ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA VÝPOČETNÍ A DIDAKTICKÉ TECHNIKY

KRYPTOMĚNY A JEJICH VYUŽITÍ ŠIRŠÍ VEŘEJNOSTÍ

BAKALÁŘSKÁ PRÁCE

Tomáš Šrail

Přírodovědná studia, obor Informatika se zaměřením na vzdělávání

Vedoucí práce: PhDr. Denis Mainz, Ph.D.

Plzeň 2018

Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 18. dubna 2018

.....

vlastnoruční podpis

Tímto děkuji vedoucímu své bakalářské práce, PhDr. Denisu Mainzovi, Ph.D., za odborné konzultace a věcné připomínky, které pro mě byly velice přínosné.

ZDE SE NACHÁZÍ ORIGINÁL ZADÁNÍ KVALIFIKAČNÍ PRÁCE.

OBSAH

SEZNAM ZKRATEK

BTC	Bitcoin
POW	Proof of Work
POS	Proof of Stake
P2P	Peer to Peer
ČNB	Česká národní banka
ECDSA	Elliptic Curve Digital Signature Algorithm
DH	Diffie-Hellman
NIST	National Institute of Standards and Technology
NSA	National Security Agency
FIPS	Federal Information Processing Standards
SHA	Secure Hash Algorithm
CPU	Central Processing Unit
GPU	Graphical Processing Unit
FPGA	Field Programmable Gate Array
ASIC	Application Specific Integrated Circuit
DoS	Denial of Service
ALU	Arithmetic Logic Unit
VHDL	Verilog Hardware Description Language
TOR	The Onion Router

ÚVOD

Peníze a měny lidstvo doprovázejí již po staletí. Za každou moderní měnou stojí významná národní banka, která jejím prostřednictvím zasahuje do chodu ekonomiky dané společnosti. Tyto měny jsou centrálně řízeny. Úplně opačným směrem se z tohoto úhlu pohledu vydávají kryptoměny. Fenomén, který vznikl jako pokus a nekladl si vysoké cíle. Díky rychlému rozvoji výpočetních a komunikačních technologií se však tento revoluční projekt velmi rychle rozšířil mezi nadšenci a v současnosti už oslovuje velký počet běžných uživatelů po celém světě.

Cílem této práce je seznámit s problematikou kryptoměn tak, aby čtenář získal komplexní informace z oblasti virtuálních měn a pochopil základní principy jejich fungování. Dále, aby byl schopen je samostatně užívat a posuzovat bezpečnostní, nikoli však ekonomická rizika s tím spojená.

V první kapitole budou nejprve připomenuty vlastnosti peněz a vymezeny požadavky, které jsou na ně kladeny. Tato fakta poté budou porovnána s vlastnostmi peněz virtuálních. Bude uvedena definice kryptoměn a také události, které bezprostředně předcházely jejich vývoji.

Ve druhé kapitole budou vysvětleny základní kryptografické postupy z oblasti asymetrických šifer a další techniky využívané ke zvýšení bezpečnosti, případně efektivity protokolů kryptoměn. Poté bude navázáno popisem nových pojmů úzce spjatých s kryproměnami.

Ve třetí kapitole budou popsány nejvýznamnější zástupci kryptoměn, konkrétně Bitcoin a Litecoin. Tyto měny budou podrobněji porovnány s ohledem na jejich praktické využití širší veřejností. Součástí kapitoly je také stručný popis problémů, které u běžných měn nejsou zcela běžné.

Pro manipulaci s kryptoměnami je nezbytné programové vybavení. V další kapitole bude představen nejrozšířenější software pro správu účtů. Zmíněna bude také problematika hardwaru, se kterým se mohou uživatelé kryptoměn setkat, a to běžným i speciálním. Na závěr budou vedena rizika bezprostředně se týkající obchodování s virtuálními měnami.

Poslední kapitola se bude zabývat dotazníkovým šetřením, které je cíleno na současné uživatele moderních platebních způsobů. Jeho evaluace by měla odpovědět na stanovené autorovy otázky. Zjistit, do jaké míry jsou lidé spokojeni se současnou podobou bankovních služeb, popřípadě poukázat na jejich nedostatky, které klientům vadí. Právě nalezení těchto nedostatků by mělo pomoci zjistit, zda existují důvody, které by motivovaly klienty bank k vyzkoušení jedné ze současných kryptoměn.

1 HISTORIE A VÝVOJ

Před zavedením peněz existoval směnný neboli barterový obchod. Lidé mezi sebou obchodovali výhradně výměnou statků a služeb, ale tento přístup k obchodu měl celou řadu známých nedostatků, přičemž tím největším byl tzv. problém dvojí potřeby. To zjednodušeně znamená, že pokud nabízíme maso a pohledáváme dřevo, je nutné hledat někoho, kdo obchoduje se stejnými komoditami ale s opačnými potřebami. (HUJOVÁ, 2014 str. 7) Jedním z těch méně zřetelných problémů byl například výběr daní, který byl velmi obtížný a neefektivní. Cílem tedy bylo zavést jednotné platidlo, které by splňovalo požadované vlastnosti a stát byl schopný ho regulovat. Platidlo, které je každý obchodník ochotný přijímat. Nalezením vhodné komodity (později vytisknutím bankovek), definováním struktury a pravidel pro jejich vydávání, používání a nespočtem dalších náležitostí vzniká měna – centrálně řízený nástroj ovládání ekonomiky. (Pagliery, 2014, s. 4)

Pokud bychom vznik měn a peněz jako platidla, které nemá žádný jiný účel než usnadnění obchodu a má minimální vnitřní hodnotu, vnímali jako významný milník, tak vznik kryptoměn můžeme považovat za stejně důležitý. Kryptoměny nabízejí zcela odlišný a nezvyklý způsob manipulace s penězi, a navzdory počáteční skepsi nadále posilují svoji pozici.

1.1 VLASTNOSTI PENĚZ

Tato práce nemá za cíl podrobně rozebírat pojmy a vztahy z oblasti ekonomie, ale je nutné předložit základní vlastnosti peněz, aby bylo možné provést porovnání s kryptoměnami. Stroukal (2015, s. 28) uvádí tyto stěžejní vlastnosti:

- **Dělitelnost** je základní vlastností moderních peněz. Virtuální měny po této stránce vynikají dělitelností prakticky neomezenou. Pro ukázku je uvedena měna Bitcoin, jejíž základní jednotkou je 1 BTC, momentálně dělitelný na šest desetinných míst. Nejmenším možným obnosem, kterým tedy lze disponovat, je 0,000001 BTC. Nespornou výhodou je, že v případě potřeby úpravy dělitelnosti není nutné tisknout nebo vydávat nové peníze. Budou provedeny pouze úpravy v kódu. Moderní peníze jsou v případě bezhotovostních plateb také velmi dobře dělitelné.
- **Přenositelnost** neboli možnost snadno přenášet velké množství peněz. Dnes není problém přepravit v příručním kufříku několik milionů a peníze v bezhotovostní podobě, jako je např. kreditní karta, nejsou v tomto ohledu limitovány nijak. Stejné je to i s virtuálními měnami, neboť na jedné adrese můžete mít

neomezený obnos. V jaké formě ho uživatel uloží, už záleží pouze na něm. Uchovávání kryptoměn se bude podrobněji věnovat samostatná kapitola Technické vybavení pro manipulaci s kryptoměnami.

- **Vzácnost**. Komodita, která se má stát platidlem musí být vzácná. To znamená, že nesmí být k dostání bez vynaloženého úsilí. Kdyby peníze nebyly vzácné, nikdo by je výměnou za své věci nebo služby nebyl ochotný přijímat. V dobách, kdy se platilo drahými kovy, existoval ještě obdobný pojem vnitřní hodnota. Ten určoval hodnotu peněz v případě, že ztratí funkci peněz. Například zlato lze jako surovina přeměnit na nespočet hodnotných výrobků – má tedy vysokou vnitřní hodnotu. Se současnými penězi se dá v nejhorším případě alespoň zatopit, ale virtuální měny prostě zmizí. Zbyde jen bezcenný řetězec znaků. Po delším zamyšlení je možné jeho vnitřní hodnotu určit délkou výpočetního času nebo objemem spotřebované elektřiny. Takový závěr je ovšem absurdní. (Stroukal, 2015, s. 20)

V minulosti[1] byly peníze kryté zlatem nebo jinými drahými kovy. To zjednodušeně znamená, že naše peníze vyjadřují hodnotu zlata, které klient nebo banka má někde uložené. Odpůrci kryptoměn často argumentují tím, že současné kryptoměny nejsou ničím kryté. Je nutné si uvědomit, že to samé už dlouho platí i o zákonných platidlech.

1.2 CO JE KRYPTOMĚNA

„A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank." (English Oxford Dictionary, 2017) Volně lze přeložit jako: Digitální měna, jejíž šifrovací postupy zajišťují emisi nových jednotek a potvrzování transakcí bez účasti centrální banky.

Mnozí si pod pojmem kryptoměny nebo virtuální peníze představí služby, jako jsou Amazon Pay, Skrill, Google Pay nebo dnes velmi rozšířený Paypal. V takovém případě by za kryptoměny mohly být považovány i peníze uložené na běžném účtu v bance. Peníze, se kterými služby jako Paypal pracují, jsou zákonná platidla neboli tzv. fiat[2] měny, a fakt, že nejsou ve fyzické podobě, na tom nic nemění. Pokud chce uživatel převést peníze na svůj účet Paypal, zadá příkaz pro převod na bankovní účet vlastněný službou Paypal. V případě kryptoměny by postup vypadal velmi podobně. ČNB ovšem kryptoměny nepovažuje za peníze ani jiné cenné papíry. Kryptoměny jsou tedy obchodovány jako elektronika, automobily nebo jakékoliv jiné zboží. (ČNB, 2014)

[1] Ve druhé polovině 19. století existoval tzv. „**zlatý standard**", který definoval hodnotu jednoho dolaru jako určitou část unce zlata. (Lioudis, 2018)
[2] **Fiat** měna je zákonná měna nebo také měna s nuceným oběhem. To znamená, že každý obchodník je povinen ji přijímat.

1.3 VLASTNOSTI KRYPTOMĚN

Současné kryptoměny jsou charakterizovány společnými znaky, které se od fiat měn diametrálně odlišují. Mezi ty důležité patří decentralizace systému prostřednictvím P2P komunikace a využití tzv. Blockchainu namísto centrálního uzlu (Oba pojmy budou vysvětleny v kapitole pojmy). Další velmi zvláštní vlastností je konečný počet jednotek těchto měn a klesající tempo vydávání nových. Většina kryptoměn má daný maximální počet jednotek, který bude dosažen. V minulosti se implementace mnoha kryptoměn ukázaly jako nefunkční a postupným vývojem začaly být výše zmíněné vlastnosti považovány za nepostradatelné.

1.4 HISTORIE KRYPTOMĚN

Přestože vznik a následný úspěch Bitcoinu jsou ve světě kryptoměn bezesporu nejvýznamnějšími událostmi, jeho vzniku předcházelo několik méně či více vydařených pokusů o vytvoření virtuálních peněz. Všechny zanikly, ale ukázaly cestu, jakou by se měl jejich nástupce ubírat.

1.4.1 VZNIK ASYMETRICKÉHO ŠIFROVÁNÍ

Prvním milníkem v historii kryptoměn je vynález Diffie-Hellmanovy výměny klíče. S tímto nápadem přišli v roce 1976 Whitfield Diffie a Martin Hellman. (Diffie, 1976) O rok později byla představena asymetrická šifra RSA[3], což je další velmi důležitá šifrovací technika. Šifře RSA se věnuje samostatná podkapitola Kryptologie v souvislosti s kryptoměnami.

Další důležitou osobností je bezesporu David Chaum, jehož jméno by se dalo považovat za synonymum slova kryptoměny. David Chaum je americký matematik a odborník na šifry, který se velmi výrazně podílel na vývoji mnoha šifer a bezpečnostních protokolů. V roce 1983 prezentoval rozšíření šifry RSA, kterým reagoval na rozvoj elektronických plateb. Ve své práci také vyjádřil obavy z omezení soukromí, vycházejícího z používání tohoto systému a navrhl způsob, jak jej anonymizovat. (Chaum, 1983)

1.4.2 ALTERNATIVNÍ ELEKTRONICKÉ BANKOVNICTVÍ

Právě David Chaum později migroval do Nizozemska a v roce 1989 založil s dalšími významnými společníky[4] společnost DigiCash, která prostřednictvím Ecash[5] umožňovala

[3] **RSA** je zkratka vytvořená z počátečních písmen jmen jejích tvůrců Rivest, Shamir a Adleman.
[4] Stefan Brands, Niels Ferguson, Gary Howland, Marcel van der Peijl, Nick Szabo a Bryce Wilcox-Ahearn.
[5] **Ecash** vznikl spojením slov *electronic* a *cash* coby systém zprostředkující elektronické platby.

anonymně provádět elektronické platby. Služba měla být levnější alternativou kreditních karet. Vynález těchto tzv. Blinded cash vzbuzoval velkou pozornost a společnost se dostala i do konfliktu s nizozemskou národní bankou. Velký zájem projevila firma Microsoft[6], když nabídla Chaumovi 180 milionů dolarů za integraci DigiCash do jejich operačního systému. Velká událost byla nasnadě, Chaum ale prohlásil, že zmíněná částka je příliš malá. Podobným způsobem odmítl i společnost Visa, která chtěla investovat 40 milionů. Nakonec společnost DigiCash roku 1998 zkrachovala, protože ecash nebyl schopen konkurovat službám, které nabízely významné banky. (Griffith, 2014)

Společnost Visa nakonec sama přišla s vlastní digitální měnou Visa Cash. Na to reagoval MasterCard koupí elektronického peněžního systému Mondex. Potenciálním uživatelům ovšem nedali žádný důvod přecházet od tradičního bankovního systému a oba projekty byly později ukončeny pro nezájem. Nejvýraznější úspěch zaznamenala společnost Paypal, kterou v roce 1998 založila skupina podnikatelů, jejímž nejvýznamnějším členem byl bezesporu Elon Musk[7]. Paypal je internetový platební systém existující už přes 20 let. Uživatelé jsou identifikování emailovými adresami a po spojení účtu s kreditní kartou nebo bankovním kontem umožňuje systém instantní bezplatné transakce.

1.4.3 ALTERNATIVNÍ MĚNY

V kapitole Vlastnosti peněz byl zmíněn pojem peníze kryté zlatem. Na základě tohoto principu vznikla měna E-gold, která skutečně byla kryta zlatem. Společnost nakupovala a skladovala velké množství zlata, což se ovšem nelíbilo americké vládě. Nahromaděný majetek byl zabaven a tvůrci měny skončili před soudem.

Ještě dál zašel Bernard von NotHaus, který nedůvěřoval americké měně, a tak si vytvořil vlastní Liberty Dollar (také krytý zlatem). V roce 2011 byl ale odsouzen za padělání peněz a terorismus, neboť se podle soudu pokoušel zničit měnu vlastní země. (Stroukal, 2015, s. 25)

Obdobných měn vzniklo v krátkém časovém sledu ještě několik. Překvapivé bylo především to, jaké popularitě se takto neortodoxní projekty těšily. Všechny měly ale stejný problém. Byly centrálně řízeny, a tak bylo snadné vypátrat autora. Otázkou tedy bylo: Jak můžeme řídit systém bez prostředníka, který na všechno dohlíží?

[6] **Microsoft** je výrobce nejrozšířenějšího komerčního operačního systému Windows.
[7] **Elon Musk** je významný americký podnikatel, který založil společnosti Paypal, Tesla a SpaceX.

1.4.4 BITCOIN

V roce 2008 na tuto otázku odpověděl Satoshi Nakamoto. Ve své práci prezentuje návrh systému včetně tzv. blockchainu, díky kterému vyřešil největší problém kryptoměn – možnost dvojí útraty peněz[8]. Tento koncept spustil na začátku roku 2009. Téměř ihned od něj dal ruce pryč a přenechal doménu Bitcoin.org Gavinu Andersonovi, který byl velký příznivec Bitcoinu a později se stal jeho hlavním vývojářem. (Stroukal, 2015, s. 14)

Satoshi Nakamoto byl pouze pseudonym. Kdo se za ním skrýval, se nikdy nepodařilo zjistit. S rostoucí popularitou Bitcoinu se zvyšoval i zájem o jeho autora. Ten však zanechal pouze několik příspěvků na diskuzních fórech z doby, kdy měnu vyvíjel. Netknuté zůstaly i vytěžené coiny na jeho účtech. Po přečtení kapitoly Kryptologie a principy kryptoměn bude jasné, proč by byla jeho anonymita ohrožena v případě, že by se je pokusil vybrat. Během let padlo podezření na několik lidí včetně krytopgrafa Davida Chauma. Více pravděpodobné ovšem je, že za vývojem protokolu stál celý tým, neboť se jedná o velice rozsáhlý projekt, jehož problematika přesahuje do několika oborů. (Stroukal, 2015, s. 20-23)

Mezitím Bitcoinová síť rostla. Stále více lidí mělo v počítači Nakamotův software, který umožňoval bitcoiny získávat a obchodovat s nimi. Ze začátku pro zábavu, později se začaly objevovat první seriózní inzeráty. S rostoucím zájmem lidí rostla hodnota této nové měny a expanze zrychlovala. Začátkem roku 2010 dosáhl Bitcoin parity[9] s dolarem a dále rostl. V té době už existovaly první burzy, z nichž mezi nejvýznamnější patřila burza MtGox. Ta původně nevznikla za účelem obchodování s kryptoměnami, nýbrž jako platforma pro směnu herních kartiček nejmenované karetní hry. Následující obchod s Bitcoiny ovšem tuto burzu zničil, neboť se stala terčem útoku hackerů. Při útoku bylo ukradeno velké množství Bitcoinu a burza zkrachovala. Právě krach této burzy způsobil v roce 2013 významný pokles hodnoty Bitcoinu a mnozí uživatelé se v obavách začali Bitcoinu zbavovat. Propad ovšem netrval déle než několik týdnů a hodnota Bitcoinu začala opět stoupat. Obrázek 1 zaznamenává vývoj hodnoty Bitcoinu vůči dolaru od poloviny roku 2010 do současnosti. Z obrázku je patrné, že téměř do konce roku 2017 zaznamenal

[8] **Problém dvojí útraty** nastává, když uživatel použije stejné peníze ve dvou různých transakcích. Přestože síť tento problém později odhalí, jeden z obchodníků o své peníze přijde. Toto byl typický problém decentralizovaných sítí.
[9] **Parita** neboli stav, kdy měl 1 bitcoin (BTC) hodnotu 1amerického dolaru (USD).

