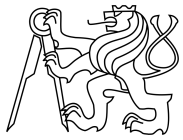
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



ZADÁNÍ DIPLOMOVÉ PRÁCE

Název:	Studie proveditelnosti nasazení technologie blockchainu v bankovnictví
Student:	Bc. Michal Rendla
Vedoucí:	Ing. Mgr. Pavla Vozárová, Ph.D., M.A.
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce zimního semestru 2017/18

Pokyny pro vypracování

Formou rešerše se seznamte s technologií blockchainu v kontextu potvrzování bitcoinových transakcí. Analyzujte, do jaké míry v současné době tradiční komerční banky implementují technologie související s digitálními měnami ve svých systémech. Vysvětlete, jakým způsobem by technologie blockchainu mohla sloužit při potvrzování transakcí v běžných měnách a sestavte studii proveditelnosti nasazení takové technologie. Diskutujte technické, ekonomické i legislativní stránky dané problematiky. Součástí studie by měl být i zjednodušený proof-of-concept.

Seznam odborné literatury

Dodá vedoucí práce.

L.S.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
děkan

V Praze dne 28. února 2016

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra softwarového inženýrství

Diplomová práce

Studie proveditelnosti nasazení technologie blockchain v bankovnictví

Bc. Michal Rendla

Vedoucí práce: Ing. Mgr. Pavla Vozárová, Ph.D., M.A.

11. ledna 2017

Poděkování

Chci poděkovat vedoucí této diplomové práce paní Pavle Vozárové za její cenné rady a vstřícné jednání. Dále bych rád poděkoval rodině, která mě při studiu podporovala.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 11. ledna 2017 .....

Odkaz na tuto práci

Rendla, Michal. *Studie proveditelnosti nasazení technologie blockchain v bankovnictví.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2017.

Abstrakt

V této diplomové práci se zabývám využitím technologie blockchainu pro banky a ostatní tradiční finanční instituce. Blockchain je hlavním technologickým prvkem dnešních veřejných decentralizovaných kryptoměn. V roce 2016 existuje již velké množství decentralizovaných kryptoměn, ovšem první a exemplární decentralizovanou kryptoměnou pořad zůstává Bitcoin. Banky si všimli těchto decentralizovaných kryptoměn a chtějí je využit pro své vlastní potřeby. Moje studie proveditelnosti se zabývá realizovatelnosti nasazení a využitelností decentralizovaných kryptoměn v bankách z technologického, ekonomického a legislativního hlediska.

Klíčová slova Blockchain, distributed ledger, Bitcoin, kryptoměny, transakce

Abstract

In this diploma thesis, I deal with the usage of technology blockchain for banks and other traditional financial institutions. Blockchain is a major technological element of today's decentralized cryptocurrency. In 2016, there are already a large number of public decentralized cryptocurrency, but first and exemplary decentralized cryptocurrency stays Bitcoin. Banks have noticed these decentralized cryptocurrency and want them used for its own needs. My feasibility study deals with the feasibility and usability of decentralized cryptocurrency for banks from technological, economic and legal point of view.

Keywords Blockchain, distributed ledger, Bitcoin, kryptoměny, transactions

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Výběr tématu a motivace

Magisterské studium a hledání diplomového téma

V rámci oboru „Webové a softwarové inženýrství se zaměřením na Informační systémy a management“ jsem hledal vhodné téma, kterému bych se chtěl věnovat. Rozhodl jsem se pro vlastní téma diplomové práce, jelikož se dlouhodobě zajímám o decentralizované kryptoměny již z dob bakalářského studia. Zaměřil jsem se na aplikaci kryptoměn v nynějším tradičním bankovnictví z hlediska převodu finančních prostředků, respektive finančních transakcí. Budu vycházet především z nynější nejznámější decentralizované kryptoměny, jejíž je Bitcoin. Je to první decentralizovaná kryptoměna svého druhů. Dnes již existuje spousta zrealizovaných decentralizovaných kryptoměn, stále ovšem jsou technologický v jádru pořad stejné. Proto vznikl akronym pro všechny ostatní decentralizované kryptoměny - altcoins[1], nebo-li „alternativní kryptoměny“.

Proč zrovna aplikace kryptoměn v bankovnictví?

Poprvé jsem se setkal s tématem digitálních měn v rámci návštěv informatických večerů organizovaných fakultou Informačních technologií ČVUT v Praze[2], kde probíhají přednášky a workshopy z různých oblastí informatiky. Navštívil jsem na podzim roku 2013 přednášku s názvem „Bitcoin - digitální měna budoucnosti nebo nafouklá bublina“, které mě oslovilo. Do tohoto informatického večera jsem o této formě měn nikdy neslyšel. O tuto alternativní formu peněz jsem se dále zajímal. V té době Bitcoin si získal velký ohlas ve světě, ale bohužel nedostal se ke komerčnímu využití v tradičním bankovnictví a stále tomu tak je. Na vině jsou různé faktory, jakožto možnost nepotvrzení transakce, nedůvěra společnosti, neakceptovatelnost finančními institucemi,

[1] Alternate cryptocurrencies

[2] http://fit.cvut.cz/fakulta/pravidelne-akce/informaticke-vecery

ale hlavně nemožnost regulace. Tyto všechny aspekty budou názorně pozorovatelné v kapitole 2. Problémem rovněž je, že Bitcoin není uvnitř jednoduchý system a neexistuje žádná centrální autorita, která by se za něj zaručila a spravovala. Člověk, který tedy nemá znalosti o Bitcoinu by měl mít přirozený strach nad ztrátou svých finančních prostředku. Většina společností má stále větší důvěru u tradičních bank. Zkratka důvodu je více. Tyto fakta budou rozebraná dále postupně v práci.
Banky a finanční instituce si všimli decentralizovaných kryptoměn a momentálně hledají způsoby využiti této technologie pro své účely. Jeden z těchto způsobu využiti jsou převody finančních prostředku mezi jednolitými bankami a ostatními finančními institucemi.

Cíl práce

V této studii proveditelnosti zkoumám realizovatelnost nasazeni blockchain technologie pro tradiční finanční instituce jako jsou příkladem banky z technického, ekonomického, legislativního hlediska.

Struktura diplomové práce

První kapitoly se zabývají obecně kryptoměnami a funkcionalitou Bitcoinu, který je hlavní exemplární decentralizovanou kryptoměnou. Blockchain je téma, které je postavené na Bitcoinu. V dalších kapitole se zabývám blochainem z technického hlediska a aplikacemi. V poslední kapitole se zabývám specifikou blockchainu pro bankovnictví.

Použité zdroje a literatura

Kryptoměna Bitcoin byla vytvořena v roce 2009. Bitcoin není spravován žádnou centrální autoritou, například komerční společnosti a podobně viz. dále v DP o centrální autoritě. Nejdříve vznikaly články v angličtině a podobně, pořádali se různé po světě přednášky o Bitcoinu. Vznikali rovněž webové portály věnující se Bitcoinu. Později začali vznikat první knížky a to především v angličtině. V podstatě Bitcoin je spravován velkou komunitou nadšenců po celém světě, kteří rovněž přispívají decentralizovaně k provozu Bitcoinu jak technický, tak literaturou.

Od roku 2013 jsme si přečetl poměrně hodně různých článku, shlédl video tutoriály, přečetl několik knížek, navštívil různé akce spojené s kryptoměnami. Z mého pohledu problémem v literatuře je, že Bitcoin ze své podstaty není žádným autorským dilem pod jednou známou autoritou, nikdo ho nevlastní. Vznikají v některých případech více terminu pro jeden tentýž pojem. Zkratka uvedu příklad: Dva jedinci vymysleli termín pro jeden a tentýž pojem. Část komunity potom používá první termín, zatímco další část se chytla jiného a

tak dále. Není zde žádný vlastník, kdo by určoval, který se má použit. Literatura je tvořena komunitou a proto i taková wikipedia byla rovněž normálním „kvalitním“ zdrojem. Časem se objevili spolky, neziskové organizace, které se snaží spravovat tyto záležitosti na pravou míru. Ovšem je na každé zainteresované osobě, zda chce tyto standarty chce dodržovat.

V této práci jsem vycházel především z oficiální webové stránky měny Bitcoin: <http://www.bitcoin.org> a dokumentace na <http://www.en.bitcoin.it>. Tyto dva zdroje zaručují nejvíce skutečně odpovídající informace o Bitcoinu, neboť se o ně stará vývojářský tým a komunita organizované kolem této měny. Další literaturu jsem se snažil pečlivě vybírat z různých anglickojazyčných zdrojů.

Na internetu lze nalézt české webové stránky věnující se Bitcoinu nebo ostatním kryptoměnám, avšak tyto české zdroje obsahují informace, které jsou primárně určené pro potenciálního zájemce, který chce používat tyto měny, aniž by je podrobněji řešil. Poměrně velké množství informací o Bitcoinu lze nalézt v novinových článcích, a to jak v anglické, tak poměrně často i v české přeložené verzi, které obsahují občas nepravdivé informace.

Ohledně literatury na téma blockchain. Čerpal jsem především z různých analýz, zprav, reportu, které byli tvořené komerčními a nekomerčními institucemi, odborníky, spolky. Knihy kolem blockchainů ještě nejsou bohužel na místě aktuální. Veškeré zdroje kolem blockchainů, které jsem používal, byli především z let 2015 až 2016. Je to téma velmi aktuální a živé. Jelikož ho paralelně řeší řada nezávisle na sobě subjektu, tak literatura tomu rovněž odpovídá. V tomto směru je trochu chaotický stav.

Banky nejsou tolik sdíleni do detailu. Z pochopitelných důvodu nechtějí sdělovat podrobnější detaily řešeni. Avšak jsem se snažil dostat se ke všem možným zdrojům. Navštívil jsem v červnu 2016 technologickou pobočku britské banky Barclays v Praze, kde rovněž jedno oddělení zkoumá blockchain. Opět jsem se převážně dozvěděl o Bitcoinu, než o podrobnějších detailech aplikace této technologie v bankovnictví. Čerpal jsem o blockchainu hodně informací z reportu společností jako je Deloitte, Pwc, Accenture a podobně. Rovněž z různých technických analýz bank jako jsou UniCredit Bank, Credit Suisse a další. Bylo těžké se shodnout na výkladu, protože hodně těchto společností provádí výzkum blockchain technologií nezávislé na sobě. Tvoří různou terminologií a tak dále.

Obrázek 0.1: Paralelní polis - logo spolku[2]

Česká komunita kolem kryptoměn

Jako centrum české komunity kolem kryptoměn bych mohl označit spolek Paralelní polis.

„Projekt Paralelní Polis v sobě spojuje umění, společenské vědy a moderní technologie. Je postaven na idejích svobody, nezávislosti a inovativního rozvoje společnosti. Jedním z hlavních konceptů je důsledná snaha zůstat „state free“. Paralelní Polis funguje zcela bez účasti státu. Zároveň nečerpá žádné prostředky z veřejných financí, tedy z peněz, které získává státní monopol prostřednictvím nedobrovolných vynucovaných plateb – daní.

