třetím stranám, které nebudou splňovat podmínky, aby dostaly potřebná povolení provozovat nějaký konkrétní druh služeb.

Finanční instituce budou poskytovat klientskou identitu, díky které se lidé budou moci snadno a rychle digitálně registrovat do dalších platforem, aplikací či sítí pro využívání služeb, a to bez osobní návštěvy pobočky.

Banky budou pravděpodobně pracovat na bázi security tokenů, které začínají být populární už v této době. Díky security tokenům budou schraňovat záznamy a zprocesovávat převody nemovitostí, cenných papírů nebo jiných movitých statků. Zavedením tohoto postupu by se značně zvýšila likvidita a zrychlily se legislativní náležitosti.

Tabulka č. 2: Shrnutí účelu a využití vybraných kryptoměn

Kryptoměna	Účel	Navrhované využití
Bitcoin	Decentralizovaná, neovlivnitelná P2P platební síť dostupná pro každého	Díky jeho pseudo anonymitě a vysokému tržnímu kapitálu je vhodnou alternativou pro uchování prostředků
Litecoin	Zabezpečené platby pro každodenní užití	Vzhledem k jeho popularitě a podporovanosti u obchodníků, je Litecoin jednou z nejlepších alternativ pro denní transakce v dnešní době
Ethereum	Zabezpečená decentralizovaná síť sloužící pro tvorbu nových aplikací různého druhu se	Ethereum není pouze platformou, ale zejména technologickou základnou připravenou pro připojení

	zaměřením na transparenci a neměnnost	dalších komponent, díky kterým může obohatit tradiční systémy
NEO	Vytvoření chytré ekonomie připravenou pro dostupnější tvorbu nových aplikací na NEO platformě, s využitím chytrých kontraktů	Implementace blockchainu NEA do tradičních informačních systémů, pro využití chytrých kontraktů s ohledem na zabezpečení a neměnnost při exekuci smluvních závazků
Ripple	Zdokonalení mezinárodních peněžních transferů, zejména pro finanční subjekty/banky	Řešení pro finanční instituce, které chtějí modernizovat systém, zrychlit transakce a snížit své náklady na zahraniční platby
Stellar	Decentralizovaná finanční platforma sloužící pro mezinárodní převody se zaměřením na rychlost a nízké poplatky, a to jak pro jednotlivce, tak organizace	Stellar je ideální volbou pro soukromé podnikatele a jednotlivce, kteří potřebují levnější a rychlejší alternativu k aktuálnímu systému mezinárodních transakcí
IOTA	Zajištění zabezpečené komunikace a plateb mezi jednotlivými zařízeními s nulovými poplatky	Díky nejvyšší škálovatelnosti a technické připravenosti s unikátním propojením je IOTA skvělým projektem pro využití pro internet věcí, ale také pro extrémně rychlé jednorázové a hromadné transakce
NANO	Rychlá, jednoduchá forma placení pro všechny uživatele s nulovými poplatky	Kryptoměnový projekt, který je nejdokonalejší platební nástroj na každodenní P2P platby pro fyzické osoby

Zdroj: Vlastní

Závěr

Řešení bakalářské práce mnou zvoleného tématu mi pomohlo ponořit se hlouběji do problematiky kryptoměn a zpracovat komplexní bakalářskou práci doplněnou o cennou praktickou část.

V první části bakalářské práce jsem se věnoval dílčím cílům, konkrétně popisu a vysvětlení základních kryptoměnových termínů a iniciálových zkratek se kterými pracuji v další teoretické a zejména praktické části bakalářské práce.

První dílčí cíl spočíval v chronologickém popisu vývoje platidel od počátku až po vznik prvních zmínek kryptografie, ze kterých se postupně vyvinuly kryptoměny. U počátků moderních kryptoměn jsem popsal historii a technologickou podstatu Bitcoinu, na který přímo navázali další projekty, jako např. Litecoin, Ripple nebo Dash, souhrnně se označují jako – Altcoiny.