Bitcoin vytrvalý růst bez významnějších krizí. V posledním čtvrtletí roku 2017 ovšem začala hodnota BItcoinu strmě stoupat a zastavila se až o Vánocích na hranici dvaceti tisíc dolarů za jeden Bitcoin, aby následně mohla pozvolna klesat. Tato událost vyvolala zájem médií i široké veřejnosti a burzy obchodující s kryptoměnami zaznamenaly rekordní příliv nových klientů.

Obrázek 1: Vývoj hodnoty Bitcoinu v letech 2011-2017 (zdroj: (Buy Bitcoin Worldwide, 2018))

Hledání příčin tohoto kolísání cen je složité a prakticky není možné je ověřit. Jedním z důvodů mohl být například uznání Bitcoinu Japonskem za legální platidlo, které platí od 1. 4. 2017. (Keirns, 2017) V průběhu ledna 2018 všechny kryptoměny oslabily téměř na polovinu své hodnoty. Tento propad byl způsoben především zprávami o zavedení regulací v Číně a Jižní Koreji. (Tassev, 2018) Takto významných propadů, které jsou v jiných oblastech považovány za krizi, prodělaly kryptoměny již několik. Vývoj se dříve nebo později vždy vrací zpět do zajetých kolejí vytrvalého růstu, ovšem veřejnost vnímá tyto výkyvy velice negativně. Poslední významnou událostí jsou finanční problémy Nobuaki Kobayashiho, správce burzy MtGox. Ten během posledních měsíců rozprodal Bitcoiny v hodnotě 400 milionů dolarů a negativně tak ovlivnil vývoj kurzu. (Higgins, 2018) Aktuální kurz je možné zjistit například na stránkách https://www.coinmarketcap.com.

Nakonec je vhodné zmínit, že v posledních letech se kryptoměny vždy staly nejvýnosnější investiční komoditou, což také významně zvyšuje jejich popularitu. Největší úspěch zaznamenala kryptoměna Ethereum, která za rok 2017 dosáhla zhodnocení přes 6000 %.

1.4.5 ALTCOINY

S úspěchem Bitcoinu vzápětí přišly stovky dalších měn založených na stejném principu. Ovšem zdá se, že základem úspěchu je přijít s něčím novým, neboť většině měn se ani nepodařilo rozšířit, a pokud ano, zase velice rychle ztratily svoji hodnotu. Mezi ty nejúspěšnější altcoiny patří Litecoin nebo Dogecoin.

2 KRYPTOLOGIE A PRINCIPY KRYPTOMĚN

V této kapitole budou objasněny elementární pojmy nezbytné pro funkci moderních kryptoměn. Výhodou je, že přes velký počet jejich realizací, se základní principy funkce napříč kryptoměnami shodují. Přesto však tato problematika zabíhá do mnoha oborů, a proto budou některé složitější pojmy popsány velice zjednodušeně.

2.1 KRYPTOLOGIE V SOUVISLOSTI S KRYPTOMĚNAMI

Kryptologie je základním kamenem moderních kryptoměn. Jejím prostřednictvím je běžně zajišťována identifikace[10] a autentizace[11] uživatelů. Protokol kryptoměn ji ovšem dokáže využívat i pro vydávání nových jednotek a zároveň potvrzování transakcí. Pro realizaci těchto operací jsou využívány níže uvedené základní techniky a funkce.

Asymetrické šifrování

Asymetrické šifry patří do skupiny šifer, které pro zabezpečenou komunikaci používají dvojici klíčů – soukromý a veřejný klíč. Oba tyto klíče jsou konstruovány tak, aby jejich vlastníkovi umožňovaly provádět pouze určité operace s šifrovanými daty. V současnosti je asymetrické šifrování využíváno nejen k šifrování dat, ale také k jejich digitálnímu podepisování. Česká legislativa využívá pojem elektronický podpis.

2.1.1 RSA (RIVEST, SHAMIR, ADLEMAN) 1977

Jednou z nejstarších a zároveň stále bezpečných šifer je šifra RSA, na které si vysvětlíme princip fungování asymetrického šifrování. Asymetrické šifrování se vždy skládá ze dvou klíčů – soukromého a veřejného. Předpokladem je, že na rozdíl od historických šifer je postup šifrování veřejně známý a bezpečnost zde zprostředkovává řešení matematického problému o asymetrické složitosti. V případě šifry RSA se jedná o faktorizaci čísla neboli inverzní operaci k násobení dvou prvočísel. Postup bude ukázán na konkrétním příkladu.

Na opačných koncích komunikačního kanálu se nacházejí fiktivní postavy Alice a Bob. Tento komunikační kanál je veřejný a kdokoli má možnost zachytit proudící data. Jak tedy navázat bezpečné spojení bez posílání hesla? Začneme tím, že Bob si vymyslí dvě celá kladná čísla *p* a *q.* Důležité je, aby tato čísla byla prvočísla, byla dostatečně velká a na

[10] **Identifikace** je proces, během kterého na základě speciálních znaků zjišťujeme totožnost subjektu.
[11] **Autentizace** je proces ověřování identity.

číselné ose vzdálená od sebe. Při nedodržení těchto požadavků se zvyšuje šance prolomení šifry hrubou silou. Součinem těchto dvou čísel získá *n*. Tedy např.:

$$p = 5, q = 19, n = p * q, n = 5 * 19 = 95$$

Pro další výpočet bude použit následující vzorec:

$$\varphi(n) = \varphi(p-1) * \varphi(q-1), po\ dosazení\ \varphi(n) = \varphi(4) * \varphi(18) = 72$$

Jedná se o tzv. Eulerovu funkci, která bude použita bez dalších důkazů nebo odvození. Pro její řešení bez znalosti členů *p* a *q* zatím nebyl nalezen efektivní algoritmus. Právě tento krok obsahuje matematický problém o asymetrické složitosti. Jak lze vidět výše, je jednoduché určit $\varphi(n)$, pokud jsou známá *p* a *q.* V opačném případě se ovšem za dodržení výše uvedených zásad, určení $\varphi(n)$ stává časově velmi náročnou operací, neboť je nutné provést faktorizaci čísla n. Na tento rozdíl v časové náročnosti se spoléhá. Je totiž možné, že potenciální útočník *n* zjistí, ale v době, kdy už toto číslo nebude platné. (Hrabáková, 2012)

Jako předposlední krok potřebuje Bob vybrat jedno číslo *e* z intervalu {1,..,*n*-1}, které je s *n* nesoudělné. Bob vybere číslo 11 a dosadí ho do rovnice níže.

$$d * e = 1 mod \varphi(n), po\ dosazení\ d * 11 = 1 mod 72$$

Výsledné *d=59* je společně s číslem *n* Bobův soukromý klíč, kterým je schopen dešifrovat zprávy. Dvojice čísel *n* a *e* je veřejný klíč, který Bob pošle Alici. Ta zašifruje svoji zprávu s=32 veřejným klíčem:

$$z = 32^{11} mod 95 = 78$$

Bob dešifruje zprávu od Alice svým klíčem (95,59):

$$s = 78^{59} mod 95 = 32$$

Bob obdržel původní zprávu od Alice s jistotou, že nikdo jiný nebyl schopen přečíst její obsah. (Hrabáková, 2012)

V případě šifry RSA jsou veřejný a soukromý klíč zaměnitelné. To znamená, že je lze využít i opačně. Pokud Bob zašifruje zprávu svým soukromým klíčem, Alice má po přijetí zprávy jistotu, že zpráva přišla skutečně od Boba a nebyla změněna, neboť soukromým klíčem disponuje pouze on. V takovém případě se jedná o digitální podpis.

Vzhledem ke stáří šifry RSA je velice překvapivé, že je stále považována za bezpečnou. Podle organizace NIST[12] je její využití bezpečné při délce klíče od 2048 bitů. Právě kvůli rostoucí velikosti klíče, už se neřadí mezi ty nejefektivnější. V případě kryptoměn se využívá eliptických křivek, které mohou operovat na méně výkonném hardware a s výrazně menšími klíči. Princip funkce zůstává stejný.

2.1.2 METODA ELIPTICKÝCH KŘIVEK (ECDSA)

Šifrování pomocí eliptických křivek (ECC) je v současnosti nejmodernější metodou využívanou k šifrování komunikace a elektronickému podepisování. Teoretický základ byl představen už v roce 1985, a to nezávisle v pracích V. Millera a N. Koblitze. Metoda ECDSA se ale začala rozšiřovat až po roce 2000. Za bezpečnou je považována už při délce klíče 256 bitů a díky tomu vyniká velmi nízkou náročností na hardware. (Klíma, 2002) V tabulce níže jsou porovnány šifry symetrické, RSA a ECC z hlediska délky klíče v závislosti na úrovni zabezpečení. Z tabulky je také vidět, že symetrické šifry vynikají v efektivitě. Jejich návrh ovšem neumožňuje bezpečné navázání spojení přes komunikační kanál.

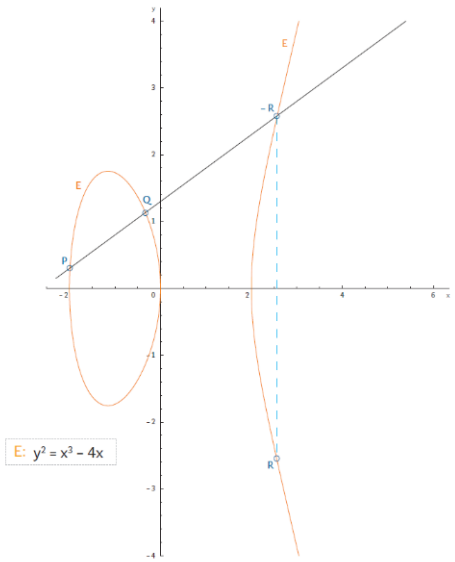
Tabulka 1: Bezpečnost jednotlivých šifer (zdroj: vlastní podle NSA, 2009)

Symetrické šifry (DES, AES)	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Stejně jako algoritmus RSA i ECDSA zakládá svoji bezpečnost na asymetrické složitosti matematické úlohy. Tentokrát se ovšem nejedná o faktorizaci čísla, nýbrž o řešení diskrétního logaritmu. Na tento problém zatím neexistuje algoritmus, který by byl schopen jej efektivně řešit v polynomiálním čase. Pro pochopení principu fungování je nutné mít znalosti z matematické analýzy a diskrétní matematiky, a proto je tato problematika představena pouze obecně bez konkrétních výpočetních operací.

[12] **NIST** je národní institut standardů a technologie spadající pod americkou vládu. Jednou z jeho mnoha činností je i zkoumání bezpečnosti šifrovacích algoritmů.

Základním předpokladem je, že obě strany znají křivku danou rovnicí $y^2 = x^3 - ax + b$, výchozí bod *P,* a také, že jsou schopny si důvěryhodně vyměnit své veřejné klíče. Bez těchto náležitostí není možné komunikaci navázat. Zmíněná rovnice reprezentující křivku je vždy daná konkrétními parametry. Pro představu je přiložena podoba křivky daná rovnicí $y^2 = x^3 - 4x$.



Obrázek 2: Eliptická křivka (zdroj: Chip, 2002)

Hashovací funkce

Hashovací funkce jsou alfou i omegou bezpečnosti v informatice už dlouhou řadu let. S jejich pomocí je možné bezpečně ukládat a efektivně pracovat s otisky jakýchkoliv choulostivých dat tak, aby nikdo jiný nebyl schopen vidět jejich pravou podobu a zároveň měl možnost se přesvědčit o jejich pravosti.

Algoritmy hashovacích funkcí se většinou skládají z elementárních operací, jako jsou například bitové posuny, logické operace (exclusive or) nebo rotace bloků. Posloupnosti takovýchto operací jsou prováděny ve více cyklech. Výhoda využití těchto jednoduchých operací spočívá ve výsledné rychlosti hashovací funkce, protože většina hardwaru je v současnosti pro tyto operace optimalizována instrukčními sadami.

2.1.3 SHA-2

Funkce SHA-2 patří do skupiny hashovacích funkcí SHA navrhovaných organizací NSA ve spolupráci s institutem NIST, který ji zařadil do amerického federálního standardu[13] FIPS (NIST, 2013). SHA-2 byla uvedena v roce 2001, je považována za vysoce bezpečnou a zatím na ni nebyl zaznamenán žádný úspěšný útok. V roce 2015 byla nicméně vydána nová verze SHA-3, která zatím není široce využívána.

Pro snazší orientaci v následujícím textu jsou dále uvedeny základní pojmy. Vstup *x* hashovací funkce je nejčastěji nazýván také předloha nebo vzor. Z toho je hashovací funkcí *H* vytvořen výstup *y* nebo také otisk (anglicky fingerprint). Délka otisku je konstantní tedy nezávislá na délce vstupu. Níže jsou všechny tři pojmy vloženy do rovnice.

$$y = H(x)$$

Hashovací funkce musí splňovat základní bezpečnostní podmínky. Obecně jsou na všechny druhy hashovacích funkcí kladeny následující nároky:

- Není možné nalézt **původní předlohy** (Preimage resistence). To je důležitá vlastnost především při manipulaci s hesly. Heslo je nutné ukládat, aby bylo možné ho porovnat s heslem, které zadá uživatel při pokusu o přihlášení. Pokud se uložené heslo shoduje se zadaným, uživatel je autorizován. Ukládat v databázi hesla jako plaintext[14] je ovšem velice nezodpovědné, a právě hashovací funkce tento problém řeší. Namísto hesla je v databázi uložen a porovnáván jen jeho otisk, který je výstupem hashovací funkce. Tento otisk je unikátní řetězec, který je možné získat pouze z jediné předlohy.
- Není možné nalézt **jinou předlohu** (2nd preimage resistence). Stejně tak je i důležité, aby útočník nebyl schopen nalézt jiný řetězec, který by generoval stejný otisk. Pokud by se výsledný hash shodoval s hashem původní předlohy, z principu by neexistovala žádná možnost odhalení problému a útočník by disponoval sice jiným, ale funkčním heslem.
- Minimální **korelace** vstupu a výstupu. Pokud se minimálně změní předloha, hashovací funkce by měla reagovat významnou změnou otisku, aby bylo zamezeno použití statistické analýzy. (Toman, 2001) (Menezes, 1997)

[13] **FIPS** je skupina standardů, které popisují šifrovací algoritmy a další technologické postupy pro nevojenské využití americkou vládou.
[14] **Plaintext** je v oblasti kryptografie chápán jako nešifrovaná textová informace.

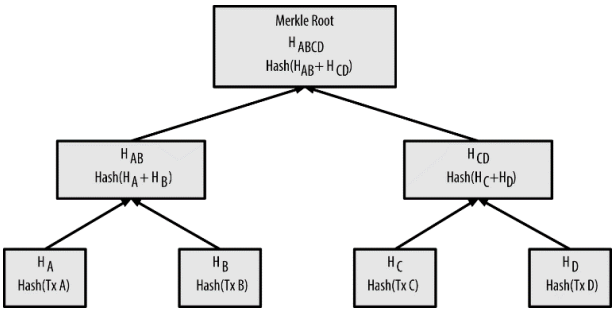
2.1.4 RIPEMD-160

Dalším významným zástupcem hashovacích funkcí je bezesporu funkce RIPEMD-160 jakožto vylepšení funkcí MD4, MD5 a RIPEMD. V druhé polovině 90. let přestaly být tyto funkce považovány za bezpečné, neboť metodou brute force[15] bylo možné s tehdejším hardwarem nalézt kolizi do jednoho měsíce. Později byly nalezeny i algoritmy, kterými bylo možné předlohu klíče získat významně rychleji. Hlavním problémem byla nedostatečná délka klíče, která byla u všech tří zmíněných funkcí 128 bitů. Jak už název napovídá, autoři RIPEMD – 160, Hans Dobbertin, Antoon Bosselaers, and Bart Preneel, použili klíč o délce 160 bitů a tím zaručili bezpečnost. (Antoon, 2012)

2.1.5 BINÁRNÍ (MERKLEŮV) STROM

Je datová struktura, umožňující snadné ukládání a vyhledávání dat. Binární strom vždy začíná jedním uzlem, který se větví na dva další potomky. Ty se v případě potřeby dále rekurzivně dělí. Binární strom se tedy staví „od kmene“.