Paralelní Polis je nezisková organizace s právní formou „spolek“. Struktura Polis staví na členské základně. Členové organizace přispívají k chodu projektu finančně nebo svou vlastní aktivitou. Každý z členů projevuje zájem o hlavní ideje Paralelní Polis a snaží se je šířit. Těmi jsou nové technologie, decentralizace a kryptoanarchie. Kryptoanarchii chápeme jako potenciální rozumnou variantu společenského zřízení. Svou činností se snažíme přispívat ke kritické diskuzi o souvisejících problémech současnosti.“[2]
Jedna se tedy o spolek a projekt věnující se nejen kryptoměnam, ale jiným tématům. Fakticky bych, ale mohl sdělit, že se věnuje především kryptoměnam. Navštívil jsem toto místo víckrát kvůli různým přednáškám kolem kryptoměn. Naposledy na „Bitcoin meetup - Anonymní kryptoměna Zcash“ nebo-li přednášce o nové kryptoměně zCash.
Předtím do roku 2014 probíhali srazy české komunity kolem kryptoměn v hospodách, kavárnách, kde se dalo zaplatit bitcoiny.

Počeštění anglické terminologie v textu

Většinu použitých zdrojů v této DP najdeme v angličtině. Jelikož jsem se rozhodl napsat tuto DP v českém jazyce, tak spolu s tímto se budu snažit

počeštit anglickou terminologii. Nicméně veškerá terminologie počeštěna nebude. U jednotlivých nových použitých pojmů budu upozorňovat na to, jak je tento pojem zavedený v DP.

Počeštění anglické terminologie na obrázcích

Veškerá terminologie na vlastních obrázcích bude použita v souladu s terminologií použitou v textu DP. Pro obrázky, které budou převzaty z anglických zdrojů, bude jejich terminologie ponechaná v angličtině.

Exaktnost použiti pojmů

Budu se snažit o co nejexaktnější použiti pojmu v tomto tématu. Některé pojmy ovšem nejsou přesně definované a dají se navzájem zaměňovat. Například viz. hned další kapitola 1.1. Budu se snažit dodržovat vhodnost použiti v pořadí navzájem si substitučních pojmu v daném kontextu.

Bitcoin díky tomu, že již vzniknul v roce 2009, tak exaktnost v terminologií se u něj ustálila. Horší případ jsou blockchain technologie, které jsou zkoumaný pro aplikaci do různých oboru různými nezávislými subjekty. Vzniká spousta nových pojmu, výkladu a tak dále. Je poměrně těžké zkompilovat shodu.

Kapitola 1

Kryptoměny obecně

1.1 Používaná terminologie měn

Po dobu psaní diplomové práce(především v kapitole 2) o Bitcoinu jsem se nejčastěji setkával s těmito termíny podle pořadí:

1. digitální měna
2. kryptoměna
3. virtuální měna
4. elektronická měna

Neexistuje zcela přesná rozlišitelnost jednotlivých termínů [19]. Nejčastěji se píše a říká, že Bitcoin je platební síť a v této síti je používána digitální peněžní měna. Tato digitální peněžní měna používá stejný název pro svůj platební systém Bitcoin, avšak píše se s malým písmenem „b“ na začátku slova. Platebním prostředkem Bitcoinu je tedy bitcoin. V této práci budu používat nejčastěji termín kryptoměna a digitální měna. Je nutno brát v potaz, že tyto pojmy jsou navzájem zaměnitelné, viz. dále.

1.2 Kryptoměna

Kryptoměna je typ digitálního platebního prostředku, který používá vysoce zabezpečenou kryptografii s cílem zvýšit bezpečnost tohoto prostředku směny [20]. Z tohoto důvodu lze usuzovat, že pojem kryptoměna je exaktnější výklad pojmů digitální měny. Respektive je to zdůraznění faktu, že digitální měna v tomto tématu používá kryptografii, která hraje klíčovou roli v existenci této digitální měny.

#	název	tržní kapitalizace	jednotková cena	množství v oběhu
1	Bitcoin	$ 12,585,865,433	$ 784.33	16,046,625 BTC
2	Ethereum	$ 680,228,467	$ 7.82	86,980,065 ETH
3	Ripple	$ 240,546,726	$ 0.006720	35,794,578,423 XRP
4	Litecoin	$ 177,400,568	$ 3.63	48,905,304 LTC
5	Monero	$ 115,185,949	$ 8.49	13,559,551 XMR

Tabulka 1.1: Pořadí kryptoměn podle objemu USD. Data jsou převzata z [22]

1.3 Vývoj kryptoměn

První funkční implementace kryptoměn se začala používat v praxi v roce 1990. Jejím autorem byl David Chaum [21]. Měla název DigiCash. Tato kryptoměna měla centralizovanou síť. Byla tedy jiná než dnešní kryptoměny, které jsou decentralizované. V roce 1998 DigiCash ohlásila bankrot[3] a veškerá aktiva této společnosti byla prodána společnosti eCash, která byla konkurentem DigiCash.

První decentralizovanou kryptoměnou je Bitcoin. Tato měna se poprvé objevila v roce 2009. Po úspěchu Bitcoinu se objevily další kryptoměny. U těchto ostatních kryptoměn se uchytil termín altcoins. Je to anglický akronym pro termín alternativní kryptoměny vůči Bitcoinu[4]. Tyto altcoiny vesměs kopírovaly a kopírují jak myšlenku, tak i vlastnosti Bitcoinu, a nesou především různé výhody pro tvůrce těchto měn. Můžou si například sami nějakou jejich část vytěžit před zveřejněním ostatním potenciálním zájemcům. Bitcoin zůstává stále nejdůvěryhodnější, nejpoužívanější a největší decentralizovanou kryptoměnou současnosti.

1.4 Srovnání největších kryptoměn současnosti podle objemu v USD

V současnosti existuje přes 700 známých kryptoměn [22]. Pro tyto kryptoměny neexistující žádné regulace, protože jejích platební sítě jsou decentralizované. Využívají technologie P2P sítí. Funguji velmi podobně jako BitTorrent technologie, která ovšem není plně decentralizovaná.

V Tabulce 1.1 vidíme srovnání prvních pěti největších kryptoměn podle hodnoty v USD. Vyjadřované hodnoty jasně ukazují, že trh kryptoměn z hlediska tržní kapitalizace ovládá pořad s přehledem Bitcoin.

1.4.1 Vlastnosti altcoinu

Ostatní kryptoměny vesměs vychází z Bitcoinu. Bitcoin je otevřený projekt od samého začátku a každý může nahlížet do kódu. Na základě tohoto vznikly

[3] http://cryptome.org/jya/digicrash.htm
[4] Alternate cryptocurrencies - bitcoin alternatives

další decentralizované kryptoměny. Rozdíly spočívají nejvíce v tom, že tyto kryptoměny mají jinak nastavena čísla[5] a používají jiné hashovací funkce či rovněž zabezpečení, validaci. Princip fungování platebního systému ovšem zůstává stejný.

1.5 Hlavní rysy současných kryptoměn

1.5.1 Kryptografie

Kryptoměny používají asymetrickou kryptografii, která je založena na šifrování a dešifrování dvěma různými klíči. V kryptografii můžeme klíč definovat jako informaci, která určuje průběh kryptografického algoritmu. Asymetrické šifrování má dva typy klíčů [23].

- veřejný klíč (public key) - říká se mu tak, protože je veřejně známý a dostupný
- privátní klíč (private key) - tajný klíč, který je znám svému držiteli

Právo použít kryptoměnu jako platební prostředek má pouze ten, kdo vlastní privátní klíč.

1.5.2 Využití P2P síti

P2P sítě, nebo-li peer-to-peer sítě jsou klient-klient decentralizované sítě. Jedná se o sítě, které nepoužívají žádný centrální uzel v síti. V tomto smyslu centrálním uzlem v síti můžeme rozumět server, či podobné zařízení, které propojuje veškeré ostatní uzly mezi sebou.

[5] Maximální počet jednotek, počet transakcí v bloku a podobně

Kapitola 2

Bitcoin a vznik prvního blockchainu

V této kapitole seznamují především s funkčností první a revoluční decentralizované kryptoměny Bitcoin. Z této kryptoměny vycházejí ostatní decentralizované kryptoměny. U všech těchto kryptoměn je hlavním technologickým prvkem blockchain, což je distribuovaná a decentralizovaná databáze transakcí.

Banky, ostatní tradiční finanční instituce a rovněž jiné společností[6] si všimli fenomenu Bitcoin a chtějí ho využít pro své účely. Bitcoinuv blockchain je pro tradiční finanční svět spíše teoretickou pomůckou, protože má některé úskalí, které jsou příliš negativní pro praktické využití u tradičních finančních instituci. Další kapitola o Blockchain technologií rozebírá všechny tyto záležitostí a rovněž proveditelnost nasazení vhodnějšího blockchainu.

2.1 Co je to Bitcoin?

Bitcoin je P2P platební síť elektronické peněžní měny, která zároveň používá stejný název pro svou digitální měnu, které se často říká virtuální měna nebo kryptoměna. Tato síť je plně decentralizovaná, nemá žádnou centrální autoritu jako například administrátora, banku a podobně.

Bitcoin mince je možné použít k úhradě zboží nebo služeb u prodejců, kteří jsou připraveni a ochotni je akceptovat. K dispozici jsou možnosti směny na obyčejné (papírové) měny pomocí burz, směnáren, tržišť bitcoinů a dalších specializovaných možností. Tyto možnosti budou v práci podrobně dále rozebrány.

[6] Mimo finanční sektor

2.2 Názvosloví platebního systému a měny Bitcoin

Kvůli exaktnějšímu pochopení výkladu mé práce je třeba rozlišovat tyto dva pojmy:

- Bitcoin – s velkým písmenem „B“ na začátku, bude nadále označovat celý systém této platební sítě, ve kterém je platebním prostředkem Bitcoin mince.
- bitcoin – s malým písmenem „b“ na začátku a rovněž Bitcoin mince bude označovat digitální měnu, neboli platební prostředek, který je značen zkratkou BTC. Nově některé subjekty používají zkratku XBT, která je nová a zatím méně používaná[7].

2.3 Počátky Bitcoinu

Dne 31.října 2008 byl veřejně publikován dokument takzvaný „Bitcoin: A Peer-to-Peer Electronic Cash System“[8]. Tento dokument popisuje koncept platební sítě zvané Bitcoin. Pod tento dokument se podepsal autor pod pseudonymem Satoshi Nakamoto. V té době se o tento koncept příliš nikdo nezajímal. Postupně Satoshi Nakamoto implementoval prvního klienta pro platební síť Bitcoin. Dne 3.ledna 2009 byl vytvořen první takzvaný „genesis“ blok Bitcoinu [24]. Počínaje tímto dnem platební systém začal běžet.