Ve druhém dílčím cíli jsem se zaměřil na rizikovost kryptoměn. Řešením práce bylo zjištěno, že velkým rizikem, ale i příležitostí je volatilita kryptoměn, z toho důvodu jsou kryptoměny považovány za vysoce rizikový typ investice. Popsal jsem důvody, proč jsou kryptoměny, často zneužívány pro ilegální aktivity, a to konkrétně z důvodu jejich pseudo anonymity a hlavně plné anonymity. Popsal jsem varianty škodlivých softwarů a jako příklad uvedl nejznámější hackerské útoky na burzy mt. Gox a Bitfinex, kdy byly odcizeny prostředky klientům, kterým doposud nebyla ztráta vyrovnána.

První kapitolou praktické části jsem navázal na předchozí dílčí cíl. V ní jsem analyzoval a doporučil jednotlivé nejznámější metody uchovávání kryptoměnových prostředků s důrazem na jejich bezpečnost. V rámci popisu jednotlivých způsobů jsem vytvořil jednoduchý názorný návod, jak si vytvořit vlastní online kryptoměnovou peněženku.

Hlavním cílem bakalářské práce je analyzovat a navrhnout ucelený systém vybraných kryptoměnových projektů, které by mohly nabídnout alternativu ke standardním platebním systémům.

Z analýzy, porovnání technických parametrů, možností zabezpečení a dalších kritérií můžeme konstatovat, že vhodných kryptoměnových alternativ je více. Kryptoměnových projektů využitelných pro finanční instituce je velmi málo. Vybral jsem ty, které tento potenciál mají.

Pro zdokonalení a zlevnění zahraničního platebního styku připadají v úvahu kryptoměny Ripple a Stellar. Stellar se hodí spíše jako řešení pro soukromé společnosti a jednotlivce, naopak Ripple pro finanční instituce, kterým Ripple nabízí technologické řešení pro zefektivnění a zlevnění jejich aktuálních řešení.

Velmi důležitými projekty, které by mohli sloužit zejména jako technologické vylepšení, zdokonalení interních procesů, např. pro podpis smluv či zabezpečeného doručení dokumentace, jsou NEO a Ethereum. Blochain s možnostmi, které poskytují právě tyto dva projekty, by mohl zajistit existenci kryptoměnových projektů i do budoucnosti a to hlavně díky možnosti využití security tokenů a chytrých kontraktů.

Kryptoměny IOTA, Bitcoin a Litecoin nemají tak vysoký potenciál pro bankovnictví, avšak pro jiné účely jako uchování prostředků nebo jako platidlo pro internet věcí je jejich možnost uplatnění vysoká a oproti ostatním kryptoměnám v nich vynikají.

Pro uživatele se z vybraných kryptoměnových produktů jako nejvíc přívětivý a výhodný tváří projekt NANO. Kryptoměna - NANO chce obejít tradiční bankovní instituce a stát se hlavním platebním prostředkem masové společnosti. Jejich vize je velmi optimistická, avšak jdou si za svým cílem a nepřijde mi nijak neuskutečnitelná. V horizontu několika – možná desítek – let se jistě vyprofilují další silné kryptografické měny a technologie, které se začlení do systému a nabydou potřebné důvěry. Tento proces připomíná „živoucí, stále se proměňující organismus“.

Zdroje a literatura

Seznam použité literatury

ANTONIA, Cameron. Bitcoin for dummies. Indianapolis, IN: John Wiley, 2016. ISBN 9781119076131.

ANTONOPOULOS, Andreas M. *Mastering bitcoin*. Sebastopol CA: O'Reilly, 2015. ISBN 9781491902608.

BARSKI, Conrad. *Bitcoin for the befuddled*. San Francisco, CA: No Starch Press, 2014. ISBN 1593275730.

BIRCH, David. *BEFORE BABYLON, BEYOND BITCOIN: From Money That We Understand To Money That Understands Us*. London: London Publishing Partnership, 2017. ISBN 978-1-907994-67-8.

JUDMAYER, Aljosha, Nicholas STIFTER, Katharina KROMBHOLZ a Edgar WEIPPL. *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms*. Morgan & Claypool Publishers, 2017. ISBN 9781627057165

HEISSLER, Herbert. *Ekonomie bitcoinu: analýza a modelování bitcoinu v rozvinutém stadiu*. Praha: Vysoká škola finanční a správní, 2014. Eupress. ISBN 978-80-7408104-0.