Americký kryptolog Ralph Merkle přišel s modifikací binárního stromu, ve které prezentoval přidání hashovací funkce, s jejíž pomocí byl schopen efektivně ověřovat konzistenci velkého množství dat uložených v binárním stromě. Merkleův nebo také hashovací strom se staví opačně, tedy „od listí“. Všechna data, která mají být zahrnuta do stromu, jsou vložena na poslední úroveň tak, aby neměla žádné potomky. Poté jsou nad dvojicemi dat provedeny hashovací funkce. Výstup hashovací funkce je vždy vstupem pro funkci na vyšší úrovni stromu. Tato operace je rekurzivně opakována na vyšších úrovních, dokud nezůstane jediný hash – tzv. Merkle Root. Postup je schématicky zobrazen (viz Obrázek 3). (Bashir, 2017, s. 95)



Obrázek 3: Merkleův strom (zdroj: (ANTONOPOULUS, 2014, s. 171))

[15] **Brute force** metoda nebo také metoda hrubé síly patří mezi nejméně efektivní metody prolamování šifer, při které se útočník snaží nalézt klíč bez znalosti algoritmu, pouze zkoušením všech možných kombinací.

Z obrázku je zřejmé, že tento postup vyžaduje sudý počet dat. V případě, že existuje pouze lichý počet, jsou poslední data duplikována. Z vlastností hashovací funkce vyplývá, že poslední tzv. kmenový hash se při změně dat kdekoliv ve stromu změní také.

2.2 POJMY

V této kapitole budou popsány dílčí pojmy a algoritmy, ze kterých se systémy kryptoměn skládají. Většina těchto algoritmů je známa desítky let. Nový je pouze způsob, jakým jsou využívány.

2.2.1 DECENTRALIZOVANÁ SÍŤ

Síť neobsahuje žádný centrální bod (server), prostřednictvím kterého by probíhala komunikace. Jinými slovy jsou si všechny body v síti rovny a mají stejné možnosti (tento model se také nazývá P2P). Z této vlastnosti plyne mnoho významných výhod. Především je síť velmi odolná vůči útokům, neboť útočník nemá možnost napadnout uzel, jehož vyřazení by způsobilo problémy.

Další nespornou výhodou je fakt, že s velikostí sítě roste komunikační rychlost a výpočetní síla. Rychlost komunikace je velkým problémem rychle rostoucích centralizovaných sítí, kdy jsou servery přetěžovány. “Nevýhodou P2P sítě je obtížnost počátečního navázání komunikace.“ (Stroukal, 2015, s. 168)

Model P2P sítí je znám už velice dlouho. Nejvýznamnějším využitím jsou různé nástroje pro sdílení dat, kdy si mezi sebou soubory posílají samotní uživatelé. Je nutné neopomenout, že mohutnější sítě umožňují velmi vysoké rychlosti sdílení. Problémem může být ochota jednotlivých uzlů sdílení zprostředkovat. Proto většina implementací kryptoměn jednotlivé uzly za jejich služby odměňuje.

2.2.2 SOUKROMÝ KLÍČ

Problematika soukromých klíčů byla již zmíněna v kapitole Kryptologie v souvislosti s kryptoměnami, kde bylo nastíněno, jak takový klíč vzniká. V oblasti kryptoměn lze soukromý klíč považovat za heslo, kterým jsou autorizovány platby. Většina kryptoměn využívá jako soukromý klíč 256 – bitové číslo, což znamená 32 bajtů neboli 64 znaků v rozsahu [0 – 9] a [A – F].

2.2.3 VEŘEJNÝ KLÍČ

Veřejný klíč má délku 65 bajtů a je vytvářen ze soukromého klíče. Tento proces samozřejmě není reverzibilní. Mnohé zdroje uvádějí, že veřejný klíč je adresa našeho účtu. Přestože toto tvrzení běžnému uživateli postačuje, není to zcela pravda. Pro zvýšení bezpečnosti je za veřejný klíč přidána další vrstva – adresa.

2.2.4 ADRESA

Adresa je alfanumerický řetězec o délce 26-35 znaků. Generace adresy je proces, během kterého jsou na veřejný klíč v daném pořadí aplikovány šifrovací algoritmy SHA-256 a RIPEMD-160, které byly popsány již dříve. Veřejný klíč a adresa jsou tedy matematicky svázány. Posledním krokem při vytváření adresy je přidání čtyř kontrolních bajtů, které zaručují, že uživatel neprovede transakci s neexistující adresou. Důležité také je, že nové páry klíčů a adres je možné vytvářet i bez připojení k síti a jejich počet prakticky není omezen[16].

2.2.5 TRANSAKCE

Transakce je soubor dat, který jako celek definuje konkrétní manipulaci peněz v síti. Co se vytvoření nové transakce týká, je na první pohled velice podobná transakci v běžném bankovnictví. Postačuje zadat adresu odkud, kam a kolik si uživatel přeje poslat. V okamžiku, kdy transakci podepíše jeho soukromým klíčem, je transakce vytvořena a odeslána k ověření. Níže jsou uvedena data obsažená v každé transakci:

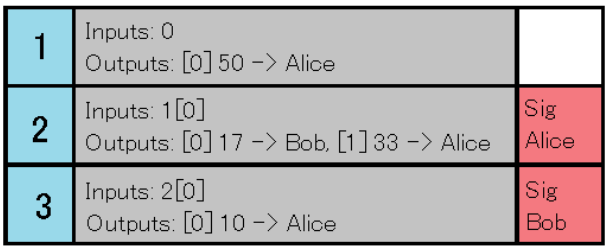
1. **Metadata** obsahují informace nezbytné pro zpracování transakce. Mezi ně patří hash kompletní transakce sloužící jako její unikátní identifikátor, počet vstupů, výstupů a velikost transakce.
2. **Vstupy** reprezentuje datová struktura pole, ve které jsou uloženy adresy, ze kterých budou odeslány prostředky. Je velice důležité si uvědomit, že tyto adresy jsou výstupy předešlých transakcí, prostřednictvím kterých byly prostředky vytvořeny. U každého vstupu je ještě podpis, který ověřuje oprávnění manipulovat s jednotkami na vstupních adresách.
3. **Výstupy** reprezentuje datová struktura pole, kde je uložena adresa příjemce a také skriptovací příkazy, které ověří platnost transakce.

Transakce jsou rozděleny na **běžné** a **generující**. Zatímco běžnými transakcemi je realizováno posílání peněz, při generující transakci vznikají nové jednotky. Taková

[16] **Počet** je omezen rozsahem funkce RIPEMD-160 na počet 2^160 adres. Z praktického hlediska se dá mluvit o nekonečnu.

transakce má prázdné pole vstupů. Problematika generujících transakcí bude popsána v následujících kapitolách Bloky a Těžba jednotek.

Z jiného hlediska se tyto transakce od těch bankovních velmi odlišují. Při provedení transakce se na všech vstupních adresách peníze „zničí“ a jsou vytvořeny nové na výstupních adresách. Obrázek 4 schématicky zobrazuje posloupnost transakcí. První z nich je generující transakce, během které bylo na Alici adrese vytvořeno 50 jednotek. Ta v následující transakci pošle Bobovi 17 jednotek a zbylých 33 jednotek bude připsáno zpět Alici. Je možné si všimnout, že vstupy této transakce odkazují na první generující transakci, tím může být potvrzen původ jednotek, kterými Alice disponuje. Pro doplnění Bob posílá 10 jednotek zpět Alici. V obou případech transakci uživatelé podepisují svým soukromým klíčem.



Obrázek 4: Transakce (zdroj: vlastní)

Pro lepší představu může být tento postup analogicky přirovnán k bankovnímu příkazu. Uživatel část peněz někomu pošle a zbytek bude převeden na novou adresu, která je právě vytvořena. Adresa je matematicky spjata s veřejným klíčem uživatele. Tím je zaručeno, že k ní bude mít přístup. Tento zdánlivě komplikovaný postup zajišťuje jednoduchou správu adres bez použití dalších struktur, které by sledovaly pohyby peněz. Navíc zvyšuje bezpečnost, neboť v případě, že by byl prolomen šifrovací protokol ECDSA, adresu uživatele stále chrání hashovací algoritmus RIPEMD160.

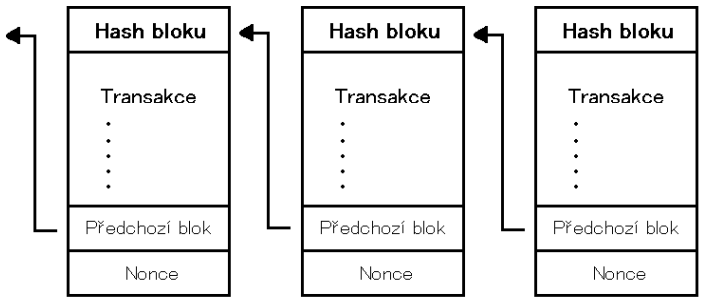
2.2.6 BLOKY

Čekající transakce je nutné nějakým způsobem potvrdit a evidovat. S rostoucím počtem uživatelů stoupá i počet transakcí a potvrzovat je po jedné by v P2P síti bylo neefektivní. K tomuto účelu byly tedy navrženy tzv. bloky konsolidující transakce do skupin, které jsou potvrzovány jako celek. Validita transakce zahrnuté v bloku vychází z přítomnosti bloku v blockchainu.

Transakce ovšem v bloku nejsou jednotlivě umístěny, ale jsou organizovány v tzv. Merklově stromu, který významně zvyšuje efektivitu ověřování proběhlých transakcí. Merkelův strom je popsán v kapitole Kryptologie v souvislosti s kryptoměnami.

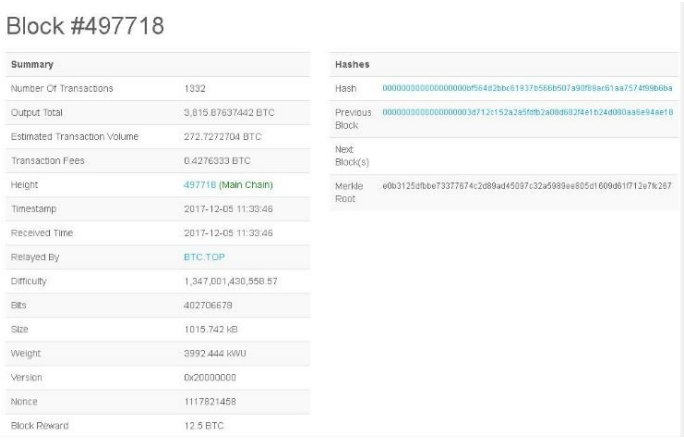
Nové bloky vznikají v uzlech, které jsou nejčastěji nazýváni „těžaři“. Ti v síti vyhledávají nové transakce, ze kterých společně s dalšími daty vytvářejí nový blok. Každý blok se skládá z následujících dat:

- **Transakce** čekající na potvrzení tvoří většinu velikosti bloku. Minimální počet transakcí zahrnutých do bloku není určen a záleží pouze na tom, kolik jich při vytvoření nového bloku bylo k dispozici. Horní hranice je omezena maximální možnou velikostí bloku. Ta se liší v jednotlivých implementacích kryptoměn. V každém bloku se nachází právě jedna generující transakce, která odměňuje těžaře za vytvoření bloku.
- **Odkaz** na poslední blok. Každý nový blok obsahuje ukazatel na blok před sebou. Tím je možné sledovat historii transakcí a ověřovat tak původ peněz použitých v nových transakcích.
- **Adresa** těžaře. Jak už bylo zmíněno dříve, těžaři jsou za vytváření nových bloků odměňováni. Do bloku tedy přidá i jednu generující transakci, ve které do výstupu zadá adresu, na kterou si v případě zařazení bloku do blockchainu přeje vyplatit odměnu.
- **Nonce**. V úvodu bylo uvedeno, že ne každý vytvořený blok je automaticky validní. Všechny bloky mají stejně jako transakce svůj unikátní hash. Právě na tom závisí validita bloku. Nonce je tedy číslo, jehož změnou se změní i hash bloku.



Obrázek 5: Struktura bloku (zdroj: vlastní)

Vytvoření bloku je velice jednoduché. Vytvoření validního bloku, který může být zařazen do blockchainu je o mnoho složitější. Každý blok je stejně jako transakce reprezentován hashem. V případě bloku musí tento hash splňovat velmi přísné kritérium, které bude přiblíženo v kapitole Těžba jednotek. Úkolem každého těžaře je zkoušet různé nonce, aby výsledný hash splňoval stanovené kritérium. Na následující stránce je zobrazen náhodný blok zahrnutý do blockchainu. (viz Obrázek 6).



Block #497718

Summary	
Number Of Transactions	1332
Output Total	3,815.67637442 BTC
Estimated Transaction Volume	272.7272704 BTC
Transaction Fees	0.4276333 BTC
Height	497718 (Main Chain)
Timestamp	2017-12-05 11:33:46
Received Time	2017-12-05 11:33:46
Relayed By	BTC.TOP
Difficulty	1,347,001,430,556.57
Bits	402706678
Size	1015.742 kB
Weight	3992.444 kWU
Version	0x20000000
Nonce	1117821458
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000000bf564d2bbc61937b566b507a90f89ac61aa7574f99b6ba
Previous Block	0000000000000000003d712c152a2e5fdfb2a08d682f4e1b24d080aa6e94ae18
Next Block(s)	
Merkle Root	e0b3125dfbbe7337787 4c2d89ad45097c32a5989ee805d1609d61f712e7fc267

Obrázek 6: Blok zařazený v blockchainu (zdroj: vlastní z www.blockchain.info)

2.2.7 BLOCKCHAIN

Blockchain je nezvýznamější inovací kryptoměn, která se poprvé objevila v měně Bitcoin. Zjednodušeně je možné ho přirovnat k nekonečné účtence, kde jsou uvedeny všechny platby, které byly provedeny. Už z názvu vyplývá, že se jedná o řetězec jakýchsi bloků. Tyto bloky byly popsány v předchozí kapitole a jejich zahrnutím do řetězce vzniká blockchain. Na obrázku níže je zobrazen jeho vrchol s několika bloky. V kapitole Bloky je uvedeno, že každý blok obsahuje odkaz na předchozí blok. Z toho vyplývá, že blockchain

<< Previous Blocks mined on: 05/04/2018 Next >>

Height	Time	Relayed By	Hash	Size (kB)
516730 (Main Chain)	2018-04-05 10:56:43	SlushPool	0000000000000000001213fe858aa83e24ec9ce7aeb9027052dc357ec83eddfd	375.49
516729 (Main Chain)	2018-04-05 10:49:50	BTC.com	0000000000000000002908150257d5d74207bb2d85d32233f2b792052df4fdfa	1,194.7
516728 (Main Chain)	2018-04-05 10:36:18	AntPool	0000000000000000002ed2f998e19deee926bdfead73390202bf723aabe22b13	1,153.01
516727 (Main Chain)	2018-04-05 10:25:32	BTC.com	0000000000000000001c9d3c33b91892f4e722e628a6c3eec2cd528aa7d3f02b	1,140.69
516726 (Main Chain)	2018-04-05 10:09:07	BTC.TOP	0000000000000000000157b93254da0fc2187b68facd722ce2481ff4dcc057c7c	1,104.54
516725 (Main Chain)	2018-04-05 09:38:29	BTC.com	0000000000000000001d9c3e3c49f6aafa21f2f77c5f865dd275ec63e8a345dd	495.96
516724 (Main Chain)	2018-04-05 09:37:22	BTC.com	0000000000000000002e93212df84093d03edad41685fc479dd72bf22ab128ca	1,114.79
516723 (Main Chain)	2018-04-05 09:20:36	SlushPool	0000000000000000049ca9b502478e1d50d280f0e6f13eb23a64a2ceca0b552	1,151.52

Obrázek 7: Blockchain (zdroj: vlastní z www.blockchain.info)

je lineární neboli spojový seznam – v informatice jedna z velmi rozšířených datových struktur. Do blockchainu je možné nahlížet prostřednictvím speciálních programů nebo přes prohlížeče v podobě webových stránek (např. www.blockchain.info). Spíš než pro uživatele, je ale určen pro systém, který podle něj zjišťuje zůstatky na všech existujících adresách. Důležité je, že pokud transakce, respektive blok, ve kterém se nachází, nebyla zahrnuta do blockchainu, je neplatná a systém ji nezohledňuje.

Technologie blockchainu je jeden z nejvýznamnějších vynálezů, který kryptoměny přinášejí. Jedná se o decentralizovaný systém, který je zároveň vysoce bezpečný a díky tomu vhodný k mnoha různým aplikacím.

2.2.8 TĚŽBA JEDNOTEK

Těžba jednotek je jediný způsob emise nových jednotek do oběhu. Je nutné si uvědomit, že za těžbu jednotek považujeme sběr transakcí a jejich následné zařazení do blockchainu v podobě bloku, přičemž vytěžené jednotky jsou vlastně odměna za vynaložené úsilí. Těžba tedy není samoúčelná operace, ale naopak zastává důležitou funkci provádění transakcí. Většina kryptoměn má omezené množství jednotek, ale po vytěžení tohoto objemu se těžba nemůže zastavit, protože by dále nebylo možné potvrzovat transakce a obchodovat. Těžaři budou nadále potvrzovat bloky a jejich odměnou budou poplatky za provedení transakcí, které zaplatí uživatelé.