2.4 Autorství Bitcoinu

Tvůrce Bitcoinu Satoshi Nakamoto je celosvětově hledán novináři. Hodně lidí totiž chce vidět hlavního autora Bitcoinu. Je těžko uvěřitelné, že ho dosud nikdo nenašel. Nějakou dobu po zveřejnění konceptu se totiž nadále podílel na vývoji Bitcoinu. Nicméně počínal si obezřetně, například oficiální webovou stránku založil s využitím speciální anonymní služby [24]. Existuje spousta teorií a spekulací ohledně skutečného autora. Nejvíce se spekuluje, že pod tímto pseudonymem se skrývá osamělý autor nebo skupina počítačových vývojářů původem z Japonska, vzhledem ke jménu a příjmení pseudonymu, které je japonského původu. Jako důvod, proč se autor nechtěl a nechce zveřejnit, se často mezi lidmi uvádí povaha daného projektu. Jsou tu ovšem i zcela jiné teorie, jako třeba projekt vlády USA či jiné země a podobně[9].

V konceptu se autor na začátku vyjadřuje k tomu, proč tento platební systém navrhl. Za cíl autora lze považovat automatizovaný platební systém, ve kterém transakce probíhají anonymně a algoritmicky bez zásahu centrální autority. Rozebereme-li to podrobněji, chtěl navrhnout platební systém, ve

[7] http://www.coindesk.com/bitcoin-gaining-market-based-legitimacy-xbt/
[8] https://bitcoin.org/bitcoin.pdf
[9] https://en.bitcoin.it/wiki/Satoshi_Nakamoto

kterém nebude existovat žádný správce a tento systém nebude nikým regulován. V tomto případě se mu záměr do jisté míry naplnil. Do jaké míry se naplnil lze rozhodnout samostatně v dalších sekcích DP. Satoshi Nakamoto pracoval na Bitcoinu nějakou dobu i po spuštění platební sítě s dobrovolnou vývojářskou komunitou, se kterou si dopisoval anonymně přes mailing list, a to do poloviny roku 2010. Po tomto datu Satoshi Nakamoto postupně přestal komunikovat. Bitcoin nemá žádného centrálního správce, který by se o tuto kryptoměnu staral. Tento problém bude nadále podrobně rozebrán. Nicméně objevila se dobrovolnická komunita, která je tvořena především počítačovými vývojáři. Tito dobrovolníci se nadále starají o dokumentaci Bitcoinu a návrh klientů, kteří se připojují do platební sítě.

Díky vzrůstající popularitě platebního systému vznikla dne 27.prosince 2012 organizace Bitcoin Foundation[10]. Jejím posláním je standardizovat, chránit a podporovat používání kryptoměny Bitcoin ve prospěch lidí na celém světě. Nicméně ani tato organizace nemůže řídit platební systém. Platební system je „řízený“ každým uživatelem Bitcoin sítě.

2.5 (Ne)oficiální terminologie

Bitcoin jako platební systém fakticky nikdo nevlastní. Veškerá nová terminologie vzniká převážně samovolně v komunitě Bitcoinu i jinde. Když se použije slovo „oficiální“, tak se tím myslí, že tento pojem nejpravděpodobněji vznikl nebo pochází z Bitcoin komunity. Bitcoin komunita je především tvořena dobrovolníky a nadšenci, kteří se starají o oficiální stránku Bitcoinu[11], referenci, dokumentaci Bitcoinu[12]. V tomto směru se snaží udělat pořádek Bitcoin Foundation, která se snaží o standardizaci.

2.5.1 Znak a logo Bitcoinu

Bitcoin je značen znakem „B“, které je vertikálně dvakrát přeškrtnuté. Existuje hodně log s tímto znakem v různém provedení. Tato loga nejčastěji můžeme vidět na internetu. Poslední dobou se začínají objevovat i v reálném světě. Ovšem kvůli variabilitě log nadále zůstává hlavním vodítkem rozpoznaní loga Bitcoinu pomocí znaku. Nejčastěji můžeme dnes potkat oficiální oranžové logo 2.1a, které bylo vytvořeno komunitou Bitcoinu stejně jako jeho praktická verze 2.1c.

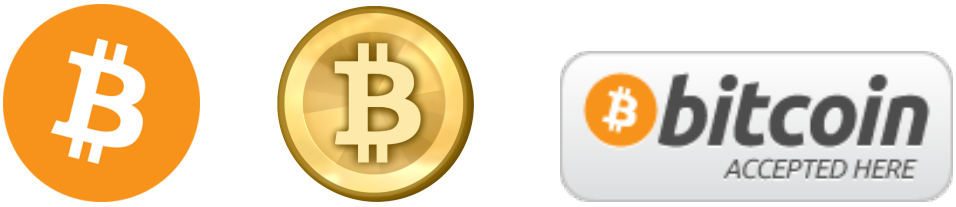
2.6 Všeobecný úvod do funkčnosti Bitcoinu

Systém fungující sítě Bitcoinu lze popsat pomocí Obrázku 2.2.

[10] https://bitcoinfoundation.org/

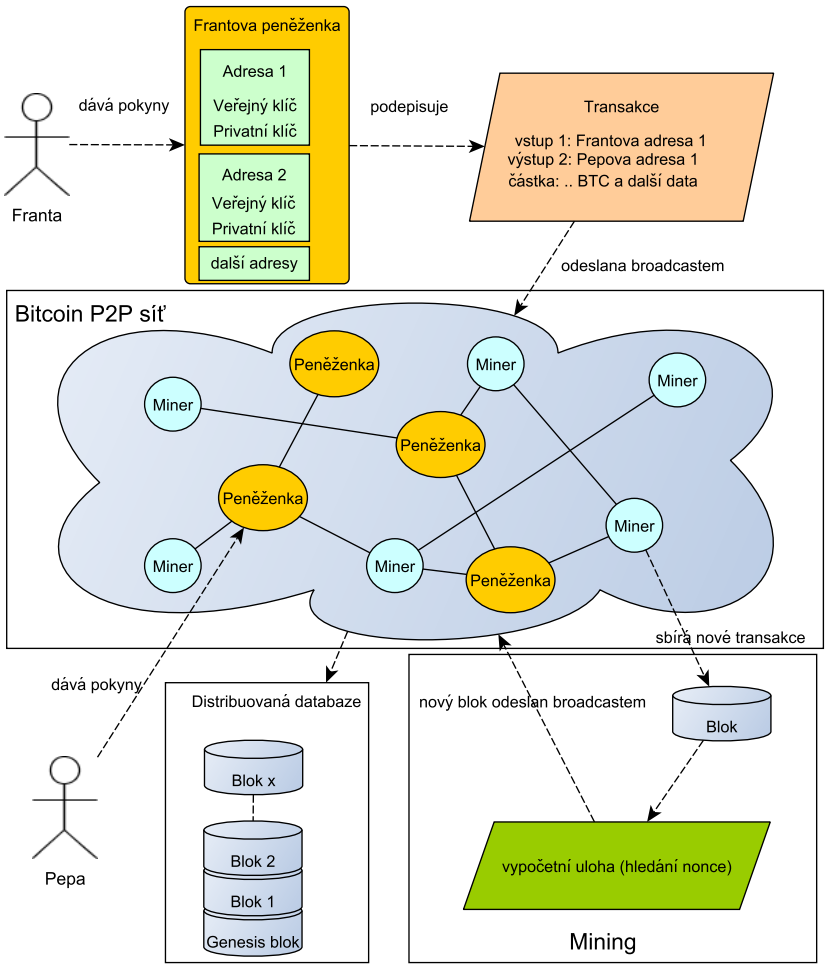
[11] `http://bitcoin.org/`

[12] `https://en.bitcoin.it/wiki/Main_Page`



(a) Běžná verze (b) Zlatá verze (c) Lze platit bitcoiny

Obrázek 2.1: Příklady nejběžnějších log [3]



Obrázek 2.2: Platební systém Bitcoinu

Bitcoin je platební systém tvořený počítačovou sítí. Tato síť je tvořena jednotlivými uzly. Na každém tomto uzlu je určitý typ aplikace. Tato aplikace komunikuje s ostatními aplikacemi pomocí protokolu Bitcoin. Aplikace jsou

dvojího základního typu.

Prvním typem je peněženka. Můžeme si ji představit jako aplikaci, která uchovává bitcoiny. Ve skutečnosti uchovává kryptografické klíče ke každé adrese v Bitcoinu, která v případě, že byla používaná, má záznamy v distribuované databázi transakcí. Pokud se jedná o verzi tlustého klienta[13], tak uchovává důležitou distribuovanou databázi, kterou si můžeme představit jako účetní knihu. Tato účetní kniha uchovává záznamy veškerých provedených transakcí v otevřené podobě a je distribuovaná mezi uzly sítě.

Druhým typem aplikace je miner. Jedna se o aplikaci, která zachycuje a zpracovává transakce v Bitcoin síti. Transakce se vytvoří ve chvíli, kdy majitel nějaké peněženky s bitcoiny chce poslat tyto bitcoiny jiné peněžence. Vytvoří se transakce, kterou je třeba ověřit. Ověřením se rozumí kontrola, zda skutečně danou částku odesílatel vlastní, respektive má-li právo s ní nakládat v síti. U bankovních převodů transakce ověřuje banka. V Bitcoin systému transakce ověřují mineři. Mineři jsou dobrovolníci sítě, kteří potvrzuji tyto transakce za odměnu ve formě nových emisních bitcoinů a přiložených transakčních poplatků odesílatelem transakce.

2.6.1 Bitcoinová počítačová síť

Počítačové sítě se dělí na dvě základní kategorie podle postavení uzlu v síti:

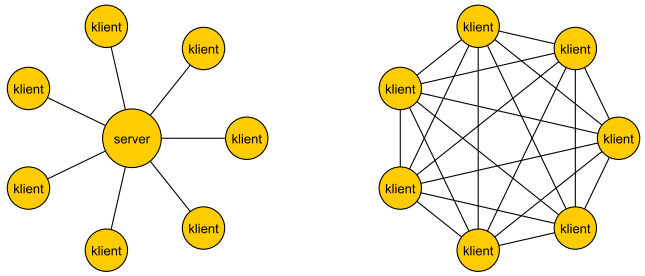
- Server-klient – tato síť je tvořena uzly, které jsou dvojího druhu server-klient. Server je uzel v síti, který zajišťuje komunikací mezi klienty. (viz. obrázek 2.3)
- Klient-klient – pro tuto síť je používaná anglická zkratka P2P. Tato síť má jediný typ uzlu a tím je klient. (viz. obrázek 2.3b)

Bitcoin používá síť klient-klient, kde klient komunikuje s klientem. V síti tedy neexistuje žádný centrální uzel, který by zajišťoval komunikaci jednotlivých klientů, proto se této sítí také říká decentralizovaná síť. Tady lze dobře vidět, že centrální autorita, v tomto případě reálný subjekt jako je banka, nemůže existovat z principu použité typu sítě.