HUJOVÁ, Gabriela, ed. *Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti*?: sborník z konference: Praha, 26. března 2014. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. ISBN 978-80-86847-71-9.

JUDMAYER, Aljosha, Nicholas STIFTER, Katharina KROMBHOLZ a Edgar WEIPPL. *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms*. Morgan & Claypool Publishers, 2017. ISBN 9781627057165.

KALISKÝ, Boris. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. Praha: IFP Publishing, 2018. ISBN 978-80-87383-71-1.

LEE, David. *Handbook of digital currency: bitcoin, innovation, financial instruments, and big data*. Amsterdam: Elsevier/ AP, [2015]. ISBN 9780128021170.

MOUGAYAR, William. *The business blockchain: promise, practice, and application of the next Internet technology*. Hoboken, New Jersey: John Wiley & Sons, [2016].

NARAYANAN, Arvind. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, [2016]. ISBN 9780691171692.

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 97880-271-0742-1.

STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Ludwig von Mises Institut CZ&SK, 2015. ISBN 978-80-87733-26-4.

SWAN, Melanie. *Blockchain: blueprint for a new economy*. O´Reilly: Sebastopol, 2015. ISBN 978-1-491-92049-7. The Bitcoin Primer – Risks, Opportunities, And possibilities by David Seaman

SWANSON, Tim. *The Anatomy of a Money-like Informational Commodity: A Study of Bitcoin*. San Francisco: Tim Swanson, 2014. ASIN: B00MEAO7XK.

Internetové zdroje

BAJPAI, Prableen. The 10 Most Important Cryptocurrencies Other Than Bitcoin. *Investopedia* [online]. 1999, 09.02.2019 [cit. 2019-03-18]. Dostupné z: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

Bitcoin [online]. 2009. Dostupné také z: https://bitcoin.org

BitGo [online]. 2013 [cit. 2019-02-22]. Dostupné z: https://www.bitgo.com/

BROWN, Mike. Ripple vs. Bitcoin: The 5 Biggest Differences Between the Cryptocurrencies. *Inverse* [online]. 2015, 05.01.2018 [cit. 2019-02-16]. Dostupné z: https://www.inverse.com/article/39947-ripple-vs-bitcoin-5-biggest-differences-between-the-cryptocurrencies

BUNTINX, JP. The Role of Cryptocurrency in Crime – Darknet Activity Soars. *Null TX* [online]. 2014, 08.06.2018 [cit. 2019-03-20]. Dostupné z: https://nulltx.com/the-role-of-cryptocurrency-in-crime-darknet-activity-soars/

Crime. *CoinDesk* [online]. 2013 [cit. 2019-02-28]. Dostupné z: https://www.coindesk.com/category/bitcoin-crime

Ethereum [online]. 2015. Dostupné také z: https://www.ethereum.org/

Glossary: Cryptocurrency and Blockchain Glossary: A-Z. *CrushCrypto* [online]. [cit. 2019-03-20]. Dostupné z: https://crushcrypto.com/glossary/

IOTA [online]. 2016. Dostupné také z: https://www.iota.org/

KHATWANI, Sudhir. Top 5 Biggest Bitcoin Hacks Ever. *Coinsutra* [online]. 2017, 13.10.2018 [cit. 2019-03-20]. Dostupné z: https://coinsutra.com/biggest-bitcoin-hacks/

Litecoin [online]. 2011. Dostupné také z: https://litecoin.org/

LUDWICK, Ibrahim. 10 Cryptocurrencies Hoping to Be the New Cash. *Invest In Blockchain* [online]. 2017, 16.09.2018 [cit. 2019-02-18]. Dostupné z: https://www.investinblockchain.com/cryptocurrencies-replace-cash/

MALIK, Nikita. How Criminals And Terrorists Use Cryptocurrency: And How To Stop It. *Forbes* [online]. 31.08.2018 [cit. 2019-02-18]. Dostupné z: https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#7ec5f0923990

MURRAY, David. Twitch Streamers Can Now Accept Nano (XRB) Donations. *BlockExplorer: News* [online]. 24.02.2018 [cit. 2019-02-18]. Dostupné z: https://blockexplorer.com/news/twitch-streamers-can-now-accept-nano-xrb-donations/