Těžaři tedy v síti vyhledávají nové transakce, které konsolidují do bloků. Maximální velikost bloku se v různých implementacích liší, ovšem minimální velikost bloku není definována. Pro zajištění rovnoměrně rozloženého potvrzování transakcí v čase je nutné zajistit, aby nové bloky byly do blockchainu zařazovány v přibližně stejných časových intervalech. Toho tvůrci docílili zavedením podmínky, kterou musí blok splňovat. Podmínka udává maximální velikost hashe bloku. Nejčastěji je tato podmínka nazývána obtížností, což je kladné celé číslo, které udává počet nul v řetězci zleva. Pro lepší představu jsou níže uvedeny hashe dvou bloků. Ten první obtížnost 17 nesplňuje, druhý ano.

$$0000000000da2a93cd20da05c74f246c4728fbd4eda2a93cd05cf36fbb7257d9$$

$$00000000000000000b9386873d70422f5d8f878fb086fa67d9fa3b01e6bf7cb$$

Cílem těžařů je vyzkoušet co nejvíce hashů, aby maximalizovali šanci, že naleznou ten validní. Pokud ovšem má být výstupem hashovací funkce jiný otisk, je nutné v bloku něco změnit. První možností je přidat do bloku nové transakce, které byly mezitím vytvořeny Daleko rychlejší variantou je změna tvz. nonce, což je náhodné číslo obsažené v bloku, určené právě ke změně hashe. Obtížnost mění systém automaticky a reaguje tak na aktuální výpočetní sílu sítě. Při nalezení bloku, jehož hash podmínku splňuje, těžař o této události informuje ostatní v síti a zároveň zveřejní obsah bloku včetně nonce, se kterou validní hash nalezl. Poté může být blok zařazen do blockchainu a celý postup se opakuje

s novými transakcemi. Jedná se tedy o soutěž. Každý těžař se snaží vyzkoušet co možná nejvíce hashů a s tím souvisí nároky na hardware, kterým se zabývá kapitola Hardware.

Tento způsob validace bloků, kdy těžař musí vynaložit úsilí v podobě času a výpočetního výkonu, respektive spotřebované elektřiny, se nazývá *proof of work*. Výhodou tohoto systému je, že spravedlivě řeší problém výběru těžaře, který vydá nový blok. Naopak nevýhodou je extrémně nízká efektivita, neboť těžaři při hledání validního hashe spotřebují zbytečně velké množství elektrické energie. Tento problém se snaží vyřešit jiné implementace zavedením metody *proof of stake*, který by těžaře spravedlivě vybíral na základě různých parametrů.

3 KRYPTOMĚNY

Se znalostí základních pojmů nyní mohou být představeny konkrétní kryptoměny. V současné době je jich nepřeberné množství, ovšem většina z nich nepřichází s inovacemi, pouze se snaží těžit z úspěchu jiných. Existence takových kryptoměn nebývá delší než jeden rok. Níže jsou uvedeny měny, které fungují již delší dobu a společnost o ně jeví zájem. Porovnány budou především vlastnosti, které vycházejí z jejich implementace a pro uživatele jsou z hlediska používání důležité.

3.1 BITCOIN

Nejrozšířenější implementací kryptoměn je bez pochyb Bitcoin. V současné době je možné s ním platit po celém světě, disponuje širokou sítí bankomatů a Japonsko ho oficiálně uznalo za platidlo. Toto jsou výhody, které momentálně žádná jiná kryptoměna nabídnout nemůže.

3.1.1 ZÁKLADNÍ ÚDAJE

- Vznik: leden 2009.
- Název a jednotka: Bitcoin (BTC).
- Maximální počet jednotek v oběhu: 21 milionů.
- Čas mezi novými bloky: ~ 10 minut.
- Algoritmus: SHA-256.

3.2 LITECOIN

Je typickým nástupcem Bitcoinu, který se pokouší vylepšit jeho nedostatky. Přestože jeho implementace zahrnuje viditelná vylepšení pro běžné uživatele, překonat Bitcoin se mu zatím ani zdaleka nepodařilo. Charles Lee, tvůrce Litecoinu, se soustředil na nevyhovující dobu potvrzování transakcí a na nedostatky týkající se těžby nových jednotek. Lee tedy zkrátil dobu potvrzování nových bloků na přibližně 2.5 minuty a také vyměnil hashovací algoritmus SHA256 za algoritmus Scrypt. Tím docílil výrazného snížení možností paralelizace[17]. (Coindesk, 2014)

[17] **Paralelizace** je postup využívaný při řešení úloh, které je možné rozdělit na více částí. Náročnost úlohy se tak rozdělí mezi více procesorů, čím se může délka zpracovávání úlohy v ideálním případě zkrátit až *n*-krát, kdy *n* je počet procesorů.

3.2.1 ZÁKLADNÍ ÚDAJE

- Vznik: říjen 2011.
- Název a jednotka: Litecoin (LTC).
- Maximální počet jednotek v oběhu: 84 milionů.
- Čas mezi novými bloky: ~ 2.5 minuty.
- Algoritmus: Scrypt.

3.3 DŮSLEDKY VYPLÝVAJÍCÍ Z IMPLEMENTACÍ

Implementace Bitcoinu zajišťuje, že nový blok bude zařazen do blockchainu přibližně každých deset minut. To samozřejmě znamená, že pokud zaplatíme za zboží, obchodník musí počkat minimálně deset minut, než bude transakce platná. Takové potvrzení ovšem není příliš důvěryhodné a je vhodné ho používat jen pro platby velmi malých částek. Může nastat situace, kdy v jiné části sítě (myšleno fyzicky vzdálené) bude do blockchainu přidán jiný blok, který ten předešlý později při synchronizaci sítě vyřadí. Z tohoto důvodu je doporučováno šestinásobné potvrzení bloku. To znamená, že blok, ve kterém se nachází transakce, bude překryt následujícími pěti bloky. To ovšem také znamená, že celý obchod může trvat přes hodinu. Charles Lee tento čas zkrátil na 15 minut. Vývojáři Bitcoinu se také snaží nalézt řešení tohoto problému a v současnosti se pracuje na nadstavbě blockchainu nazývané Lightning Network. Ta by měla zajistit instantní provádění transakcí a zároveň významně snížit poplatky za jejich provedení. Projekt je nyní ve fázi testování. (Torpey, 2018)

Dalším problémem, který se Charles Lee v implementaci své měny snaží vyřešit je snadná paralelizace a následná centralizace potvrzování transakcí. Prvotní myšlenkou při návrhu Bitcoinu bylo, že část uživatelů bude zároveň plnit i funkci těžařů. Tento plně decentralizovaný stav ovšem neměl dlouhého trvání. Snahou každého těžaře bylo maximalizovat šanci, že právě on nalezne další validní blok a bude odměněn. Majetnější uživatelé tedy investovali do výkonnějšího hardwaru, který jim zajistil výhodnější postavení. Později začala vznikat různá sdružení těžařů, tzv. mining pooly, které zajišťovaly menší, ale za to stabilní příjem. Následovali je výrobci speciálních integrovaných obvodů,

kteří vycítili příležitost zisku a začali navrhovat zařízení určená pro těžbu Bitcoinu. Tato zařízení svou výpočetní silou znemožnila rentabilní těžbu na osobních počítačích. Do speciálních obvodů investovala především větší sdružení těžařů, která si zajistila majoritní postavení v síti. To sice není přímá bezpečnostní hrozba, ovšem zcela odporuje původní vizi decentralizované sítě zakladatele Nakamota. Nejvýznamnějšího podílu v síti dosáhl v červnu roku 2014 mining pool Ghash.io, kterému se podařilo dosáhnout podílu 50 % výpočetního výkonu celé sítě. (Naranyanan, 2016) Takový podíl významně zvyšuje šanci na úspěšné pokusy manipulace s transakcemi. Uživatelé i těžaři jsou ovšem přirozeně motivováni udržovat měnu v bezpečí a v těchto případech příliš veslké pooly opouštějí. Zmíněné problematice speciálních obvodů se věnuje kapitola Speciální hardware. V implementaci Litecoinu se díky algoritmu Scrypt dostaly ke slovu zpět grafické karty. Především ty herní, které disponují velkou kapacitou operační paměti.

Jak už bylo řečeno, důvodem změny hashovací funkce ze SHA2 na Scrypt je znemožnění používání levných integrovaných obvodů s vysokým výkonem. Algoritmus Scrypt svými nároky na kapacitu operační paměti vrací těžbu zpět na osobní počítače, které disponují běžnými grafickými kartami, protože výroba speciálních obvodů s velkou kapacitou paměti je momentálně nevýhodná. Podobným způsobem paralelizaci brání i další kryptoměny, jejichž algoritmy mají v čase proměnné nároky na operační paměť.

3.4 ETHEREUM

Pro doplnění je zmíněn systém Ethereum, který ovšem neplní pouze funkci měny. Jedná se o decentralizovanou síť tvořící Turingovsky úplný virtuální stroj spravující tzv. Smart contracts – komplexní platební systém nahrazující jednotlivé transkace. Ethereum představil v roce 2013 ruský programátor Vitalik Buterin. Během roku 2014 byl vývoj zafinancován prostřednictvím crowdfundingu a o rok později byl v červenci systém spuštěn. (Hertig, 2017) V současnosti se kryptoměna Ether stává velmi populární. Její technická implementace umožnuje mimo okamžitého potvrzování transakcí spoustu sofistikovaných funkcí, které mají ambice automatizovat v současnosti zpoplatněné služby jakou je například Kickstarter.

4 TECHNICKÉ VYBAVENÍ PRO MANIPULACI S KRYPTOMĚNAMI

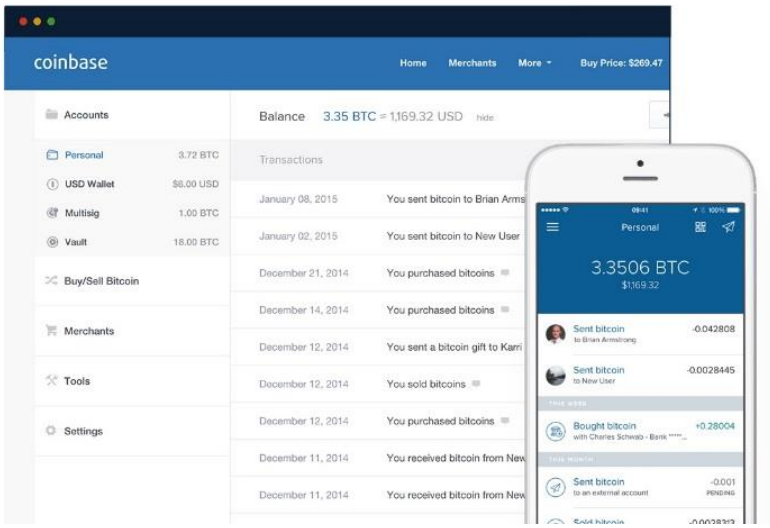
Protokoly kryptoměn využívají pro zajištění bezpečnosti mnoha pokročilých technik. Pokud chceme s kryptoměnami obchodovat, potřebujeme určité technické vybavení. Software, prostřednictvím kterého je možné spravovat účty a vytvářet transakce. Pokročilejší uživatelé, kteří by chtěli plnit roli plnohodnotného uzlu, potřebují také další hardware s vysokým výpočetním výkonem a kapacitou uložiště. V následujících kapitolách budou všechny tyto aspekty přiblíženy.

4.1 SOFTWARE

Programové vybavení rozlišujeme především podle jejich účelu. V tomto ohledu je můžeme rozdělit na tzv. lehké a těžké klienty. Z pohledu četnosti je v daleko větší míře využívaný odlehčený software, který běžným uživatelům umožňuje provádět základní operace a není nijak náročný na hardware. Naopak pro pokročilejší uživatele je určen plnohodnotný software, který v kombinaci s vhodným hardwarem umožňuje navíc těžbu jednotek. Peněženek, jak se tento software také jinak nazývá, existuje celá řada, přičemž většina organizací na svých stránkách uvádí ty, které podporují danou měnu.

4.1.1 ONLINE PENĚŽENKY

Nejjednodušší a nejrychlejší variantou, jak si založit účet na kryptoměny, je online peněženka. Stačí si vybrat jednu z mnoha stránek (např. www.coinbase.com) a zaregistrovat se. Tyto stránky často provozují i vlastní směnárny a burzy. Do peněženky se uživatel registruje přístupovým heslem. Pro aktivaci všech funkcí je nutná identifikace řidičským průkazem nebo cestovním pasem. Samozřejmostí je dvojfázové ověřování při přihlašování a provádění plateb. Uživatelské prostředí se velice podobá standardnímu internetovému bankovnictví. Samozřejmostí je také možnost spravovat svůj účet přes mobilní aplikaci. Na následující stránce je zobrazeno uživatelské prostředí peněženky Coinbase (viz Obrázek 8).



Obrázek 8: Uživatelské prostředí účtu (zdroj: vlastní z www.coinbase.com)

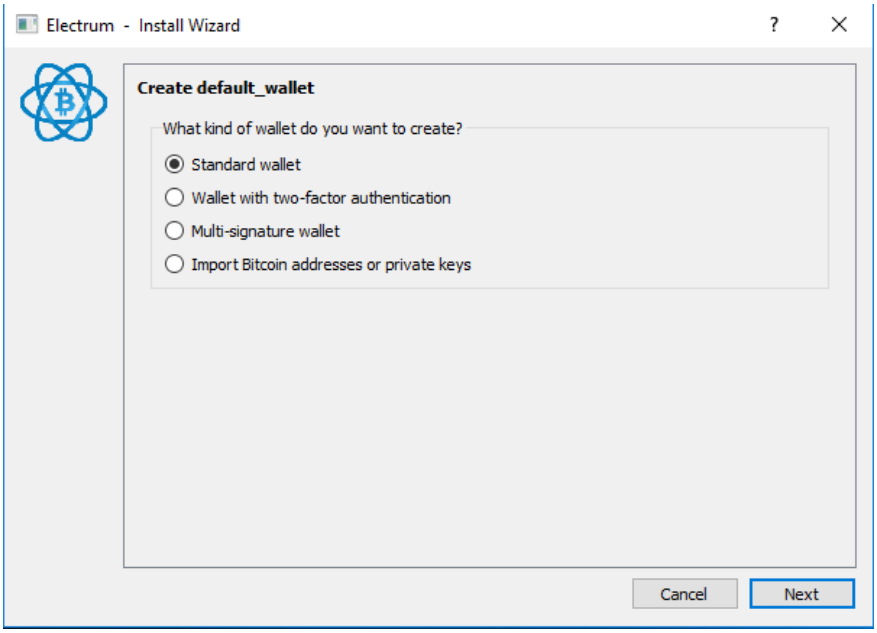
Jednotlivé online peněženky poskytují různé způsoby a úrovně zabezpečení. U některých se uživatel autorizuje pouze přístupovým heslem. Jenže když uživatel nemá přístup ke svému soukromému klíči, nemá ani plnou kontrolu nad svým účtem. Tento přístup má své výhody i nevýhody. V případě ztráty hesla je možné ho cestou alternativního ověření obnovit a uživatel tak nepřijde o svůj účet, což může být u jiných typů peněženek velký problém. Pokud se ovšem provozovatel dostane do problémů, může se stát, že uživatel o své vklady přijde. Příkladem za všechny je krach japonské burzy MtGox v roce 2014, kdy se ztratilo přes 700 000 Bitcoinů a významná část uživatelů o všechny peníze přišla. (Osterman, 2015) Zatím není jisté, kdo Bitcoiny odcizil a vyšetřování stále probíhá. Online peněženka není vhodná pro zkušenější uživatele obchodující s velkými částkami. Tento typ peněženky mohou ocenit naopak začátečníci, kteří se nechtějí zatěžovat složitější manipulací se soukromými klíči. Daní za jednoduchost jsou ovšem poplatky, které si služby účtují za manipulaci s coiny, a také fakt, že tento přístup se vlastně zcela vymyká základním principům kryptoměn, neboť vlastník účtu není anonymní a jeho účet spravuje třetí strana.

4.1.2 ODLEHČENÉ PENĚŽENKY

Velmi populárními se v současnosti stávají odlehčené verze peněženek, které umožňují plnohodnotnou administraci účtů a zároveň nekladou vysoké nároky na hardware. V tomto případě má uživatel přímou kontrolu nad všemi svými adresami, ovšem není nutné mít v počítači uložený celý blockchain. Odlehčené peněženky si stahují pouze tu

část blockchainu, ze které je možné vypočítat zůstatek na adresách vlastněnými uživatelem. S výběrem peněženky může pomoci i seznam ověřených peněženek, který bývá dostupný na oficiálních stránkách konkrétní kryptoměny. Obsluha se napříč peněženkami a měnami příliš neliší. Následující text se tedy bude věnovat jedné z nejrozšířenějších – peněžence Electrum.

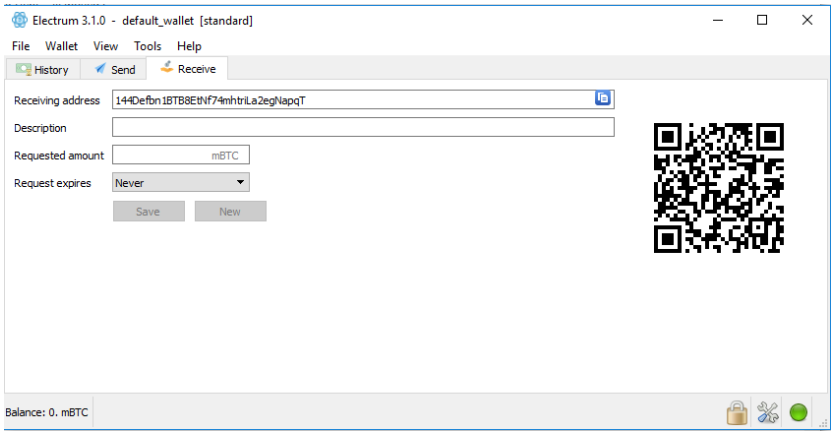
Instalace takové peněženky zabere jen několik minut a zvládne ji i uživatel se základními znalostmi práce s počítačem. Při prvním spuštění má uživatel možnost si vybrat úroveň zabezpečení nové peněženky nebo importovat již existující peněženku uloženou v počítači (viz Obrázek 9).