2.7 (Ne)úplná decentralizace sítě

Říká se, že Bitcoin je plně decentralizovaná síť. Nicméně plně decentralizovaná síť nemůže v praxi existovat. Každý klient se musí připojit podle nějaké adresy. Počet nakonfigurovaných adres v klientu, podle kterých se musí připojit, je sice obrovský, avšak tento počet je vždy podmnožinou všech uzlů v síti. Tyto uzly sítě do jisté míry tvoří centralizaci. Jinými slovy vyřadí-li se tento určitý počet uzlů, potom se klient nebude moci k platební sítí připojit.

[13]Tento termín bude vysvětlen podrobněji v sekci 2.13



(a) Server-klient (b) Klient-klient

Obrázek 2.3: Počítačové sítě podle postavení uzlu

Plně decentralizovaná síť je tedy spíše teoretický pojem. Nicméně vzhledem k množství adres v klientech se to velmi blíží k plné decentralizované síti. Postup připojení klientů k síti, neboli hledání ostatních uzlů v síti je popsán zde: `https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery`.

2.8 Emise

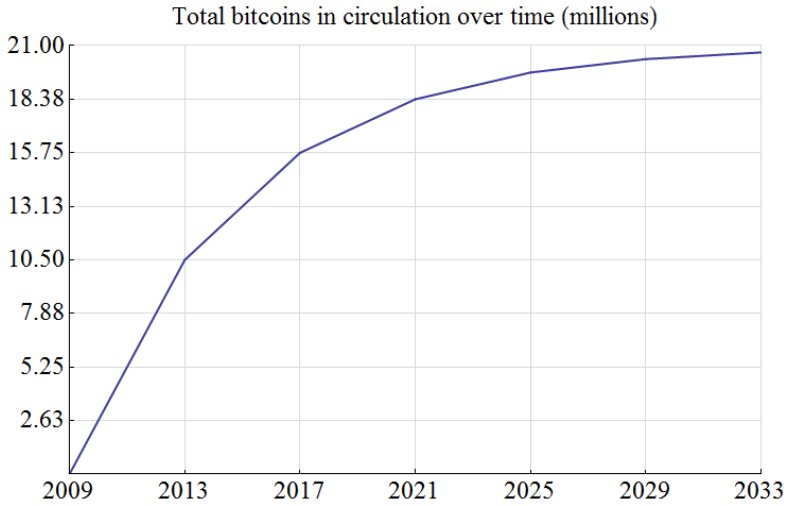
Jedna z hlavních vlastností Bitcoinu je emise nových bitcoinů, neboli tvorba a výdej nových bitcoinů do oběhu platebního systému. Bitcoin nabízí jenom jednu cestu vydání nových Bitcoin mincí do oběhu sítě a to pomocí emisí. Nové Bitcoin mince jsou udělované jako odměna minerovi, který vygeneroval další blok distribuované databáze.

Výše odměny za blok formou emisí se vždy snižuje na polovinu po 4 letech. Původně měla na začátku každá emise hodnotu 50 BTC v nově vytvořeném bloku. Po 28.listopadu 2012 se hodnota snížila na 25 BTC podle algoritmického postupu [4]. V dubnu 2013 se v oběhu nacházelo již téměř 11 milionů bitcoinů, což je více než polovina konečného počtu bitcoinů, který bude činit 21 milionů [4]. Další snížení bude až v roce 2017, kdy výše odměny za blok bude 12,5 BTC. Na Obrázku 2.4 vidíme model emisí, kde na ose y je znázorněn počet milionu BTC v oběhu.

2.8.1 „Sporný“ pojem deflace

Do roku 2040 bude vytěžena většina bitcoinů, viz. obrázek 2.4. Emise budou sice dále pokračovat až do roku 2140, ale v zanedbatelných částkách za každý nový zpracovaný blok. Po této době bude měna deflační. Bitcoiny se již budou jen ztrácet. V tomto případě lidé budou například zapomínat či ztrácet privátní klíče se kterými můžou v distribuované databázi manipulovat.

Avšak toto tvrzení nemusí být úplně pravdivé. Momentálně nejmenší jednotkou bitcoinů je satoshi, která je pojmenovaná na počest autora Bitcoinu. Jeden bitcoin má 100 000 000 satoshi. Bitcoin je tedy nyní dělitelný na osm



Obrázek 2.4: Emise nových bitcoinů [4]

desetinných míst. Konečný počet nejmenších jednotek, které bude existovat v sítí je $21 * 10^{6+8}$ satoshi. V budoucnosti ovšem existuje možnost změnit dělitelnost jednoho bitcoinu, čímž počet jednotek, kterými lze platit, se zvětší a dojde opět k inflaci[14]. Na tuto změnu ovšem musí přistoupit většina klientů sítě formou používání nové verze klienta, který tuto změnu dělitelnosti na ještě menší jednotky bude obsahovat.

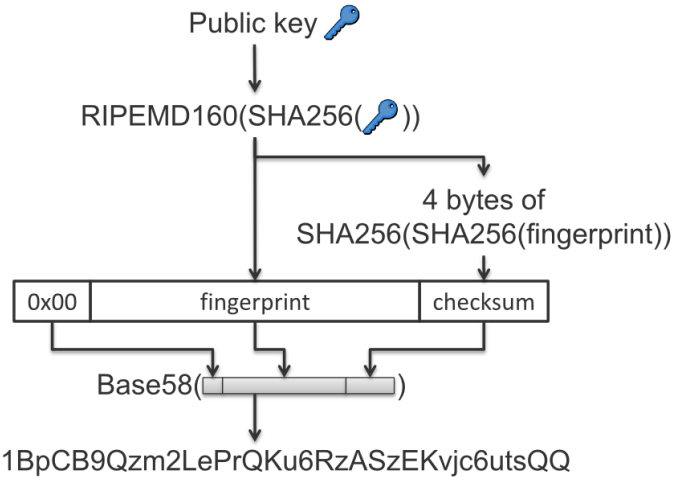
2.9 Účet v Bitcoin platebním systému

2.9.1 Adresa

Adresu v Bitcoin platebním systému si můžeme představit jako „číslo účtu“, na které se dají posílat bitcoiny.
Příklad takové adresy: 18K1E6WbXeuN2kqVW3r66vR9rrsieTh8Mu

Bitcoinová adresa je vždy reprezentovaná alfanumerickým řetězcem, který je dlouhý 27 až 34 znaků. Tento řetězec začíná číslem 1 až 3 a neobsahuje znaky malé a velké „o“, „l“ a nulu kvůli možnému špatnému rozpoznání znaku uživatelem při zadávání adresy. Řetězec má navíc ochranu proti překlepům při zadávání ve formě kontrolního součtu. Pokud se uživatel splete při zadávání adresy příjemce o jedno písmenko, tak je pravděpodobnost přibližně 1 ku 4,29 bilionu, že tato adresa bude platná a tím pádem se transakce neodešle ke zpracování minery.

[14] Respektive existuje možnost „jednorázových inflaci“



Obrázek 2.5: Postup generování adresy [4]

2.9.2 Generování klíčů a adresy

Adresa se generuje peněženkou na základě privátního a veřejného ECDSA klíče, které jsou podle algoritmického postupu náhodně zvolené peněženkou. Pomocí privátního klíče lze podepisovat transakce a odesílat je s veřejným klíčem. Pomocí veřejného klíče mineři ověřují podpis transakce a tím právo manipulace s bitcoiny.

Dalo by se hrubě říci, že adresa je 160-ti bitový hash veřejného klíče. Maximální možný počet adres v distribuované databázi je proto 2^{160}. Generování adres v peněžence nevyžaduje připojení k Bitcoin síti. Generování klidně může probíhat offline. Distribuovaná databáze „zaregistruje“ adresu ve chvíli, kdy jsou na tuto adresu odeslány nějaké bitcoiny. Do této doby žádný záznam o adrese v distribuované databázi není.

Privátní klíč je dlouhý 256 bitů. Pokud se klíč uživateli ztratí, tak bitcoiny zůstanou „viset“ na adrese. Nikdo k nim nebude mít přístup bez určitého privátního klíče k adrese, respektive nebude mít možnost s nimi manipulovat. Prakticky se nemůže stát, že peněženka vygeneruje z 2^{256} možných privátních klíčů stejný privátní klíč, který již je v distribuované databázi používán a má na dané adrese bitcoiny. Tato náhodná kolize privátních klíčů dostala pojmenování „Bitcoin birthday paradox“. Šance, že u někoho peněženka vygeneruje stejný privátní klíč je mizivá[15].

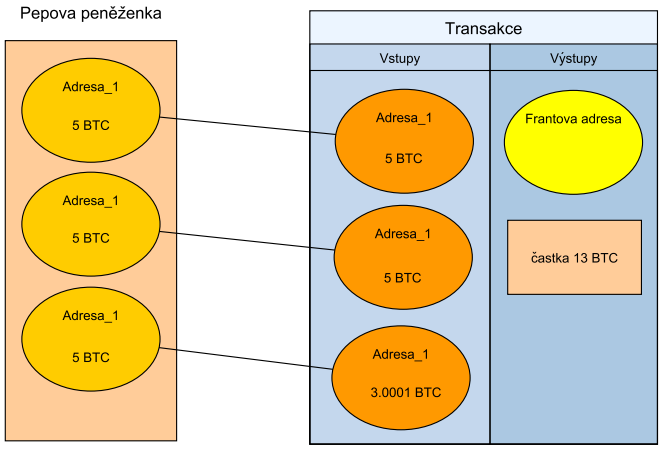
Na Obrázku 2.5 vidíme postup generování adresy. Peněženka algoritmicky zvolí privátní klíč a podle něj veřejný klíč. Tento veřejný klíč prochází různými hashovacími funkcemi, až z něj vznikne Bitcoinová adresa.

[15] http://download.wpsoftware.net/bitcoin-birthday.pdf

Obrázek 2.6: QR kód adresy „1F5zcrM7B77QoJR5R9Vfoy1yEB2ZzwyQvk“

2.9.3 QR kód adresy

Jelikož adresa je poměrně komplikovaná pro zadávaní platby (především v obchodech, restauracích) využívá se proto QR kódu. QR kód uchovává informaci o adrese. V obchodech či restauracích akceptujících bitcoiny to většinou probíhá tak, že příjemce ukáže svůj QR kód, následně tento QR kód vyfotí odesílatel aplikací, v tomto případě většinou peněženkou, která je v mobilu nebo v tabletu. Peněženka po rozpoznání adresy z QR kódu už jen žádá potvrzení o odeslání zadané částky. V tomto případě se urychluje zadávání transakce a placení probíhá pohodlnější pro obě strany. Příklad vygenerovaného QR kódu můžeme vidět na Obrázku 2.6.