NANO [online]. 2015. Dostupné také z: https://nano.org

Nano price prediction 2019. *Finder* [online]. 2006, 03.01.2019 [cit. 2019-03-15]. Dostupné z: https://www.finder.com/nano-xrb-price-prediction

NEO [online]. 2017. Dostupné také z: https://neo.org/

Ponzi Scheme. *Investor.gov: Types of Fraud* [online]. Washington, DC [cit. 2019-02-11]. Dostupné z: https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme

Ripple [online]. 2012. Dostupné také z: https://ripple.com/

SCHWARTZ, David. An Explanation of Ripple's XRP Escrow. *Ripple* [online]. 2012, 15.12.2017 [cit. 2019-03-13]. Dostupné z: https://ripple.com/dev-blog/explanation-ripples-xrp-escrow/

Slushpool [online]. 2010 [cit. 2019-03-20]. Dostupné z: https://slushpool.com/home/

Stellar [online]. 2014. Dostupné také z: https://www.stellar.org/

Symmetric cryptography. *IBM®: Knowledge Center* [online]. 1994 [cit. 2019-02-11]. Dostupné z: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.15/gtps7/s7symm.html

SZABO, Nick. Bit Gold. *Satoshi Nakamoto Institute* [online]. 29.12.2005 [cit. 2019-02-12]. Dostupné z: https://nakamotoinstitute.org/bit-gold/

TAPANG, Carlos. Will Cryptocurrencies Replace Fiat?. *Medium: Coinmonks* [online]. 06.05.2018 [cit. 2019-03-14]. Dostupné z: https://medium.com/coinmonks/will-cryptocurrencies-replace-fiat-732ca57b751b

VÁVRA, Aleš. Po Bitcoinu se Českem šíří Litecoin. Podívejte se, jak se platí appkou v mobilu. *Mobilmania.cz* [online]. 2008, 26.06.2017 [cit. 2019-03-27]. Dostupné z: https://www.mobilmania.cz/bleskovky/po-bitcoinu-se-ceskem-siri-litecoin-podivejte-se-jak-se-plati-appkou-v-mobilu/sc-4-a-1338873/default.aspx

What is Nano (NANO)?: Future of NANO Cryptocurrency and know how to buy NANO. *CoinSwitch* [online]. [cit. 2019-03-11]. Dostupné z: https://coinswitch.co/info/nano/what-is-nano

WHIPPS, Heather. The Profound History of Coins. *Live Science* [online]. 2004, 16.11.2007 [cit. 2019-03-20]. Dostupné z: https://www.livescience.com/2058-profound-history-coins.htm

Seznam obrázků a tabulek

Abstrakt a klíčová slova

Anotace

Bibliografický údaj: Grossmann, Zdeněk. Faktory ovlivňující práci s vybranými kryptoměnami. Olomouc 2019.

Bakalářská práce. Moravská vysoká škola Olomouc. PhDr. Jan Lavrinčik, Ph.D.

Název práce: Faktory ovlivňující práci s vybranými kryptoměnami

Autor: Zdeněk Grossmann

Ústav: Ústav informatiky a aplikované matematiky

Vedoucí práce: PhDr. Jan Lavrinčik, Ph.D.

Počet stran: 63

Abstrakt: Hlavním cílem této bakalářské práce je provedení důkladné analýzy zajímavých kryptoměnových projektů. Na základě vypracované analýzy vybrat nejvhodnější projekt, který má potenciál vylepšit, či úplně nahradit aktuální, tradiční platební systém s důrazem na bankovnictví.

Klíčová slova v českém jazyce: kryptoměna, blockchain, digitální technologie

---

Title: Factors which affect operations with selected cryptocurrencies

Author: Zdeněk Grossmann

Department: Department of Computer Science and Applied Mathematics

Supervisor: PhDr. Jan Lavrinčik, Ph.D.

Number of pages: 63

Abstract: Main goal of this bachelor's thesis is to thoroughly analyse interesting cryptocurrency projects. based on analysis to recommend the most suitable cryptocurrency project or projects which could improve or replace traditional payment system with emphasis on banking.

Keywords: cryptocurrency, blockchain, digital technology