Obrázek 9: Intalace peněženky Electrum (zdroj: vlastní)

Standardní peněženka je zabezpečena uživatelským heslem a úroveň jejího zabezpečení tedy závisí na dodržení zásad při tvorbě hesla. Další možností je peněženka s dvoufaktorovým ověřováním, které přináší významné navýšení bezpečnosti, ovšem na úkor pohodlí. Pro přístup do peněženky uživatel potřebuje navíc aplikaci Google Authenticator, která zajišťuje druhý ověřovací krok.

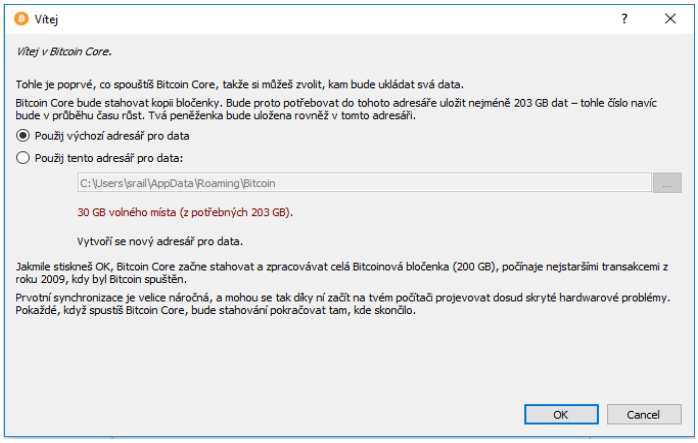
Uživatelské rozhraní je jednoduché a velice intuitivní. Zároveň díky velmi podrobnému nastavení ji mohou využívat i náročnější uživatelé. Po přihlášení do peněženky se zobrazí základní nabídka (viz Obrázek 10). Zde jsou po ruce nejpoužívanější akce jako odesílání, přijímání plateb a přehled historie transakcí. V levém dolním rohu je zobrazena celková částka, kterou uživatel disponuje na všech jím spravovaných adresách. Výhodou může být možnost nastavení poplatku za provedení transakce, čímž může uživatel sám určit její prioritu. Velmi pohodlnou funkcí je také možnost zakódovat svoji adresu do QR kódu, který lze posléze vytisknout nebo uložit do chytrého telefonu a vyhnout se tak ručnímu zadávání v obchodech.



Obrázek 10: Electrum-základní obrazovka (zdroj: vlastní)

4.1.3 PLNOHODNOTNÝ SOFTWARE

Pokud se uživatel chce stát plnohodnotným uzlem sítě, musí využívat plnohodnotnou peněženku, která pracuje s kompletním záznamem blockchainu. V tu chvíli se uživatel může aktivně podílet na provozu sítě tím, že bude sám sbírat nové transakce a potvrzovat je. Významným zástupcem je oficiální aplikace Bitcoin Core vyvíjená organizací spravující Bitcoin. I zde se vývojáři snaží uživateli nabídnout co největší pohodlí. Uživatelské rozhraní obsahuje detailní vysvětlivky v mnoha jazycích a uživatel tak má vždy přehled o prováděných akcích. Při prvním spuštění programu je nabídnuto stažení aktuálního blockchainu, který je pro další funkčnost nezbytný. (viz Obrázek 11).



Obrázek 11: Instalace Bitcoin Core – stahování blockchainu (zdroj: vlastní)

Ačkoli je uživatelské prostředí velmi podobné jako u odlehčených peněženek, stát se plnohodnotným uzlem v síti neboli těžařem už vyžaduje více znalostí. Uživatel si musí zvolit hardware, na kterém bude těžbu provádět, případně kontaktovat jeden z těžebních poolů. Těžba v poolech je v mnoha případech výrazně výhodnější. Více o této problematice je uvedeno v kapitolách Těžba jednotek a Hardware.

4.2 HARDWARE

Nároky na hardware jsou velice individuální a závisí na záměrech uživatele a také na konkrétní volbě kryptoměny. Tato kapitola se bude zabývat běžným hardwarem, který využijí pokročilí uživatelé. V kapitole Kryptoměny bylo uvedeno, že těžba měny Bitcoin v současnosti klade vysoké nároky na speciální hardware, zatímco jiné měny, jako například Litecoin, se tento problém snaží vyřešit implementací jiných hashovacích algoritmů.

4.2.1 PEVNÝ DISK

Při použití odlehčeného klienta jsou nároky na uložiště nízké (v řádech desítek megabajtů). Na disk jsou ukládána pouze data, potřebná ke zjištění zůstatku na adresách vztažených ke konkrétnímu veřejnému klíči. Naopak v případě plnohodnotného klienta se nároky na diskový prostor pohybují v řádech desítek gigabajtů. Jak už bylo zmíněno dříve, těžký klient vyžaduje pro svoji funkci stažení kompletního blockchainu. Například v síti Bitcoin je jeho velikost po necelých deseti letech provozu 165 GB. Stahování je tedy také náročné na internetové připojení a tato operace může v závislosti na vytížení sítě trvat i několik dní. Následné udržování aktuální verze blockchainu již není náročné, ale je nutné počítat s jeho vytrvalou expanzí.

4.2.2 PROCESORY (CPU)

V začátcích byla těžba kryptoměn realizována na běžných osobních počítačích prostřednictvím jejich procesorů. Hashovací algoritmus SHA256 se nacházel ve většině realizací kryptoměn a procesory dokázaly hledat řešení s výkonem 0.2 až 140 MHash/s v závislosti na hardware, který uživatel vlastnil. Jednotka MHash/s udává počet provedených výpočtů hashe v milionech za sekundu. S rostoucí výpočetní silou sítě začali uživatelé hledat výkonnější alternativu, prostřednictvím které by získali výhodu nad ostatními.

4.2.3 GRAFICKÉ KARTY (GPU)

Ke slovu se dostaly herní grafické karty, které disponují velkou kapacitou operační paměti a větším množstvím ALU. Pokročilejší grafické karty obsahují i tisíce těchto jednotek, přičemž každá z nich je schopna provádět výpočty. Výraznou paralelizací úlohy se podařilo navýšit výkon až na 1GHash/s a současně snížit pořizovací náklady a energetickou náročnost. (BitcoinWiki, 2015)

V současnosti se především díky algoritmům náročným na operační paměť, použitým v některých typech kryptoměn, vrací těžba na osobní počítače a výrobci grafických karet přicházejí s modely určenými speciálně pro těžbu. Tyto modely nedisponují výstupními porty ani elektronikou s nimi spojenou, což umožňuje nepatrně snížit výrobní náklady a provozní spotřebu. Naopak karty disponují větší kapacitou paměti a chlazením dimenzovaným pro zatížení dlouhodobějšího charakteru. Jedním ze zástupců je například grafická karta Asus Mining P106 (viz Obrázek 12). Podstatnou nevýhodou takto

Obrázek 12: Absence video výstupů (Zdroj: (ASUS, 2017))

upravených grafických karet je jejich zúžená možnost využití právě z důvodu absence výstupních portů. Velká část těžařů grafické karty po několika měsících používání prodávala. Díky tomu měli možnost získat většinu investovaných prostředků zpět ještě před morálním zastaráním karty a významnou ztrátou její hodnoty. Tyto speciální grafické karty nás přivádějí ke kategorii speciálního hardwaru.

4.3 SPECIÁLNÍ HARDWARE

Za speciální hardware je považován takový hardware, který je navržen pro jedinou funkci a v dané konfiguraci ho obvykle není možné využít pro jiné aplikace. Existují zařízení určená pro zvýšení bezpečnosti při manipulaci s kryptoměnami a zařízení s vysokým výpočetním výkonem určená k těžbě.

4.3.1 TREZOR – HARDWAROVÁ PENĚŽENKA

Peněženky, které byly dosud představeny, byly všechny softwarové. V roce 2014 uvedl jeden z nejvýznamnějších českých bitcoin vývojářů, Marek Palatinus, hardwarovou peněženku nazývanou Trezor. I přes relativně vysokou cenu (89 euro) se tento český vynález těší velké popularitě po celém světě. Jedná se o počítač velikosti flashdisku, který disponuje micro USB konektorem a malým displejem. Jeho úkolem je ověřovat transakce zadané v počítači a výrazně snižovat riziko odcizení přístupových hesel metodou Keyloggingu[18]. S počítačem se spojuje prostřednictvím USB rozhraní (viz Obrázek 13).

Obrázek 13: Trezor (zdroj: (Trezor, 2017))

S pořízením Trezoru získává uživatel přístup k online peněžence MyTrezor, kde může spravovat své adresy. Zde uživatel zadává nové transakce, k jejichž potvrzení využije Trezor. Postup potvrzení je velice podobný tomu ze softwarové peněženky. Uživatel zadá adresu a obnos, který si přeje odeslat a klikne na tlačítko send. Trezor připojený k počítači obdrží tuto transakci a vyzve uživatele k zadání pinu. Na displeji Trezoru (viz Obrázek 14) se zobrazí devítimístný číselník s náhodně umístěnými čísly, přičemž na obrazovce počítače je zobrazena silueta číselníku bez čísel. Uživatel zadá svůj PIN kód v závislosti na

[18] **Keylogger** je obvykle software spadající do kategorie spyware. Bez vědomí uživatele zaznamenává stisknuté klávesy včetně hesel zadaných prostřednictvím klávesnice a odesílá je útočníkovi. Existuje i hardwarová varianta.

rozmístění čísel zobrazeném na displeji. V tomto způsobu zadání hesla spočívá největší výhoda Trezoru, neboť keylogging je považován za jednu z nejsnazších cest k získání přístupových údajů. Po zadání pinu stačí transakci potvrdit stisknutím tlačítka na Trezoru, který následně v šifrované podobě odešle do počítače soukromý klíč potřebný k podepsání transakce.

Obrázek 14: Zadání PIN kódu (Zdroj: (Do, 2017))

4.3.2 PROGRAMOVATELNÁ HRADLOVÁ POLE (FPGA)

Možnost paralelizace výpočtů je v oblasti hashovacích funkcí obecně považována za výhodu. V případě kryptoměn je to ovšem nepříjemná vlastnost, která běžné uživatele postavila do velmi nevýhodné situace. Dalším krokem se po grafických kartách stala programovatelná hradlová pole. Ta je prostřednictvím jazyků HDL (VHDL, Verilog) možné programovat pro konkrétní výpočty. Hradlová pole jsou jednoduchá zařízení, disponující zpravidla sériovým portem, popř. USB a dalšími sběrnicemi. Jejich výhodou oproti grafickým kartám je jednoduchost návrhu, díky které tak vynikají ve výpočetní efektivitě. Výkonový nárůst byl v tomto případě přibližně desetinásobný. V porovnání s grafickými kartami také ovšem klesla spotřeba elektrické energie. (Stroukal, 2015, s. 68) Konkrétní příklad zařízení FPGA je zobrazen na následující stránce (viz Obrázek 15).

Obrázek 15: Hradlové pole Xilinx Spartan 3A (zdroj: (Numato, 2017))

4.3.3 SPECIÁLNÍ INTEGROVANÉ OBVODY (ASIC)

Posledním vývojovým článkem v oblasti těžby kryptoměn jsou speciální integrované obvody. Ty jsou od návrhu určeny ke konkrétnímu výpočtu a jejich funkce je na rozdíl od FPGA neměnná. Výpočetní výkon se pohybuje od 1GHash/s do 14THash/s. Nicméně návrh zařízení je finančně velice náročný a jeho cena se pohybuje v řádech tisíců dolarů. (BitcoinWiki, 2017) Tato zařízení jsou určena především pro společenství neboli pooly, do kterých se těžaři spojují. Vznikají tak výpočetní centra o výkonu stovek Phash/s. Na obrázku níže je zobrazeno zařízení Antminer S9 disponující výkonem 14THash/s.

Obrázek 16: Antminer s9 (zdroj: (Antminer, 2017))

4.4 ZÁSADY BEZPEČNÉ MANIPULACE S KRYPTOMĚNAMI

Následující text má povahu všeobecného přehledu, který poukazuje na základní potenciální problémy vznikající při manipulaci s kryptoměnami. Autor navíc uvádí několik doporučení pramenících z praktických zkušeností získaných používáním kryptoměn.

Stejně tak, jako u běžného internetového bankovnictví, i při manipulaci s kryptoměnami je nutné dodržovat základní bezpečnostní pokyny, aby byla minimalizována možnost neoprávněného přístupu k účtu. Základní pokyny, jako jsou zásady při výběru silného

hesla a jeho následného přechovávání, jsou stejné. Existují ale i aspekty, ve kterých se kryptoměny odlišují.

Mnohé zdroje uvádějí, že v případě kryptoměn je vhodné uložit si své heslo (soukromý klíč) do papírové podoby, protože je to bezpečnější způsob, než ho přechovávat v elektronické podobě v zašifrovaném souboru. Nespornou výhodou je, že zabráníme jeho ztrátě selháním počítače nebo nechtěným smazáním souboru. S rostoucí popularitou kryptoměn, ale také roste šance, že případný zloděj bude umět nalezený klíč vytisknutý na papír využít. I přesto je začátečníkům doporučeno si svůj soukromý klíč vytisknout a bezpečně uložit na média s nevolatilním typem paměti, trvale odpojená od počítače.

Pravdou ovšem zůstává, že zapomenuté heslo je jedním z největších slabin decentralizovaného systému kryptoměn, neboť neexistuje žádná autorita, která by rozhodovala o resetování nebo vydání nového hesla. Nehledě na to, že vydání nového hesla ke stávající adrese by vlastně znamenalo nalezení kolize šifrovací funkce a selhání její bezpečnosti. Takto ztracené heslo znamená nenávratné ztracení přístupu a tím i všech jednotek na dané veřejné adrese.

Neposledním problémem je situace, kdy majitel účtu zemře. V podobných situacích je momentálně nutné se preventivně obrátit na notáře a celou situaci vyřešit s ním. Ten by v případě úmrtí vydal oprávněné osobě přístupové údaje. V opačném případě, není možné používat nebo vypátrat účet zemřelého uživatele.

Kryptoměny jsou také často spojovány s nelegálním obchodováním s drogami či přístupy k tzv. Botnetům[19]. Především kvůli tržištím vznikajícím na anonymní síti zvané Tor[20], kde zpravidla není možné platit penězi nebo kreditní kartou. Mnoho států se snaží obchod s kryptoměnami regulovat také z důvodu možnosti financování terorismu a praní špinavých peněz. Česká legislativa se zatím problematikou kryptoměn příliš nezabývá, to ovšem neznamená, že uživatelé nemusejí dodržovat žádná pravidla. Podle §9 ze zákona 253/2008 Sb. jsou banky povinny zjišťovat původ příchozích peněz. Transakce spojené s kryptoměnami při překročení částky 15 tisíc euro nahlašují Finančnímu analytickému útvaru Ministerstva financí jako podezřelé. Od roku 2013 je také nutné při směně peněz

[19] **Botnet** je skupina počítačů napadená škodlivým softwarem, jehož prostřednictvím jsou útočníci schopni počítače zneužívat k DoS útokům a další trestné činnosti bez vědomí majitele.
[20] **Tor** je nejznámější anonymizační síť. Přístup do sítě je umožněn prostřednictvím speciálního prohlížeče.

na kryptoměny dokládat svoji totožnost. (Vejvodová, 2017) S tím souvisí pojem Bitcoin laundry, což je služba, která uživatelům umožňuje anonymizovat jejich platby, tím že provádí další posloupnost převodů a téměř znemožňuje vypátrat majitele účtu. Tento postup není protizákonný, ale má charakter velice podezřelého chovaní.

5 DOTAZNÍKOVÉ ŠETŘENÍ

Praktickou součástí této práce je návrh a evaluace dotazníkového šetření, které má za cíl zjistit, zda současná podoba kryptoměn motivuje k jejich využití širší veřejnost. V úvodním odstavci jsou stručně shrnuty pohnutky, které vedly k uvedeným předpokladům při tvorbě dotazníku. V následujících kapitolách jsou předloženy další položky, které jsou nedílnou součástí dotazníku.

5.1 ÚVOD

V posledním desetiletí prodělala společnost významnou proměnu, během které se velká část klientů různých finančních institutů naučila spravovat své účty vzdáleně. Průzkumy uvádějí, že zatím co v roce 2009 82 % klientů upřednostňovalo správu účtu na pobočce, dnes již nadpoloviční většina svůj účet raději spravuje prostřednictvím internetového bankovnictví. (Eurostat, 2018) S příchodem chytrých telefonů se internetové bankovnictví prostřednictvím aplikací rozšířilo i na mobilní telefony a správa účtu se tak maximálně zjednodušila. Zdá se tedy, že významná část populace je ochotna ukládat své peněžní prostředky v institucích, se kterými již zpravidla není fyzicky v kontaktu. Na výběr je z nezměrného množství služeb. Od dlouhodobě existujících bank (Komerční banka, Česká spořitelna) přes moderní banky (Airbank, Mbank), které upřednostňují méně formální přístup ke klientovi, až po komerční služby jako jsou například Paypal. Všechny zmíněné služby jsou v současnosti velice rozšířeny. Měli by však lidé zájem o službu, která je spravována samotnou veřejností? Službu, ve které mají své finance v rukou pouze klienti samotní? Právě takové možnosti nabízejí kryptoměny.