Obrázek 2.7: Princip transakce

2.10 Transakce

Když chce jeden uživatel poslat bitcoiny jinému uživateli, vytváří transakci. Transakce na rozdíl od bankovních transakcí mají vícenásobné vstupy a výstupy. Každý vstup a výstup je reprezentován adresou Bitcoinu. Proto si lze

představovat Bitcoinovou transakci jako množinu bankovních transakcí. Na Obrázku 2.7 rozeberme příklad transakce. Pepa má privátní a veřejné klíče uložené v peněžence ke třem adresám Bitcoinu. Na těchto adresách je v distribuované databázi evidováno 5 bitcoinů na každé. Pepa chce poslat Frantovi jen 13 bitcoinů. Pepa zadá peněžence adresu Franty a částku 13 bitcoinů. Pepova peněženka vytvoří transakci a do ní přidá na vstup první dvě adresy a u každé nastaví částku 5 BTC. Následně do této transakce přidá třetí vstup jen se 3 bitcoiny a transakční poplatek 0.001 BTC jako odměnu za zpracování u minera. Tuto transakci peněženka podepíše privátními klíči a odešle do sítě Bitcoin broadcastem, což je rozeslání transakce na všechny uzly sítě. Digitální podpis u transakce ověřují mineři pomocí přiloženého veřejného klíče. Pokud je tento podpis platný, tak tuto transakci dál rozesílají po síti, jinak je zahozena prvními minery na cestě. Veškeré transakce mineři zahrnují do nového bloku. Transakce je potvrzená tehdy, až se mineři shodnou na novém bloku distribuované databáze. To trvá přibližně 10 minut.

Každá transakce má aspoň jeden výstup a jeden vstup. Výjimka je jen u emisní transakce, která nemá vstupní adresu, ale jenom výstupní adresu minerovi a obsahuje aktuálně částku 25 BTC jako odměnu za vytvořený blok distribuované databáze. Je nutno rovněž dodat, že po odeslání transakce do sítě není možné transakci jakkoliv zastavit nebo zrušit.

2.10.1 Transakční poplatky

Systém nemá zavedené povinné transakční poplatky. Uživatelé Bitcoinu mohou volitelně zahrnovat do převodu jakoukoliv částku transakčních poplatků. Přidání více prostředku na vstup transakce než na výstup zvyšuje prioritu zpracování takové transakce. Poplatek jde do uzlu, který vytvořil blok distribuované databáze s touto transakcí. Miner do generujícího nového bloku může podle svého uvážení přidávat nepotvrzené transakce z fronty. Například do nového bloku může vzít transakce, které pouze obsahující transakční poplatek. Minimální transakční poplatek je dnes stanoven na 0.001 BTC, což je v přepočtu při dnešním kurzu (1 BTC = 400 dolaru) kolem 10 Kč[16]. Téměř každý miner zahrnuje do bloku transakce s 0.001 BTC, proto se mu říká minimální. Nutno ovšem dodat, že na rozdíl od bankovních transakcí tato transakce může obsahovat libovolné množství vstupu a výstupu[17]. Je to tedy množina bankovních transakcí. Transakce s minimálním transakčním poplatkem je v drtivé většině případů potvrzená do 10 minut. V opačném případě bude potvrzená, až se jí uvolní místo. U každého vytvářeného bloku je nastaven limit počtu transakcí bez transakčních poplatků, který je proměnlivý. Uživatel peněženky může samozřejmě přidat větší částku na transakční poplatek než je minimální 0.001 BTC, ale je to zbytečné.

[16]Důvod proč je stanoven, bude vysvětlen v další kapitole

[17]Vstup a výstup je reprezentován adresou učtu v síti

Transakční poplatky do budoucna budou narůstat, protože odměna ve formě emisí za blok se každé čtyři roky snižuje. V budoucnu tedy budou mineři ověřovat transakce jen kvůli transakčním poplatkům.

2.11 Distribuovaná databáze transakcí

2.11.1 Řetězec bloku - „Blockchain“

Distribuovaná databáze je tvořena řetězcem bloku nebo si ji můžeme představit jako účetní knihu veškerých provedených a zaznamenaných transakcí od samého začátku fungování platební sítě. Tato distribuovaná databáze je tvořena bloky a v těchto blocích jsou zaznamenané potvrzené transakce. Databáze je distribuovaná, protože je sdílena mezi jednotlivými klienty v síti. Přibližně každých 10 minut je vytvořen nový blok „nasbíraných“ transakcí v síti. Pokud se tento blok transakcí minery ověří, tak se přidá k distribuované databázi. Databáze tedy postupně narůstá na velikosti. Momentálně velikost databáze činí přes 95 GB.

Distribuovaná databáze je v nezašifrované podobě. Veškeré proběhlé transakce proto můžeme vidět pomocí různých aplikací, přesněji prohlížečů této databáze. Nejpoužívanější online prohlížeč databáze je `https://blockchain.info/`.

2.11.2 Struktura bloku

Blok se skládá z hlavičky a seznamu transakcí. Hlavička bloku zahrnuje svůj hash, hash předchozího bloku, hashe transakcí a další potřebné servisní informace. První transakce v bloku obsahuje generaci nových Bitcoin mincí, které v případě úspěšného vytvoření nového bloku budou odměnou uživateli za vytvořený blok. Dále jsou tam všechny nebo některé z posledních transakcí, které ještě nebyly zapsané v předchozích blocích.

Vytvořený blok bude akceptován ostatními uživateli, pokud číselné označení hashe hlavičky je stejné nebo nižší než určitý cíl. Tato hodnota je pravidelně korigovaná. Pokud blok nesplňuje cíl, tak se mění blok servisní informace v hlavičce a hash se přepočítá. Obvykle se vyžaduje obrovský počet pokusů, jelikož výsledek hashování (funkcí SHA-256) je prakticky nepředvídatelný. Když je nalezena varianta splňující cíl, tak uzel rozesílá obdržený blok ostatním připojeným uzlům sítě. Ostatní uzly ověřují blok. Pokud nemá chyby, tak se tento blok přidává do řetězce bloku a další blok musí obsahovat v sobě jeho hash.

Velikost cílového čísla, se kterým se srovnává hash, se upravuje po každém zpracování 2016 bloků. Předpokládá se, že celá síť bude utrácet na tvorbu bloku přibližně 10 minut. Z toho lze vyvodit, že 2016 bloků bude trvat přibližně okolo dvou týdnů. Pokud se 2016 bloků vytvoří rychleji, tak se cílové číslo mírně sníží a dostihnutí se stává složitější, v opačném případě se zvýší. Změna výpočetní složitosti nemá vliv na spolehlivost sítě Bitcoin a vyžaduje se pouze

proto, aby systém generoval bloky s téměř konstantní rychlostí, nezávisle od celkového výpočetního výkonu sítě.

2.12 (Pseudo)-anonymita uživatelů Bitcoin

Říká se, že Bitcoin je zcela anonymní. Toto tvrzení není pravdivé. Distribuovaná databáze uchovává veškeré potvrzené transakce v nezašifrované formě. Veškeré potvrzené transakce lze proto dohledat v prohlížeči distribuované databáze a stejně tak záznamy transakcí jednotlivých adres. V konečném důsledku lze vidět, kolik adresa celkem provedla transakcí a aktuální částku v bitcoinech na adrese. Ovšem tato adresa v databázi nemá uvedené žádné osobní udaje. Je tedy v tomto případě anonymní, ale tuto anonymitu lze lehce ztratit následujícím příkladem.

Nakoupím na burze milion bitcoinů, které mě burza pošle na adresu Bitcoinu. Kdokoliv v prohlížeči může najít transakci s milionem bitcoinů a nebo zadat rovnou mojí adresu a vidět aktuální zůstatek milion bitcoinů na adrese. Nikdo (vyjma burzy) neví, komu tato adresa patří. Horší to začíná být při placení různých služeb. Například firma bude chtít zaplatit 10 bitcoinů. Pošle mi svoji adresu a na tuto adresu pomocí peněženky pošlu 10 bitcoinů z „milionové“ adresy. Firma se v tu chvíli může podívat na moji adresu z transakce a nyní ví, že jsem milionář. Toto lze ovšem obejít tak, že si uživatel nechá vytvořit více adres a na tyto adresy si nechá z milionové adresy posílat bitcoiny. Aplikuji toto nyní na předchozí příklad.

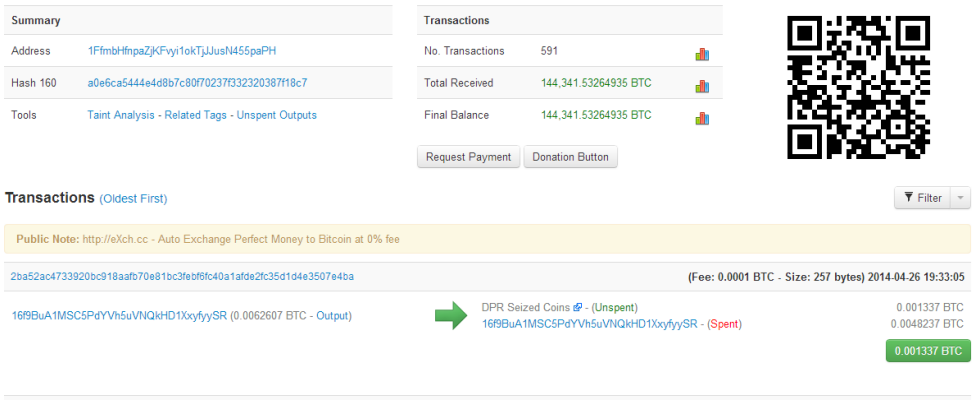
Nakoupím na burze milion bitcoinů a nechám si je poslat na jednu adresu. Vytvořím další adresy a na tyto adresy pošlu například po 20 BTC. Následně chci zaplatit a příjemci pošlu 10 BTC. Příjemce se koukne na moji adresu a uvidí, že mám na adrese 20 BTC a tyto bitcoiny jsem dostal od adresy, na které je milion BTC. Už ovšem neví, zda tato „milionová“ adresa patří mě nebo ne. Může si rovněž myslet, že je to můj bohatý zaměstnavatel.

Na Obrázku 2.8 vidíme výpis „nejbohatší“ adresy z distribuované databáze pomocí prohlížeče včetně poslední zaznamenané transakce. Můžeme vidět, že adresa za dobu existence provedla 591 transakcí a má aktuálně na kontě přes 140 000 bitcoinů. Identita, která vlastní tuto adresu již je veřejně prozrazena. Tuto adresu vlastní bezpečnostní složky USA, které v rámci v boji proti SilkRoad[18], zabavili veškeré klíče ke všem bitcoinům a nechali je „nahromadit“ na jedné adrese. Bitcoin tedy má účty pseudoanonymní.