Po technologické stránce jsou kryptoměny připraveny k masovému využití veřejností. V současnosti již není problém vytvořit takovou realizaci kryptoměny, která je schopna potvrzovat mikrotransakce instantně a převody vyšších částek během několika minut. Komplikaci by mohly způsobit poplatky za transakce. V současnosti je sice věnováno velké úsilí jejich minimalizaci, ale úplné odstranění je prozatím nejspíše nemožné. Z bezpečnostního hlediska vynikají kryptoměny vysokou mírou zabezpečení již několik let.

Pojem široká veřejnost zastupuje množinu lidí, kteří mohou, ale nemusí disponovat znalostmi technologie kryptoměn a v jejich zájmu je pouze využívat tuto službu jako nástroj pro správu svých finančních prostředků. Níže navržený dotazník by měl zjistit, zda

kryptoměny mají veřejnosti co nabídnout a zda jsou tyto výhody pro veřejnost motivující. Významné jsou pro mě informace o spokojenosti klientů bank s jejich službami a schopnosti klientů využívat v této oblasti moderní technologie.

5.2 CÍL

Cílem dotazníkového šetření je ověřit předložené důvody, které by veřejnost vedly ke změně jejích platebních návyků ve prospěch kryptoměn, s přihlédnutím na její schopnost využívat aktuální způsoby platebního styku.

5.3 VÝZKUMNÉ OTÁZKY A HYPOTÉZY

O_1: Umožňuje způsob používání bankovních služeb veřejností využívat kryptoměny?

O_2: Je veřejnost spokojena s bankovními službami spojenými s převody peněz?

O_3: Motivují předložené výhody kryptoměn veřejnost k jejich využívání?

H_{O1_0}: Respondenti nezávisle na věku využívají internetové bankovnictví stejně.

H_{O2_0}: Respondenti nezávisle na věku jsou s trváním převodu stejně spokojeni.

5.4 METODY SBĚRU DAT A DOTAZNÍKOVÉ SLUŽBY

Nejvýznamnějšími metodami sběru dat jsou pozorování, analýza dat a dotazování. Vzhledem k povaze problému, jsem zvolil metodu dotazování s kvantitativním přístupem k výzkumu. Výhodou této metody je rychlé a pohodlné získání velkého množství dat. Naopak nevýhodou je nízká míra návratnosti dotazníku a také omezený rozsah informace o respondentech. (Majerová, 2008)

Mezi nejvýznamnější platformy pro tvorbu a realizaci nejrůznějších dotazníkových šetření patří například služby Survio nebo Google forms. K tvorbě a distribuci vytvořeného dotazníku jsem využil služby Google forms. Tato služba umožňuje dotazník přehledně členit do jednotlivých částí s oddělenými názvy. Další výhodou jsou základní grafické výstupy ze získaných dat přímo v aplikaci s možností pokročilých úprav v tabulkovém procesoru.

5.5 VZOREK RESPONDENTŮ A JEHO VELIKOST

Výběr vzorku respondentů není komplikovaný, neboť aktivních uživatelů internetového bankovnictví je v České republice v současnosti velké množství. Údaje zveřejněné statistickým úřadem Evropské unie uvádí 57 %, což je v Evropě nadprůměr (Eurostat,

2018). Kryptoměny prošly za posledních několik let významným vývojem, který výrazně usnadnil jejich používání. Schopnost využívat internetové bankovnictví je z hlediska náročnosti tedy téměř totožná se schopností používat kryptoměny. To považuji za základní předpoklad. Otázky v dotazníku budou formulovány s přihlédnutím na to, že respondenti problematiku kryptoměn nemusí znát, popřípadě nejsou schopni vyhodnocovat výhody a nevýhody této technologie.

Co se týká velikosti vzorku respondentů, ten není zásadně omezen a záleží jen na možnostech autora respondenty oslovit. Vzhledem k použití online dotazníku s předpokládanou návratností 30 %, bude nutné pro dosažení statisticky důvěryhodných dat oslovit co největší počet potenciálních respondentů.

5.6 TVORBA DOTAZNÍKU

Při tvorbě otázek byly dodrženy zásady pro tvorbu dotazníku, které ve své publikaci uvádí Chráska (2007, s.169-171). Otázky byly pokládány tak, aby nebyly příliš složité a pro respondenta bylo jednoduché na ně bez dlouhého přemýšlení odpovědět. Velmi důležité bylo formulovat otázky jednoznačně, aby respondenti odpovídali vždy na správnou věc. Co se týká kompozice, snazší otázky (motivační) byly umístěny na začátek a složitější až doprostřed dotazníku. Otázky osobního charakteru jsou pokládány na konci dotazníku. Jejich počet byl minimalizován, aby respondenti nenabyli dojmu, že dotazník naruší jejich soukromí.

Po předchozí rozvaze nebyl respondentům předem sdělen fakt, že se dotazník primárně zabývá kryptoměnami. V poslední době se kryptoměny dostávají do popředí prostřednictvím masmédií, které o nich informují. S těmito informacemi ovšem velmi často přicházejí také negativní zprávy o spojení kryptoměn s daňovými úniky a praním špinavých pěněz. Velmi často jsou také prezentovány jako významný prostředek financování terorismu a jiných forem protizákonného chování. Není vhodné, aby výsledky dotazníku byly ovlivněny těmito problémy. Proto byly otázky zprvu zaměřeny pouze na vlastnosti kryptoměn.

Při tvorbě dotazníku byly otázky rozděleny do několika skupin. Do první skupiny spadají otázky zjišťující, jak velká část veřejnosti využívá internetové bankovnictví, neboť pro manipulaci s kryptoměnami je schopnost využívat tento přístup zatím zcela

bezpodmínečná. Významné také bude, zda se klienti obejdou bez kamenné pobočky nebo je pro ně naopak fyzický kontakt s bankou důležitý. Získaná data z této skupiny otázek tedy pomohou zjistit, zda je veřejnost bez ohledu na ostatní aspekty schopna kryptoměny využívat.

Druhá skupina otázek má za cíl poukázat na nedostatky, které bankovní služby doprovázejí. Velký tlak je v současnosti vyvíjen především na jejich rychlost a cenu. Některé finanční instituce dnes nabízejí vedení účtu zdarma, jiné chtějí zaujmout bezplatnými peněžními převody do zahraniční banky. Bankovní služby zaznamenaly významný pokrok. Zatímco před několika lety byly výhody služeb, jako jsou Paypal nezpochybnitelné, dnes již podobnou ergonomií disponují i bankovní služby. Pro konkurenci je tedy mnohem složitější zaujmout. Přesto existují nedostatky jako velmi drahé mezinárodní platby a celkově dlouhá doba vyřízení bankovních převodů. Kryptoměny mohou nabídnout bezplatné vedení účtu a velmi rychlé převody peněz bez komplikací s platbami do zahraničí. Vyhodnocením dat z druhé části bych rád zjistil, který z uvedených nedostatků považuje veřejnost za nejvýznamnější.

Další část otázek zjišťuje, jestli by uvedené výhody přiměly veřejnost k využívání alternativních platebních služeb a jak velká část veřejnosti zná pojem kryptoměny. Nachází se zde také několik otázek, které jsou určeny pro případné respondenty orientující se v problematice kryptoměn. Tyto otázky by mohly přinést zajímavé statistiky motivující k hlubšímu průzkumu mezi aktivními uživateli kryptoměn.

V poslední části se nacházejí otázky osobního charakteru. Statisticky významným údajem je věk respondentů. Pomůže zjistit, zda jsou požadavky veřejnosti stejné nebo mají různé věkové skupiny odlišné požadavky.

5.7 VYHODNOCENÍ ZÍSKANÝCH DAT

Tato kapitola bude věnována analýze získaných dat a následnému vyhodnocení výzkumných otázek a hypotéz. Podstatná data budou graficky znázorněna přímo u řešení jednotlivých otázek a hypotéz. Ostatní získané údaje budou zobrazeny v grafech umístěných mezi přílohami. Jako nástroje vyhodnocení výzkumných otázek byly použity otázky z dotazníkového šetření. Konkrétní otázky jsou vždy uvedeny při analýze výsledků. Pro zodpovězení výzkumných otázek bude použita popisná statistika. Poslouží následující

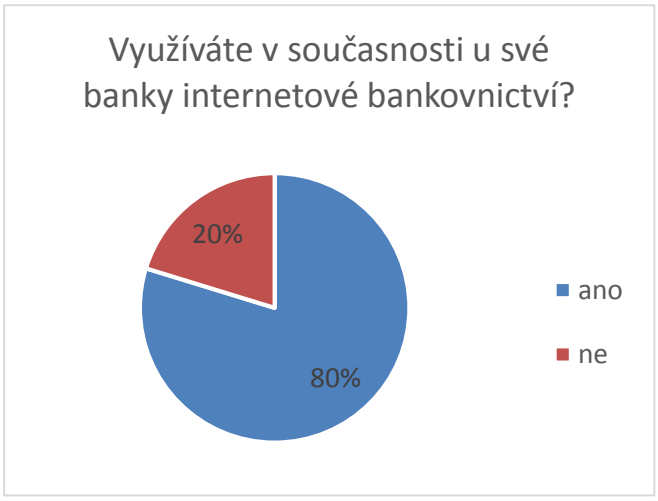
kritérium. Otázka bude vyhodnocena kladně v případě, že 70 % a více získaných dat bude hovořit ve prospěch takové odpovědi. Pro potvrzení nebo vyvrácení stanovených hypotéz budou použity statistické testy.

5.7.1 SKUTEČNÁ NÁVRATNOST DOTAZNÍKU

V průběhu měsíce března bylo osloveno přibližně 500 potenciálních respondentů. Zpět se vrátilo celkem 158 vyplněných dotazníků. Výsledná návratnost tedy je okolo 31 %. Tento údaj souhlasí s dříve předpokládanou 30 % návratností dotazníku.

5.7.2 VÝSLEDKY

Pro vyhodnocení první výzkumné otázky byla použita data získaná z otázek 3 a 4. První významnou informací bylo zjištění, jak velká část respondentů používá internetové bankovnictví. Data byla přenesena do grafu (viz Graf 1).



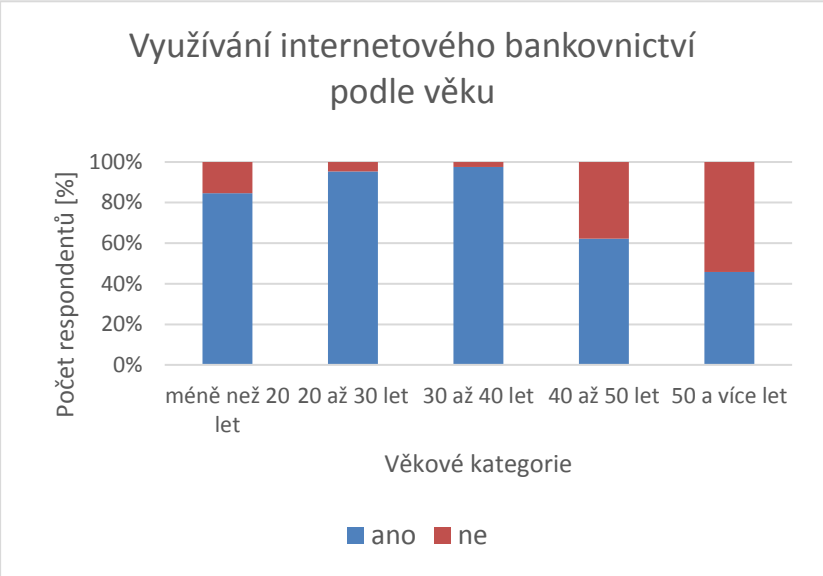
Graf 1: Využívání internetového bankovnictví (zdroj: vlastní)

Z grafu vyplývá, že významná většina respondentů internetové bankovnictví využívá. Hodnota 80 % dokonce předčila dříve uvedený údaj poskytnutý ústavem Eurostat. Z podrobnějšího zkoumání ovšem vyplývá, že tento údaj se liší mezi jednotlivými věkovými kategoriemi (viz Graf 2 na následující stránce). Je patrné, že lidé do věku 40 let využívají internetové bankovnictví téměř všichni. V kategoriích nad 40 let již nezanedbatelná část respondentů tuto službu nevyužívá, přičemž v kategorii nad 50 let je to každý druhý.

Vzájemná závislost jevů (věk respondentů a využívání bankovnictví) byla potvrzena statistickým testem dobré shody *chí-kvadrát*, který uvádí Chráska (2007, s. 76). Po dosazení do rovnice: $\chi^2 = \frac{(\mathrm{P}-\mathrm{O})^2}{O}$ pro všechny kombinace polí získáváme hodnotu $\chi^2 = 38{,}9$. Při testování na hladině významnosti $\alpha = 0.05$ porovnáváme s tabulkovou hodnotou 9,488. Jelikož je námi zjištěná hodnota významně vyšší, odmítáme nulovou hypotézu H_{O1_0} a přijímáme alternativní hypotézu:

H_{O1_A} *Využívání internetového bankovnictví závisí na věku respondentů.*

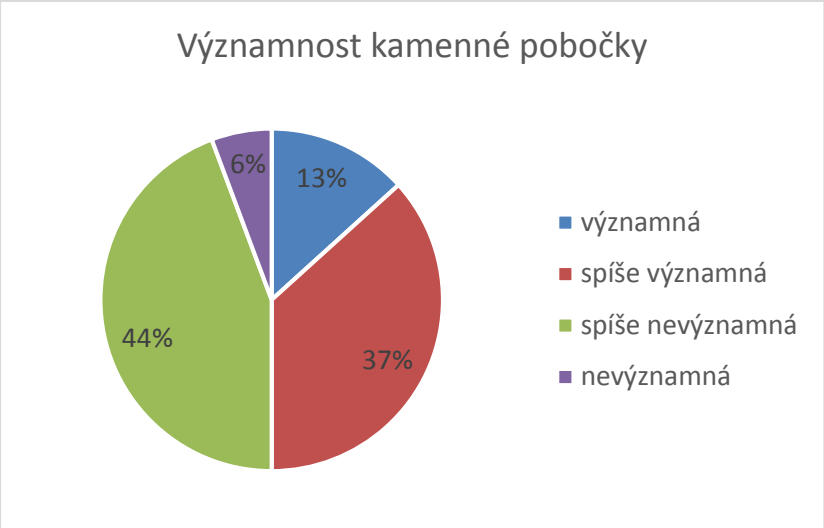
Graf využívání internetového bankovnictví podle věku respondentů je přiložen níže.



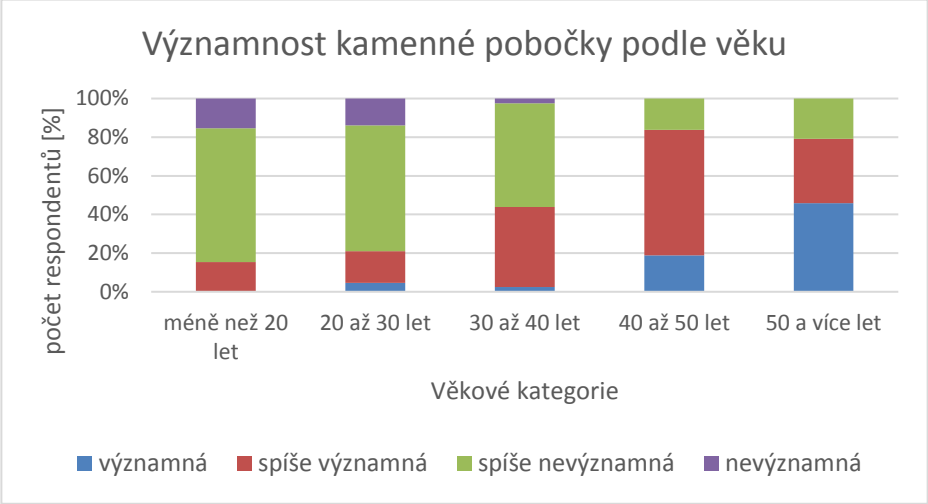
Graf 2:Četnost využívání internetového bankovnícství podle věku (zdroj: vlastní)

Další podstatnou informací je míra významnosti kamenné pobočky z pohledu respondentů (viz Graf 4 na následující stránce). Respondenti, kteří preferují přímý kontakt s bankou, v současné době podobnou službu v oblasti kryptoměn nenaleznou.

Ohledně rozhodování o existenci kamenné pobočky byli respondenti opatrní. Přesně polovina uvedla, že by se bez ní obešla, naopak druhá polovina nikoliv. Pro získání lepšího pohledu na problém je předložen graf, na kterém jsou respondenti rozděleni podle věku (viz Graf 4 na následující stránce). Z grafu je názorně vidět trend, který popisuje závislost významnosti pobočky na věku respondentů. Opět se ukazuje, že klienti nad 40 let se významně odlišují od nižších věkových kategorií a kamennou pobočku by ve většině případů postrádali.



Graf 3: Významnost kamenné pobočky (zdroj: vlastní)

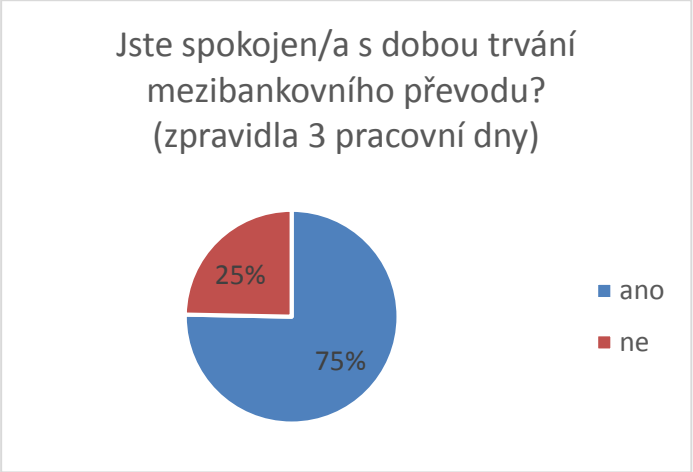


Graf 4: Významnost kamenné pobočky podle věku (zdroj: vlastní)

Zbývající grafy věnující se této skupině dat se nacházejí v příloze. Na otázku, jestli způsob využívání bankovních služeb veřejností umožňuje využívat kryptoměny můžeme odpovědět ano, částečně. U respondentů ve věku nad čtyřicet let existují překážky, které by jim využívání kryptoměn komplikovaly. Především z důvodu absence kamenných poboček, kde by bylo možné spravovat účet.

Na druhou výzkumnou otázku se v dotazníku zaměřují otázky č. 7 a 9. Pozornost byla věnována rychlosti a ceně bankovních převodů.

Co se týká rychlosti bankovního převodu, respondenti jsou v tomto ohledu tolerantní. Garance tří pracovních dní nadpoloviční většině vyhovuje. Výjimkou jsou opět respondenti ve věku nad 40 let, kteří jsou velmi spokojeni (viz Graf 6).



Graf 5: Spokojenost s trváním převodu (zdroj: vlastní)

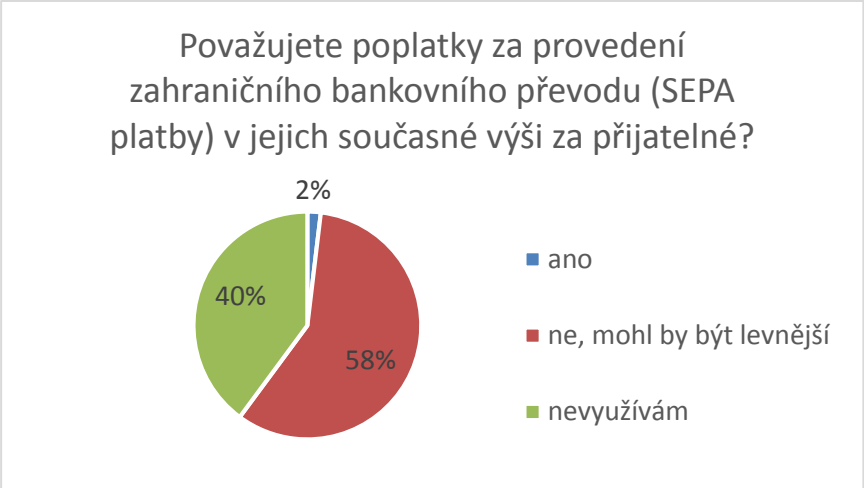
Provedený test dobré shody na hladině významnosti $\alpha = 0.05$ prokázal, že ve vztahu věku respondentů a jejich spokojenosti s dobou trvání převodu existuje závislost. Odmítáme tedy nulovou hypotézu H_{O2_0} a přijímáme alternativní hypotézu:

H_{O2_A}: *Spokojenost s trváním bankovního převodu závisí na věku respondentů.*

Provedené výpočty se nacházejí v přiloženém souboru Srail_survey.xlsx

Graf 6: Spokojenost s trváním převodu podle věku (zdroj: vlastní)

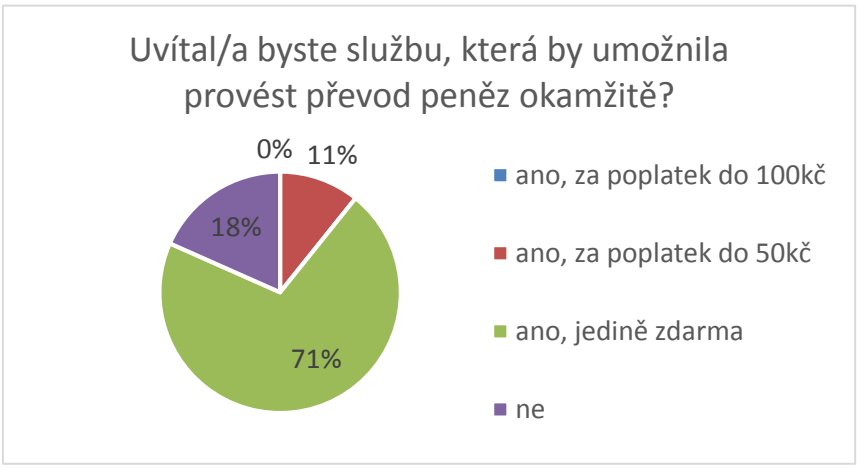
Respondenti se shodli v otázce cen zahraničních převodů. Drtivá většina z těch, kteří jej využívají, považují převod do zahraniční banky za předražený (viz Graf 7).



Graf 7: Názor na poplatky za zahraniční převody (zdroj: vlastní)

Z výsledků vyplývá, že pro většinu respondentů je prioritou cena služeb. Tuto domněnku podporuje i průzkum, který provedla poradenská společnost Ernst&Young. Z něj vyplývá, že 69 % Čechů změnilo svoji banku z důvodu vysokých poplatků. Evropský průměr činí 53 %. (Ernst&Young, 2012, s. 44). Na otázku, zda jsou klienti spokojeni s bankovními službami spojenými s převody peněz lze odpovědět tak, že klienti částečně nejsou spokojeni. Především s cenou zahraničních plateb.

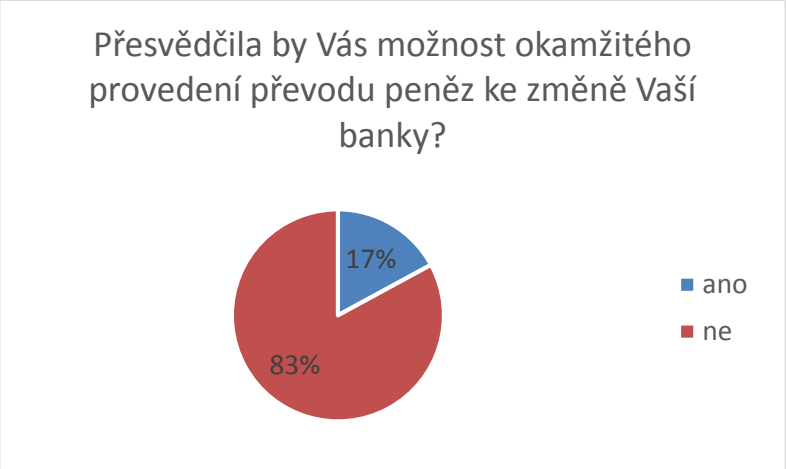
Třetí výzkumné otázce se v dotazníku věnovaly otázky č. 8, 10 a 11. Získaná data se nacházejí v grafech níže. Vzhledem k velmi jednoznačným výsledkům, byla k vyhodnocení použita pouze popisná statistika.



Graf 8: Zájem o instantní bankovní převod (zdroj: vlastní)

Přestože čtvrtina respondentů by uvítala rychlejší provedení bankovního převodu, pouze desetina z nich by za takovou službu byla ochotna zaplatit poplatek do 50 Kč. Téměř pětina uživatelů by takovou službu neuvítala (viz Graf 8 na předchozí stránce).

Provádění transakcí okamžitě nebo v rámci několika minut je silnou stránkou kryptoměn. To navíc platí bez rozdílu bank nebo států, což zjednodušuje především platby do zahraničí. Respondenty tato možnost ovšem příliš nezaujala. Pro možnost využívat takovou služby by bylo ochotno změnit poskytovatele služeb pouhých 17 % dotázaných (viz Graf 9).



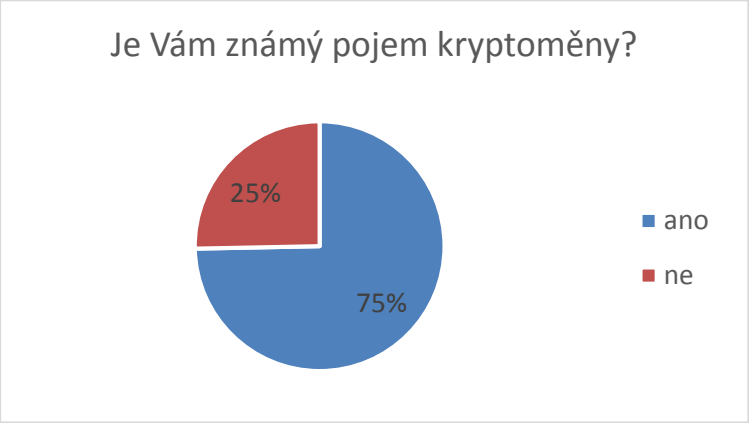
Graf 9: Možnost okamžitého převodu (zdroj: vlastní)

Společně s daty získanými z otázky číslo 11 (viz Graf 10) tyto výsledky opět ukazují, že veřejnost se orientuje především na cenu služeb. Podstatná většina respondentů uvedla, že možnost vedení účtu zdarma by je přesvědčila ke změně jejich banky.

Graf 10: Možnost vedení účtu zdarma (zdroj: vlastní)

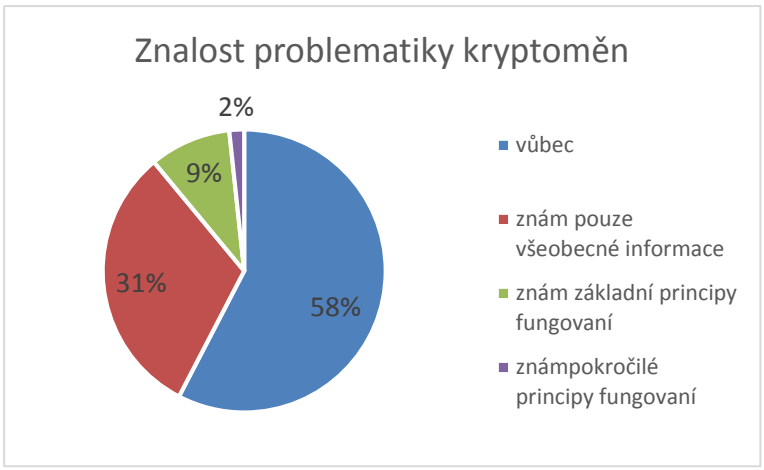
S přihlédnutím k faktům, že v současné době se na trhu nachází několik společností nabízejících vedení účtu zdarma a také to, že kryptoměny v současnosti nenabízejí zcela bezplatné transakce, neexistují žádné výhody, které by kryptoměny mohly širší veřejnosti nabídnout.

Následující získané informace, které mohou přiblížit pohled na situaci kryptoměn a případně motivovat k dalšímu průzkumu jsou předloženy v grafech uvedených níže. Jedná se o zjištění popularity pojmu kryptoměny, způsobu, jakým se o něm respondenti dozvěděli a míra jejich znalostí problematiky kryptoměn. V posledním případě se jedná jen o subjektivní názor respondentů.



Graf 11: Popularita kryptoměn (zdroj: vlastní)

Graf 12: Polularita kryptoměn podle věku (zdroj: vlastní)



Graf 13: Znalost problematiky kryptoměn (zdroj: vlastní)

Graf 14: Způsob seznámení s kryptoměnami (zdroj: vlastní)

ZÁVĚR

Kryptoměny v roce 2017 zaznamenaly významné zvýšení popularity, které přitáhlo pozornost širší veřejnosti. Koncem roku tento trend dosáhl svého dosavadního vrcholu. Nové účty si zakládaly miliony uživatelů a téma kryptoměn se objevilo v mnoha informačních médiích. Tento zájem přinesl dobré, ale i špatné zprávy. Zatímco po technologické stránce kryptoměny obstály, po té ekonomické je jejich budoucnost stále velmi nejistá. Volatilita, kterou způsobuje fluktuace uživatelů, přitahuje pozornost takzvaných spekulantů. Ti nemají zájem kryptoměny využívat k placení, ale pouze jako prostředek riskantní investice s vidinou velkých výdělků. Další nedůvěru podle mého názoru vzbuzuje také fakt, že se jedná o novou technologii, se kterou uživatelé nemají žádné zkušenosti.

Cílem této práce bylo uvést čtenáře do problematiky kryptoměn. Především představit strukturu a principy funkce. Významnou komplikací byl nízký počet důvěryhodných publikací, které byly navíc až na jednu výjimku cizojazyčné. Technická angličtina pro mě nebyla velkou překážkou. Problematika kryptoměn je velice rozsáhlá a bylo náročné téma zpracovat přehledně a současně neopomenout žádné důležité aspekty. Mimo všechny technické pojmy byla také stručně popsána historie, mé vlastní postřehy a možnosti manipulace s kryptoměnami, jejichž popis považuji za velmi důležitý. V závěru bylo provedeno dotazníkové šetření, zaměřené na spokojenost veřejnosti s bankovními službami a možnostmi využití alternativních služeb.

Výsledky šetření měly získat odpovědi na stanovený cíl. Konkrétní získaná data potvrdila nejistotu, která v oblasti kryptoměn momentálně panuje. Přestože je veřejnost ve využívání současných platebních způsobů zběhlá, tato nová technologie prozatím nenabídla žádné zásadní výhody, které by motivovaly k využívání kryptoměn. Bankovní služby prodělaly v posledních letech vývoj, který je v porovnání s kryptoměnami činí velmi konkurenceschopné. Z výsledků výzkumných otázek vyplynulo, že podstatným faktorem při výběru služeb je pro veřejnost jejich cena. Tu se některým poskytovatelům bankovních služeb podařilo stlačit na absolutní minimum. Respondenti do věku 40 let jsou schopni kryptoměny využívat, ovšem jen malá část z nich by ocenila předložené výhody.

Podle výsledků šetření 75 % veřejnosti zná pojem kryptoměny. Tento údaj se shoduje s údajem, který byl v roce 2018 zjištěn magazínem Studenta. V roce 2016 byl údaj 47 % (Studenta, 2018, s. 19). Zatímco tedy popularita kryptoměn roste, zájem o jejich využívání nikoliv. Podle mého názoru bude v budoucnosti podstatné, jak se k rychlému rozvoji kryptoměn postaví stát a jestli možné regulace kryptoměny zcela neochromí.

Vývoj kryptoměn stále pokračuje, ale i kdyby se časem ukázaly jako nevhodná technologie pro platební styky, díky vynálezu blockchainu přinesla revoluční pohled na důvěryhodné zpracovávání a ukládání dat bez zásahu centrální autority. Tento decentralizovaný přístup umožňuje vedení nejrůznějších registrů a záznamů, které by neměly podléhat zájmům jednotlivců.

Veškerá data získaná z dotazníkového šetření jsou dostupná v přiloženém souboru Srail_survey.xlsx, který se nachází na CD vloženém v zadní části pevné vazby. Na CD se také nachází vypracovaná práce ve formátech PDF a DOCX.

RESUMÉ

Nine years ago a blank new section of cryptography developed. Unknown author launched first cryptocurrency – worldwide payment system, which is completely decentralized throught the peer to peer network.

The aim of this thesis is to introduce this technology of cryptocurrencies to unexperienced ones. To show them it's development from beginning of the year 2009 until present and bring back the most important events. Split this entire system to a parts and describe them in order to reveal it's simplicity and efficiency. Last but not least, to show to the potencial users the best way how to store and use their coins and present them risks, that are related to the use of digital currency.

Last part of this thesis is a survey, which is targeted at anyone, who actively uses bank services. It's purpose is to confirm previously established benefits of cryptocurrencies and show if there are any reasons to use them for the general public.

SEZNAM LITERATURY

Antminer. *Antminer* [online]. Breda: Antminer Distribution Europe B.V., 2017 [cit. 2017-11-12]. Dostupné z: https://www.antminerdistribution.com/antminer-s9/

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

Bitcoin Price History Chart. *Buy Bitcoin Worldwide* [online]. Buy Bitcoin Worldwide, 2018 [cit. 2018-04-07]. Dostupné z: www.buybitcoinworldwide.com/price/

BOSE, Antoon. The hash function RIPEMD-160. *Home pages of ESAT*[online]. Leuven: Katholieke Universiteit te Leuven, 2012 [cit. 2018-01-20]. Dostupné z: https://homes.esat.kuleuven.be/~bosselae/ripemd160.html

Mining-P106-6G. *Asus* [online]. Taipei: ASUSTeK Computer, 2012 [cit. 2018-01-20]. Dostupné z: https://www.asus.com/Graphics-Cards/MINING-P106-6G/

ČNB. Obchodování s bitcoiny. *Stanoviska a odpovědi* [online]. Praha: ČNB, 2014 [cit. 2017-10-26]. Dostupné z: https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/stanoviska_a_odpovedi/pdf/obchodovani_s_bitcoiny.pdf

BASHIR, Imran. *Mastering Blockchain*. Birmingham: Packt Publishing, 2017. ISBN 978-1-78712-544-5.