2.13 Klient

V počátcích platebního systému existoval jen jeden typ klienta a tím byla dnešní oficiální peněženka Bitcoin-QT, která se také nazývá Satoshi klient na

[18] Jednalo se webový portál, kde lidé anonymně platili bitcoiny za nelegální služby a zboží



Obrázek 2.8: Aktuálně nejbohatší adresa Bitcoinu [5]

počest zakladatele Bitcoinu. Tento oficiální klient plní veškeré funkce platební sítě Bitcoin, mezi nimiž jsou:

- generování klíčů s adresami
- vytváření transakcí
- ověřování transakcí (Mining)
- držení distribuované databáze (transakční historie)

Klienti komunikovali a komunikují pomocí protokolu Bitcoinu, který v sobě mají implementovaný. Oficiální klient má po celou dobu existence platebního systému veřejně přístupný otevřený kód. Každý vývojář se proto mohl a může přesvědčit na vlastní oči, jak tento platební systém funguje do nejmenších detailů na adrese `https://github.com/bitcoin/bitcoin`. Tohoto klienta spravuje vývojářská komunita Bitcoinu. Když se vývojářská komunita rozšiřovala, začali se vyvíjet noví klienti a došlo k dělení klientů na podtypy. Vznikly dva základní podtypy klientů:

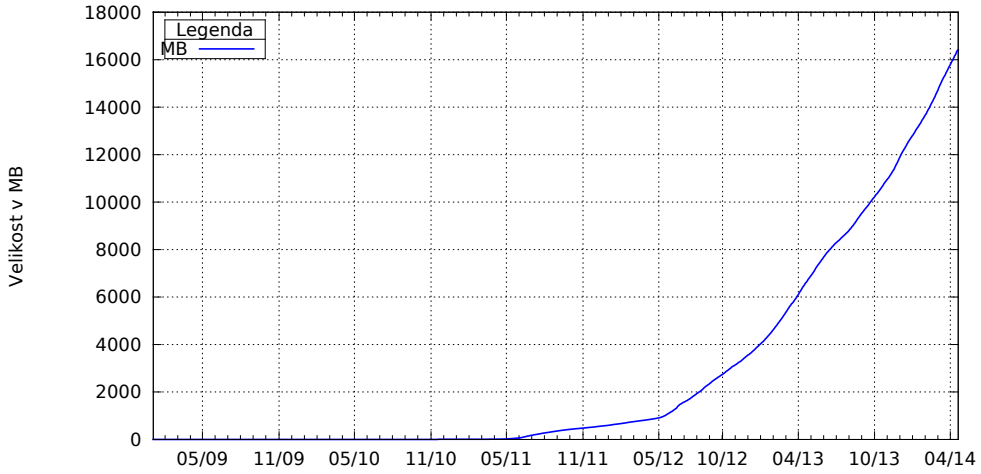
- Miner – Aplikace, která zpracovává a ověřuje transakce za odměnu ve formě transakčních poplatků a emisí nových bitcoinů
- Peněženka – Aplikace, která vytváří nové klíče a k nim adresu, vytváří nové transakce

Se vzrůstající popularitou používaní Bitcoinu se naskytl technický problém. Tímto problémem byla rostoucí distribuovaná databáze záznamů transakcí. V tomto směru totiž platí jednoduché pravidlo: čím více transakcí, tím více je potřeba uchovat záznamů, které jsou nezbytné k prokázání vlastnictví bitcoinů. Rychlost růstu velikosti databáze lze vidět na Obrázku 2.9. V dnešní době má tato databáze přes 95 GB. To představuje velký problém pro mobilní

zařízení a podobně. Naštěstí se našlo řešení a tímto řešením bylo dělení klientů na dvě kategorie:

- lehký klient
- tlustý klient

Lehký klient nemusí stahovat celou distribuovanou databázi, ale pouze hlavičky jednotlivých bloků. Tlustý klient je takový klient, který musí mít staženou celou distribuovanou databázi. V podstatě když se dnes mluví o klientovi, tak se tím myslí peněženka, ačkoliv klientem jsou rovněž aplikace minery. Důležité je zmínit, že všichni dostupní klienti mají otevřený zdrojový kód. Každý vývojář se tedy může přesvědčit o funkčnosti jednotlivých klientů.



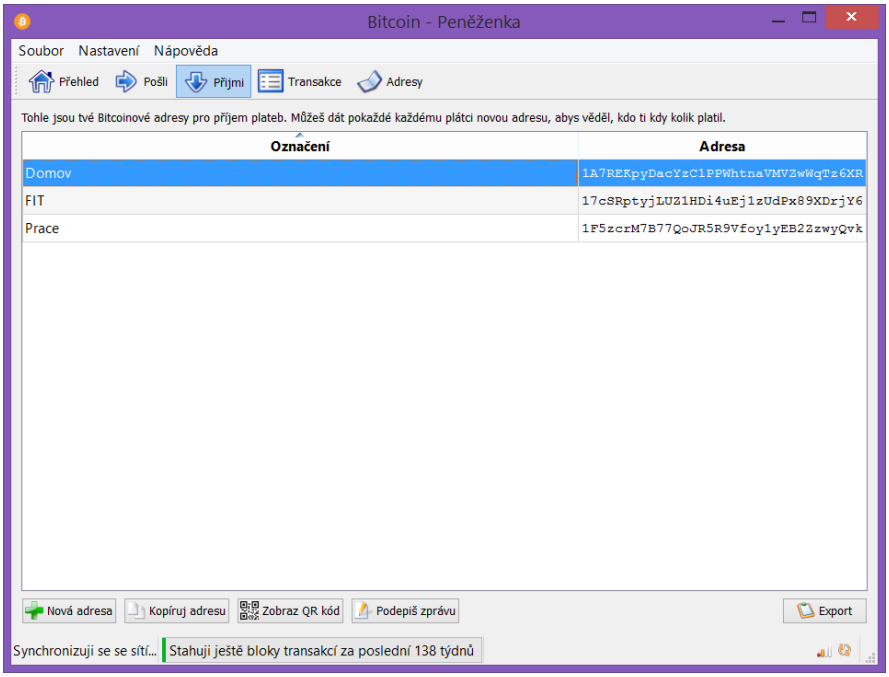
Obrázek 2.9: Vývoj velikosti distribuované databáze [5]

2.13.1 Tlustý klient(validator, miner)

2.13.1.1 Oficiální klient

Tento klient(validator, miner) i nyní má veškeré funkce v platební síti. Problémem je, že vyžaduje celou distribuovanou databázi. Po nainstalování a připojení k Bitcoin síti začne tuto databázi o velikosti přes 95 GB stahovat. Klient má také funkci miningu, která je ve výchozím nastavení již vypnutá. Důvodem proč je vypnutá je to, že tato funkce klienta už není nadále vyvíjena. K miningu se hodí klienti mineři, kteří jsou aktualizovaní. Všechny klíče, které klient vygeneruje, jsou uložené v souboru „wallet.dat“. Tento soubor je terčem útočníků, kteří chtějí převést bitcoiny na svou adresu. Peněženka již nabízí funkci zašifrování tohoto souboru, což je velmi užitečná funkce, protože když tento soubor s klíči ukradne útočník, tak tento soubor jen tak nedešifruje. Obecně je dobré tento soubor v zašifrované podobě uschovávat na několika

místech. V případě ztráty klíčů totiž zůstanou bitcoiny „viset“ nepřístupné v distribuované databázi. Nikdo s nimi nebude moci manipulovat. Další možností je v konzoli peněženky příkazem vypsat veškeré privátní klíče a zapsat si je někam tajně na papír. V tomto případě by vám ovšem klíč mohl ukrást v reálném světě inteligentní zloděj a importovat ho do peněženky. Uživatelské prostředí oficiálního klienta můžeme vidět na Obrázku 2.10.



Obrázek 2.10: Oficiální klient

2.13.1.2 Ostatní tlustí klienti

Mezi další klienty, kteří vychází z oficiálního klienta patří například Armory, Cocoin. Tito klienti nabízí jiné uživatelské rozhraní nebo o něco více funkcí, jako správu více peněženek a podobně. Za zmínku stojí klient Bitcoind. Jedná se fakticky o verzi oficiálního klienta bez uživatelského rozhraní, které lze ovládat v terminálu. Je rovněž spravován vývojářskou komunitou Bitcoinu.

2.13.2 Tencí klienti

Jak již bylo zmíněno, jsou to klienti, kteří nemusí stahovat celou databázi. Stahují jen specifickou informaci o adresách v peněžence a rovněž hlavičky jednotlivých bloků, které vyžadují jen desítky MB na datovém médiu. Veškeré privátní klíče jsou uložené v těchto klientech. Takže se jedná prakticky o stejnou bezpečnost jako u tlustých klientů. Tito klienti se dnes běžně instalují do počítačů, protože fakticky nemá smysl pořizovat tlustého klienta,

který vyžaduje 95 GB místa. Distribuovanou databázi v dnešní době již potřebují v Bitcoin síti jen mineři k ověřování transakcí za odměnu. Nemůže se v budoucnu stát, že distribuovaná databáze zmizí ze všech uzlu sítě. Přesto lidé, především noví uživatelé Bitcoinu, stahují oficiálního klienta do počítače, ačkoliv toto již není potřeba. Jsou tu samozřejmě i jiné důvody jako důvěra. Například uživatelé chtějí prohlížet distribuovanou databázi, která je uložena u tlustých klientů. Tenké klienty vždy najdeme na mobilních zařízeních, které mají omezenou paměť.

2.13.2.1 Tencí klienti na počítačích

Mezi známé tenké klienty na počítačích patří Electrum, MultiBit a Hive. Jsou vesměs stejné. Liší se především uživatelským prostředím.

2.13.2.2 Tencí klienti na mobilních zařízeních

Mezi tenké klienty na mobilních zařízeních patří „Bitcoin Wallet“. Tato peněženka je speciálně adaptovaná pro platby v reálném světě, například v restauracích. Dokáže lehce rozpoznat QR kód a také ho vygenerovat pro příchozí platbu.

2.13.3 Online (webová) peněženka

Jedná se většinou o službu, která nabízí založení peněženky na své webovém portálu, respektive serveru. Je to velmi podobné internetovému bankovnictví. Uživatel založí účet a vygeneruje adresu na účtu, na kterou může posílat bitcoiny. Problémem je, že je to velmi nebezpečné. Klíče jsou uložené na serveru služby. Uživatel důvěřuje službě. V dnešní době některé služby slibují, že peněženky uživatelů jsou v zašifrované podobě uložené na jejich serveru, avšak tato důvěra může vyjít draho. Servery jsou často napadány útočníky a jakmile zkopírují nebo odcizí klíče, tak převádí bitcoiny na jinou adresu. Rovněž samy tyto služby můžou okrást, takže je lépe se vyvarovat online peněženek. Někdy to ovšem není možné, viz. dále.

2.13.3.1 Peněženky na burze

Pokud uživatel chce nakupovat nebo prodávat bitcoiny na burze, musí založit v účtu na burze online peněženku. Tyto klíče budou uložené na burze, respektive jejím serveru. Je vhodné při každém nákupu bitcoinů, které se ocitnou na burzovní adrese peněženky, přemístit tyto bitcoiny bezprostředně po nákupu na adresu, u které má uživatel klíče jen u sebe, nikoliv jinde na serveru.

2.13.3.2 Služby online peněženek

Existuje více služeb, které nabízí založení online peněženek. Je to výhodné hlavně kvůli přístupu k peněženkám odkudkoliv, kde je přístup k internetu.

Stačí se přihlásit pod svým emailem a heslem a už lze spravovat v internetovém prohlížeči svou peněženku. Tyto služby rovněž nabízí menší aplikace, které se připojují k serverům. Tyto aplikace se dají nainstalovat do počítače nebo mobilu, ovšem aplikace nestahují distribuovanou databázi ani nemají v sobě uložené klíče, pouze přes ně lze přistupovat a ovládat na serveru veškeré operace peněženky jako je vytváření nové transakce a podobně.

Obrázek 2.11: První nejznámější hardwarová peněženka Trezor [6]

2.13.4 Hardwarová peněženka

Jedná se o nový typ peněženky, která je v podobě flešky, viz. Obrázek 2.11. Pravděpodobně se dnes jedná o nejbezpečnější typ peněženky. Tato peněženka při vytváření nové adresy vygeneruje 12 slov ze své velké databáze slov, které reprezentují privátní klíč. V případě ztráty této peněženky stačí koupit novou peněženku a tato nová peněženka vypočítá privátní klíč pomocí zadaných 12 slov podle algoritmu a z toho pak veřejný klíč a adresu. Je to lepší způsob než si zapisovat na papír 256-bitový privátní klíč.

Provádění transakcí probíhá tak, že je třeba připojit peněženku k zařízení s přístupem na internet. Po této akci vyskočí offline statická stránka (počítač nepotřebuje instalovat žádnou další podpůrnou aplikaci). V této statické stránce se můžou vytvářet transakce. Následně vytvořená transakce putuje do hardwarové peněženky, které vyžaduje potvrzení tlačítkem na peněžence a zadání čísel do statické stránky, které se objeví na displeji peněženky. Následuje další potvrzení po zadání hesla a tato transakce se podepisuje v peněžence privátním klíčem a putuje do sítě Bitcoin přes pomocný webový server, který jen odesílá podepsané transakce do Bitcoin sítě.

Obrázek 2.12: Papírová peněženka jako dárek [7]

2.13.5 Papírová peněženka

Tuto peněženku lze vytvořit pomoci různých nabízených služeb na internetu. Fakticky se jedná o službu na webové stránce, která vygeneruje náhodně privátní klíč s adresou a tuto adresu s privátním klíčem včetně jejich reprezentace QR kódu zarámuje „krásně“ do dokumentu. Následně tento dokument lze vytisknout na tiskárně a poslat na adresu bitcoiny. Tato papírová peněženka (nebo si ji můžeme představit jako kupón s klíči) může sloužit jako dárek blízkým. Existují služby, které rovněž tyto dobrovolně nabité papírové peněženky nechají udělat na kvalitnější papír a za poplatek poslat na adresu zvolenou uživatelem. Příklad papírových peněženek viz. Obrázek 2.12.

2.14 Mining(validating)

Činnost, která má vytvářet nové bloky s možností získat odměnu ve formě emisních bitcoinů a transakčních poplatků dostala název mining, což je v překladu těžba. Produkované výpočty jsou potřebné pro zajištění ochrany před dvojitým utracením bitcoinů. Spojitost miningu s emisemi povzbuzuje lidi, aby poskytovali svůj výpočetní výkon na údržbu sítě Bitcoin. Klienti, kteří provádí těžbu, jsou mineři, neboli v překladu těžaři bitcoinů.

Mineři se připojují do sítě a sbírají do bloku transakce, které kolují broadcastem po síti. Mezitím co sbírají transakce do bloku, počítají kryptografickou výpočetní úlohu. Ten, kdo vyřeší tuto výpočetní úlohu jako první, vygeneruje nový blok, a tím pádem získá odměnu ve formě nových emisních bitcoinů a

k tomu všechny transakční poplatky transakcí, které byly zahrnuté do tohoto bloku. Tento nový blok je následně distribuován po síti. Hlavičky bloku mají velikost 80 Bytů pro tenké klienty. Celý blok pro tlusté klienty má velikost do 1 Mb[19]. Aktuální počet bloků je již téměř 300 000. Až dojdou bloky s emisemi bitcoinů, tak mineři budou těžit jenom kvůli transakčním poplatkům. Aktuálně minimální transakční poplatek je 0.001 bitcoinů[20]. V budoucnu se počítá, že se bude zvětšovat.

2.14.1 Kryptografická výpočetní úloha

Kryptografická výpočetní úloha spočívá v hledání takového hashe funkce SHA-256, které je menší než stanovený cíl. Tento cíl je rovněž ve formátu hashe funkce SHA-256. Tento problém se řeší hashovaním náhodných řetězců funkcí SHA-256. Pokud funkce SHA-256 vydá menší hodnotu než zadaný cíl, tak miner vítězí v hledání bloku. Šance se zvyšují u toho, kdo má vyšší výpočetní výkon v síti. Například zařízení minera, které dokáže zpracovat 400 milionů hashů za sekundu, má větší šanci najít řetězec než zařízení minera, který má výkon zařízení 20 milionů hashů za sekundu, avšak slabší zařízení minera může narazit na řetězec, který bude vyhovovat dřív.

Nejjednodušeji si tuto úlohu obecně lze představit tak, že je zadán určitý rozsah hashů. V této množině hashů je podmnožina hashů, které jsou výsledkem řešení výpočetní úlohy, a pak je tu podmnožina hashů, která není výsledkem řešení. Větší šanci narazit na podmnožinu řešení má ten miner, který má větší výpočetní výkon.

Tomuto validačnímu algoritmu se říká PoW - proof of work. V další kapitole budou popsaný jiné validační algoritmy.

2.14.2 Složitost výpočetní úlohy

Model emisí Bitcoinu počítá s tím, že každý nový blok bude nalezený za 10 minut. Problémem je, že výkon celé sítě je proměnlivý. Uvedu příklad:

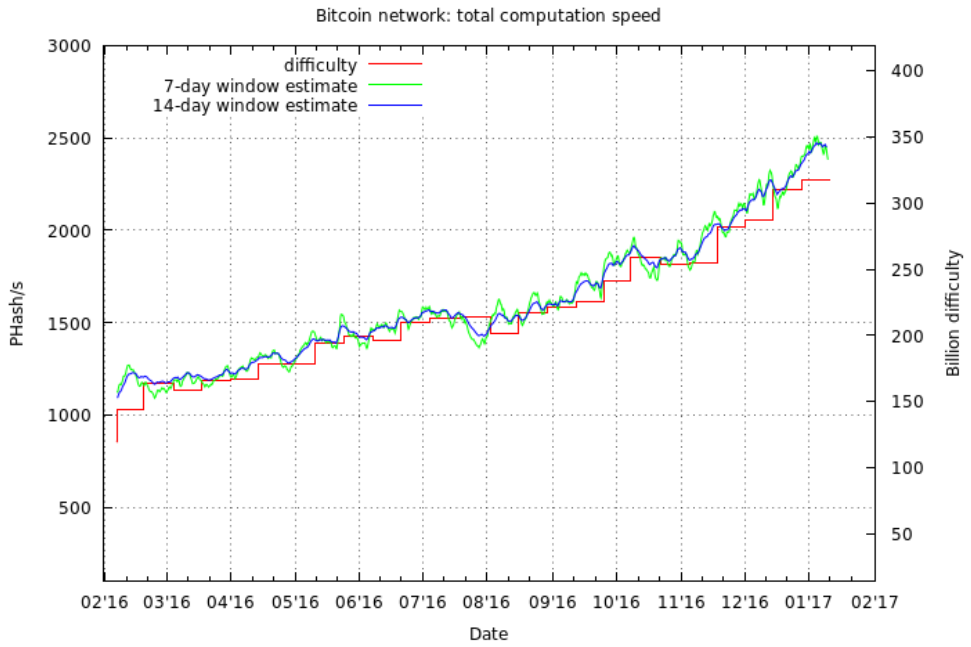
Když začal fungovat Bitcoin, tak bylo 100 minerů. Každý tento miner měl pro jednoduchost stejné výpočetní zařízení, které dokázalo zpracovat 20 milionů hashů za sekundu. Výkon celé sítě tedy v tomto případě je $100 * 20 =$ 2000 milionů hashů za sekundu. Poté co Bitcoin začal být populárnější, počet minerů se zvětšil a výkon sítě například už byl 5000 milionů hashů za sekundu. Celá síť s výkonem 5000 milionu hashů za sekundu vyřeší výpočetní úlohu pravděpodobněji rychleji než síť s 2000 miliony hashů za sekundu.

Z tohoto důvodu po každém 2016 bloku mineři hlasují o obtížnosti nového cíle. Při faktu, že každý blok se musí vytěžit za 10 minut, musí trvat 2016 bloků $2016 * 10 = 20160$ minut (2 týdny). Klienti sítě se podívají na tuto hodnotu a pokud tato hodnota bude menší, tak se zvětší složitost výpočetní úlohy, v

[19]Podle počtu transakcí zahrnutých do bloku

[20]Důvod proč je nyní nastaven, bude uveden v další kapitole

opačném případě se zlehčí. Touto akcí se cílí na to, aby byl zachován emisní model. V praxi se tedy bloky negenerují přesně 10 minut, ale v intervalu 5 až 15 minut. 2016 bloků ovšem nutně musí dávat 20160 minut. Tento fakt hlídají a korigují klienti většinovým názorem pomocí složitosti cíle.



Obrázek 2.13: Vývoj výkonu sítě [8]

2.14.3 Možnosti těžby

Úplně na začátku existoval jen jeden model těžby, kde každý miner se svým zařízením těžil sám v síti jako jedinec. Jedinci nakupovali co nejvýkonnější zařízení na počítaní hashů. Tento model fungoval určitou dobu do chvíle než český vývojář Marek Palatinus vymyslel mining pool.

Mining pool je systém, ve kterém se sdruží více minerů. Každý miner v této těžařské síti provádí určitý rozsah výpočtů určený mining poolem. Pokud mining pool vyřeší úlohu, tak odměna za nový blok s transakčními poplatky se rozdělí mezi minery v mining poolu podle podmínek, které stanoví provozovatel mining poolu. V dnešní době většina minerů těží v mining poolu. Důvodem je výpočetní výkon celé sítě. Na Obrázku 2.13 můžeme vidět vývoj výpočetního výkonu sítě s vývojem složitosti výpočetní úlohy. Aktuální výkon sítě je 70000 trilionů hashů za sekundu. Miner, který se zapojí jako jedinec, má extrémně malou šanci s disponovaným výkonem vyřešit nejrychleji úlohu a získat odměnu.