Mining hardware comparison. *BitcoinWiki* [online]. Bitcoin community, 2018 [cit. 2017-11-19]. Dostupné z: https://en.bitcoin.it/wiki/Mining_hardware_comparison

Non-specialized hardware comparison. *BitcoinWiki* [online]. Bitcoin community, 2018 [cit. 2018-04-06]. Dostupné z: https://en.bitcoin.it/wiki/Non-specialized_hardware_comparison#Intel

CHAUM, David. *Advances in Cryptology: Proceedings of Crypto 82*. New York: Plenum press, 1983. ISBN 978-1-4757-0604-8.

CHRÁSKA, Miroslav. *Metody pedagogického výzkumu: základy kvantitativního výzkumu*. Praha: Grada, 2007. Pedagogika (Grada). ISBN 978-80-247-1369-4.

What is the Difference Between Litecoin and Bitcoin?. *Coindesk* [online]. New York: Coindesk, 2014 [cit. 2017-11-25]. Dostupné z: https://www.coindesk.com/information/comparing-litecoin-bitcoin/

Definition of cryptocurrency. *English Oxford living dictionaries* [online]. Oxford: Oxford University Press, 2014 [cit. 2017-12-10]. Dostupné z: https://en.oxforddictionaries.com/definition/cryptocurrency

DO, Tuan. TREZOR Bitcoin Hardware Wallet Review: A Bitcoin Safe for Hodlers. *Techwalls* [online]. Los Angeles: Techwalls, 2017 [cit. 2018-01-07]. Dostupné z: https://www.techwalls.com/trezor-bitcoin-hardware-wallet-review/

LIOUDIS, Nickolas. What is the gold standard?. *Investopidea* [online]. New York: Investopedia, 2018 [cit. 2018-03-01]. Dostupné z: https://www.investopedia.com/ask/answers/09/gold-standard.asp

GRIFFITH, Ken. A Quick History of Cryptocurrencies BBTC — Before Bitcoin. *Bitcoin Magazine* [online]. Fayetteville: BTC Media, 2014 [cit. 2017-04-06]. Dostupné z: https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/

HERTIG, Alyssa. Who Created Ethereum?. *Coindesk* [online]. New York: Coindesk, 2014 [cit. 2017-12-23]. Dostupné z: https://www.coindesk.com/information/who-created-ethereum/

HIGGINS, Stan. Mt Gox Trustee Sells $400 Million in Bitcoin and Bitcoin Cash. *Coindesk* [online]. New York: Coindesk, 2018 [cit. 2018-03-08]. Dostupné z: www.coindesk.com/mt-gox-trustee-sells-400-million-bitcoin-bitcoin-cash/

HRABÁKOVÁ, Jitka. Chceme komunikovat zabezpečeně - šifrování. *Otevřená Fakulta informačních technologií ČVUT* [online]. Praha: ČVUT, 2012 [cit. 2017-10-11]. Dostupné z: www.otevreno.fit.cvut.cz/sifrovani/

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.

KEIRNS, Garret. Japan's Bitcoin Law Goes Into Effect Tomorrow. *Coindesk*[online]. New York, 2017 [cit. 2017-11-29]. Dostupné z: https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow/

KLÍMA, Vlastimil. Kryptografie eliptických křivek. *CHIP : magazín informačních technologií.* Praha: Vogel Publishing. 2002. č. 10, str. 160-162. ISSN 1210-0684.

MAJEROVÁ, Věra. *Sociologie venkova a zemědělství*. Vyd. 4., přeprac. Praha: Credit, 2000. ISBN isbn978-80-213-0651-6.

MENEZES, A. J., Paul C. VAN OORSCHOT a Scott A. VANSTONE. *Handbook of applied cryptography*. Boca Raton: CRC Press, c1997. ISBN 978-0-84-938523-0.

NARAYANAN, Arvind. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, 2016. ISBN 978-0-691-17169-2.

FIPS General Information. *NIST* [online]. Gaithersburg: NIST, 2018 [cit. 2018-02-14]. Dostupné z: https://www.nist.gov/itl/fips-general-information

Elbert V2 – Spartan 3A FPGA Development Board. *Numato Lab* [online]. Colorado Springs: Numato systems, 2017 [cit. 2018-03-21]. Dostupné z: https://numato.com/product/elbert-v2-spartan-3a-fpga-development-board

OSTERMAN, Cynthia. MtGox insolvent long before collapse - FT.com. *Reuters* [online]. Londýn: Reuters, 2015 [cit. 2018-04-06]. Dostupné z: https://uk.reuters.com/article/uk-bitcoin-trading-mtgox/mtgox-insolvent-long-before-collapse-ft-com-idUKKBN0NB01120150420

PAGLIERY, Jose. *Bitcoin and the future of money*. Chicago, Illinois: Triumph Books, 2014. ISBN 978-1-62937-036-1.

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.

TASSEV, Lubomir. Roles of Regulators Decided in India, Rules on Bitcoin Coming Soon. *Bitcoin News* [online]. Saint Bitts, 2018 [cit. 2018-03-22]. Dostupné z: https://news.bitcoin.com/roles-of-regulators-decided-in-india-rules-on-bitcoin-coming-soon/

TOMAN, Kamil. Kryptografické hashovací funkce. *Karlínský Lab* [online]. Praha: Matematicko-fyzikální katedra, 2017 [cit. 2017-12-29]. Dostupné z: http://artax.karlin.mff.cuni.cz/~toman/crypto/img9.html

TORPEY, Kyle. Bitcoin's Highly-Anticipated Lightning Network Goes Live As Startup Raises $2.5 Million. *Forbes* [online]. New York: Forbes Media, 2018 [cit. 2018-3-28]. Dostupné z: https://www.forbes.com/sites/ktorpey/2018/03/15/bitcoins-highly-anticipated-lightning-network-goes-live-as-startup-raises-2-5-million/#7c3df3cf7eb0

TREZOR. Bitcoin wallet: The original & most secure hardware wallet. *Trezor*[online]. Praha: SatoshiLabs, 2018 [cit. 2018-02-17]. Dostupné z: www.trezor.io

VEJVODOVÁ, Alžběta. Česko zavádí první zákon, který omezuje anonymitu bitcoinu. Brzy přijdou další. *Právní rádce* [online]. Praha: Economia, 2017 [cit. 2017-10-27]. Dostupné z: http://pravniradce.ihned.cz/c1-65598690-cesko-zavadi-prvni-zakon-ktery-omezuje-anonymitu-bitcoinu-brzy-prijdou-dalsi

DIFFIE, Whitfield a Martin HELLMAN. *Multiuser cryptographic techniques*. National conference and exposition. New York, 7. června 1976. New York: ACM, 1976. s. 109-112. DOI: 10.1145/1499799.1499815.

EUROSTAT. Individuals - internet activities. *Eurostat* [online]. Lucemburk: Eurostat, 2018 [cit. 2018-04-01]. Dostupné z: http://appsso.eurostat.ec.europa.eu/nui/show.do?query=BOOKMARK_DS-053730_QID_4CBC0374_UID_-3F171EB0&layout=TIME,C,X,0;GEO,L,Y,0;INDIC_IS,L,Z,0;UNIT,L,Z,1;IND_TYPE,L,Z,2;INDICATORS,C,Z,3;&zSelection=DS-053730INDICATORS,OBS_FLAG;DS-053730UNIT,PC_IND;DS-053730INDIC_IS,I_IUBK;DS-053730IND_TYPE,IND_TOTAL;&rankName1=UNIT_1_2_-1_2&rankName2=INDICATORS_1_2_-1_2&rankName3=INDIC-IS_1_2_-1_2&rankName4=IND-TYPE_1_2_0_1&rankName5=TIME_1_0_0_0&rankName6=GEO_1_2_0_1&sortC=ASC_-1_FIRST&rStp=&cStp=&rDCh=&cDCh=&rDM=true&cDM=true&footnes=false&empty=false&wai=false&time_mode=ROLLING&time_most_recent=true&lang=EN&cfo=%23%23%23%2C%23%23%23.%23%23%23

ERNST&YOUNG. The customer takes control: Global Consumer Banking Survey 2012. In: *EY: Building a better* [online]. EYGM, 2012 [cit. 2018-03-06]. Dostupné z:

http://www.ey.com/Publication/vwLUAssets/ey-global-consumer-banking-survey-2012/$FILE/ey-global-consumer-banking-survey-2012.pdf

SAMŠUKOVÁ, Eva. Blockchain. *Studenta*. Praha: Economia, 2018, 2018(2), 18-20.

SEZNAM OBRÁZKŮ, TABULEK, GRAFŮ A DIAGRAMŮ

PŘÍLOHY

DOTAZNÍK

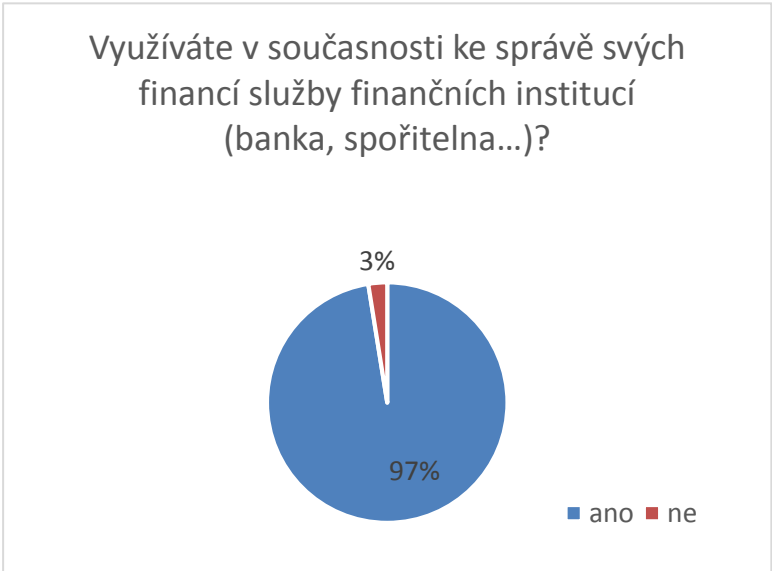
Tento anonymní dotazník se zabývá zájmem veřejnosti o rozvíjející se platební služby, které mohou být alternativou k těm běžným bankovním. V závislosti na Vašich odpovědích Vám bude položeno 1 až 19 otázek, jejichž vyplnění netrvá déle než 3 minuty. Získaná data pomohou nalézt důvody motivující klienty bank k využívání jiných platebních služeb.

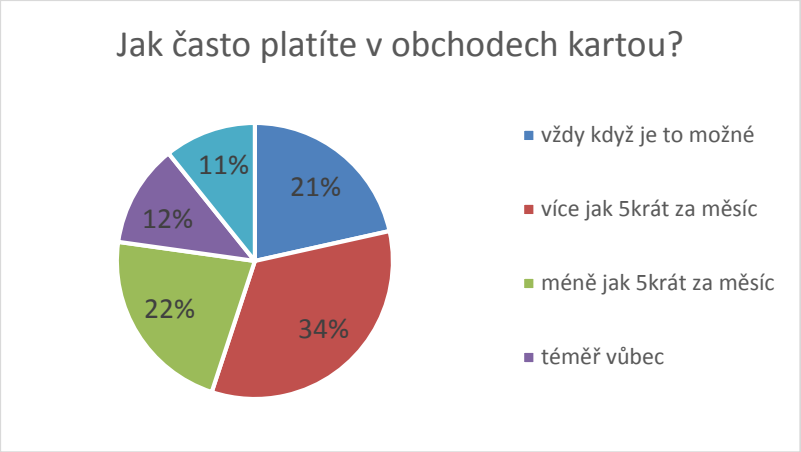
Alternativní finanční služby		
1	Využíváte v současnosti ke správě svých financí služby finančních institucí (banka, spořitelna…)?	
		ano
		ne
2	Jakou část ze svých finančních prostředků máte uloženou v bance/bankách?	
		téměř všechny
		více jak polovinu
		méně jak polovinu
		žádné
3	Využíváte v současnosti u své banky internetové bankovnictví?	
		ano
		ne
4	Nakolik je pro Vás významná existence kamenné pobočky Vaší banky?	
		významná
		spíše významná
		spíše nevýznamná
		nevýznamná
5	Jak často platíte v obchodech kartou?	
		vždy když je to možné
		více jak pětkrát za měsíc
		méně jak pětkrát za měsíc
		téměř vůbec
		ještě jsem kartou neplatil

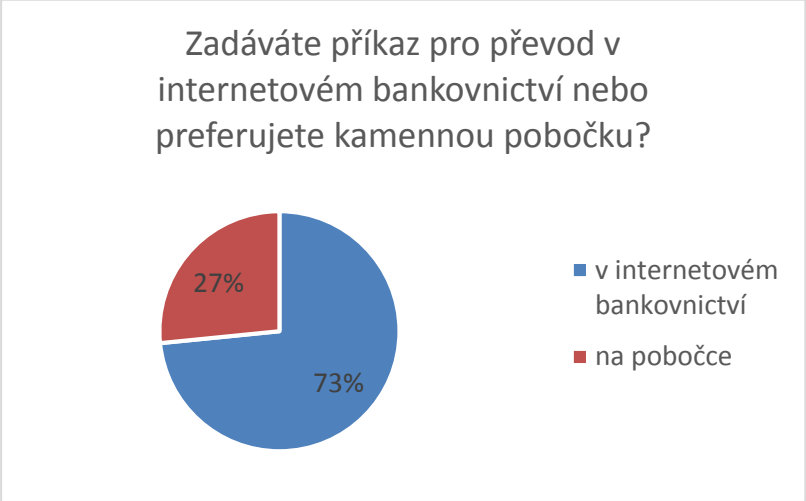
6	Zadáváte příkaz pro převod v internetovém bankovnictví nebo preferujete kamennou pobočku?	
		v internetovém bankovnictví
		na pobočce
7	Jste spokojen/a s dobou trvání mezibankovního převodu? (zpravidla 3 pracovní dny)	
		ano
		ne
8	Uvítal/a byste službu, která by umožnila provést převod peněz okamžitě?	
		ano, za poplatek 100kč
		ano, za poplatek 50kč
		ano, jedině zdarma
		ne
9	Považujete poplatky za provedení zahraničního bankovního převodu (SEPA platby) v jejich současné výši za přijatelné?	
		ano
		ne
10	Přesvědčila by Vás možnost okamžitého provedení převodu peněz ke změně Vaší banky?	
		ano
		ne
11	Přesvědčila by Vás možnost vedení účtu zcela bez poplatků ke změně Vaší banky?	
		ano
		ne
12	Důvěřoval/a byste možnosti uchovávat peníze v elektronické podobě i bez účasti banky?	
		ano
		ne
13	Je Vám známý pojem kryptoměny?	
		ano
		ne
14	Jak Jste se o existenci kryptoměn dozvěděli?	
		od známých nebo kamarádů
		v zaměstnání
		z massmédií (TV, rádio, tisk)
		jinak
15	Do jaké míry se vyznáte v problematice kryptoměn?	
		vůbec
		znám pouze všeobecné informace
		znám základní principy fungování
		znám pokročilé principy fungování

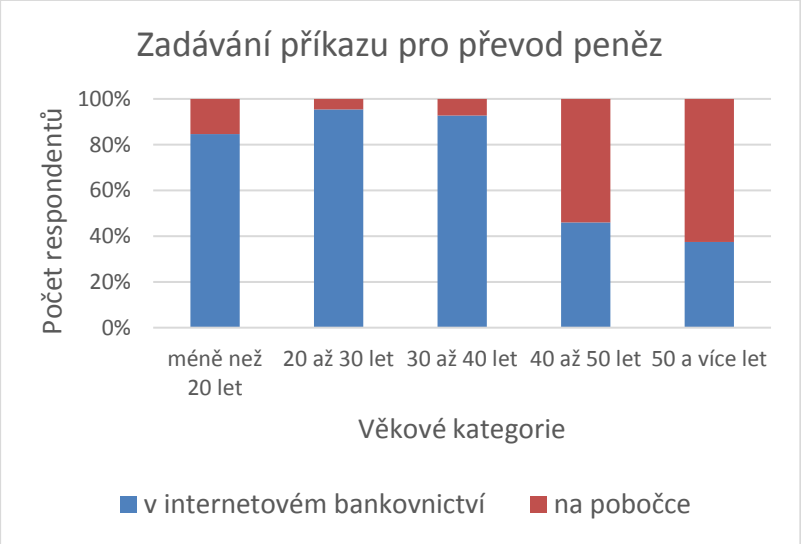
16	Využíváte v současnosti kryptoměny?	
		ano
		ne
17	Myslíte si, že by se technologie blockchainu mohla v budoucnosti uplatnit i v jiných oblastech, než jsou kryptoměny?	
		ano
		ne
		nevím co je to blockchain
18	Která kryptoměna by podle Vás byla vhodná pro využití širokou veřejností jako alternativa bankovních služeb?	
19	Vyberte Váš věk.	
		méně než 20 let
		20 až 30 let
		30 až 40 let
		40 až 50 let
		50 a více let

OSTATNÍ GRAFY




Jak často platíte v obchodech kartou?
11%
21%
12%
22%
34%
vždy když je to možné
více jak 5krát za měsíc
méně jak 5krát za měsíc
téměř vůbec


Zadáváte příkaz pro převod v internetovém bankovnictví nebo preferujete kamennou pobočku?
27%
73%
v internetovém bankovnictví
na pobočce


Zadávání příkazu pro převod peněz
Počet respondentů
100%
80%
60%
40%
20%
0%
méně než 20 let
20 až 30 let
30 až 40 let
40 až 50 let
50 a více let
Věkové kategorie
v internetovém bankovnictví
na pobočce