2.15 Dvojité utracení bitcoinů

S miningem úzce souvisí nechtěné větvení řetězce bloku, které může nastat ze dvou důvodu:

- kolize minerů (neúmyslné větvení)
- útok dvojitého utracení bitcoinů (úmyslné větvení útočníkem)

Nejdříve rozebereme kolizi minerů a následně útok dvojitého utracení.

Obrázek 2.14: Počet potvrzení transakce

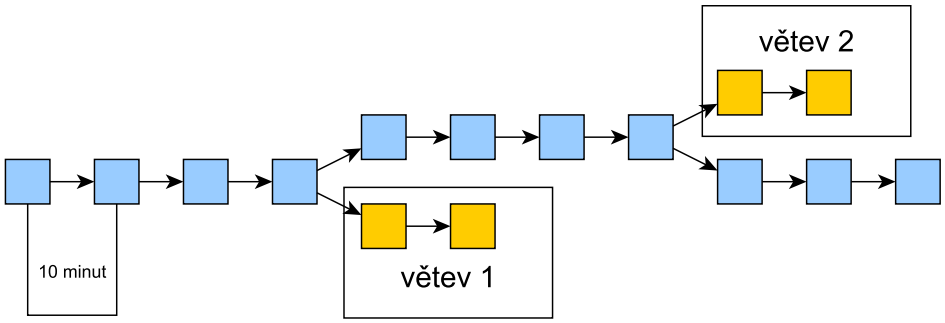
2.15.1 Pojem počet potvrzení transakce

Obvykle při obdržení Bitcoin mincí s nimi nový vlastník nemůže hned počítat. Pro zmenšení pravděpodobností dvojitého použití jakákoliv transakce musí mít nějaké množství ověření, neboli potvrzení. Za jedno potvrzení se považuje jeden nový blok, ve kterém je transakce zabalena. Nezbytné množství potvrzení závisí od software klienta nebo pokynů z přijímací strany.

Obdržené Bitcoin mince za vytvoření nového bloku se nemůžou použít, dokud počet potvrzení nedosáhne 120. Bitcoin mince obdržené od jiných uživatelů klient Bitcoin-QT dovoluje použít až po 6 potvrzení (obvykle 60 minut). Různé online služby často stanovují mez počtu potvrzení. Na Obrázku 2.14 lze ilustrovat počet potvrzení. Řekněme, že mineři ověřili transakci a zahrnuli ji do nového bloku. Tato transakce bude mít čtyři potvrzení, až se vytvoří další tři bloky.

2.15.2 Kolize minerů

Dva mineři těsně v rozmezí několika sekund vyřešili kryptografickou výpočetní úlohu a publikovali své výsledky síti. Část uzlu se stihla přidat na stranu jed-



Obrázek 2.15: Větvení řetězce bloku

noho bloku, druhá část začala uznávat druhý blok. Tento fakt se občas stává, viz. Obrázek 2.15. Oba tyto paralelní bloky můžou mít část stejných transakcí nebo mít úplně stejné transakce. Každá část minerů nadále pokračuje ve výpočtu dalších bloků a zvítězí ta větev, která roste rychleji. Mineři si toto uvědomí. Zahodí kratší větev a veškeré transakce z kratší větve dají opět do fronty, a jelikož určitá část z nich již byla potvrzená ve větvi, která zvítězila, tak tato část transakcí již nebude přidaná do databáze, protože fakticky už tyto transakce byly použity a tyto bitcoiny má nový vlastník. Stejně tak transakční poplatky s emisemi. To je jeden z důvodu, proč se čeká aspoň na několik potvrzení. Další důvod je útok dvojitého utracení.

2.16 Útok dvojitého utracení bitcoinů

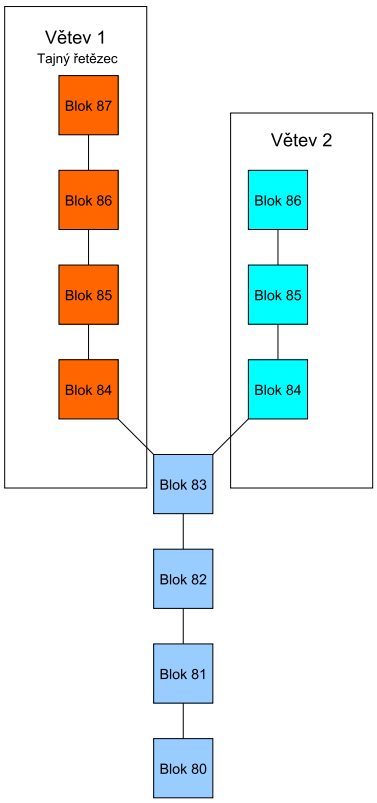
Pokud se uživatel pokusí použít již utracené bitcoiny, síť neakceptuje tuto transakci jako platnou. V paralelních řetězcích bloku můžou být transakce, které různě utrácí jedny a tytéž počáteční prostředky. Pravděpodobnost existence paralelních řetězců je velmi nízká a exponenciálně klesá s růstem délky řetězce a počtu nezávislých minerů. To znamená, že čím více potvrzení transakce má, tím menší je pravděpodobnost zrušení transakce kvůli vedlejším řetězcům bloku, které v budoucnu budou zahozeny. Nicméně v případě, že útočník má dostatečně velký podíl celkového výpočetního výkonu miningu, existuje nenulová pravděpodobnost „tajné“ tvorby paralelních řetězců bloku. Po jejich zveřejnění v síti bude uznán nejdelší řetězec bloku. Zrušení řetězce bloku může vést k neplatnosti transakce dokonce potvrzených několika bloky a k další opakované utratě prostředku. V případě výskytu v jediných rukou více než 50% celkového výkonu miningu taková situace může nastat v jakémkoliv stádiu potvrzení. Pokud je výpočetní výkon v jediných rukou menší než 50%, tak se pravděpodobnost úspěchu exponenciálně snižuje s každým potvrzením. Provedení úspěšného útoku například neumožňuje:

- změnit výši odměny za vytvoření nového bloku

- získat neomezený počet bitcoinů
- zničit celou síť
- utratit bitcoiny, které dříve nepatřily útočníkovi

Umožňuje ovšem například:

- bránit ostatním těžařům ve vytěžení bloku
- bránit potvrzování transakcí
- „utratit“ bitcoiny vícekrát



Obrázek 2.16: Příklad dvojitého utracení

2.16.0.1 Příklad dvojitého utracení

Tento příklad má názorně ukázat problem zákeřného útoku dvojitého utracení podle pomocného Obrázku 2.16

Pepa s komplicem má záměr okrást Frantu. Pepa přišel do Frantovy restaurace. Na konci Pepa platil bitcoiny Frantovi přes mobilní peněženku. Pepova

transakce se dostala do bloku 84 větve 2 a tento blok potom byl následně rozeslán po síti minery. Franta uviděl ve své peněžence transakci s danou částkou od Pepy, která má jedno potvrzení a pustil ho. Když Pepa vyšel ven, zavolal komplici, který vlastní superpočítač na mining. Tento superpočítač má obvykle 40% výpočetního výkonu celé sítě. Pepa dal komplici tyto pokyny:

1. Začni tajně těžit bloky superpočítačem.

2. Vytvoř transakci z mé adresy a pošli ji na jinou mou adresu.

3. Tuto transakci přidej do nového vytvořeného, tajného bloku 84 (větev 1)

Superpočítač tajně začal počítat výpočetní úlohy a nacházel nové bloky ve své tajné větvi 1 rychleji než ostatní mineři v síti (ve větvi 2). Když vyřešil ve své větvi blok 87, rozhodl se zveřejnit celé síti svou tajnou větev 1. Ostatní mineři v síti do zveřejnění této větve zatím našli blok 86 (větev 2). Když k ostatním minerům dorazil blok 87 z větve 1 se třemi předchozími bloky, zahodili svou větev 2. Všechny transakce z větve 2 jsou přesunuty do fronty potenciálního nového bloku 88 větve 1. U Frantovy transakce ovšem nastal problém, protože bitcoiny z této transakce jsou již použity v bloku 84 (větev 1). Tato transakce je následně minery zahozená. Franta po 3 potvrzeních (30 minut) zjišťuje, že transakce s bitcoiny byla zrušena. Franta byl okraden.

Útočník, který měl výkon superpočítače 40% výkonu celé sítě, by mohl tento útok provést pravděpodobností 58%, viz. dále.

q	1	2	3	4	5	6	7	8	9	10
2%	4%	0.237%	0.016%	0.001%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
4%	8%	0.934%	0.120%	0.016%	0.002%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
6%	12%	2.074%	0.394%	0.078%	0.016%	0.003%	0.001%	≈ 0	≈ 0	≈ 0
8%	16%	3.635%	0.905%	0.235%	0.063%	0.017%	0.005%	0.001%	≈ 0	≈ 0
10%	20%	5.600%	1.712%	0.546%	0.178%	0.059%	0.020%	0.007%	0.002%	0.001%
12%	24%	7.949%	2.864%	1.074%	0.412%	0.161%	0.063%	0.025%	0.010%	0.004%
14%	28%	10.662%	4.400%	1.887%	0.828%	0.369%	0.166%	0.075%	0.034%	0.016%
16%	32%	13.722%	6.352%	3.050%	1.497%	0.745%	0.375%	0.190%	0.097%	0.050%
18%	36%	17.107%	8.741%	4.626%	2.499%	1.369%	0.758%	0.423%	0.237%	0.134%
20%	40%	20.800%	11.584%	6.669%	3.916%	2.331%	1.401%	0.848%	0.516%	0.316%
22%	44%	24.781%	14.887%	9.227%	5.828%	3.729%	2.407%	1.565%	1.023%	0.672%
24%	48%	29.030%	18.650%	12.339%	8.310%	5.664%	3.895%	2.696%	1.876%	1.311%
26%	52%	33.530%	22.868%	16.031%	11.427%	8.238%	5.988%	4.380%	3.220%	2.377%
28%	56%	38.259%	27.530%	20.319%	15.232%	11.539%	8.810%	6.766%	5.221%	4.044%
30%	60%	43.200%	32.616%	25.207%	19.762%	15.645%	12.475%	10.003%	8.055%	6.511%
32%	64%	48.333%	38.105%	30.687%	25.037%	20.611%	17.080%	14.226%	11.897%	9.983%
34%	68%	53.638%	43.970%	36.738%	31.058%	26.470%	22.695%	19.548%	16.900%	14.655%
36%	72%	59.098%	50.179%	43.330%	37.807%	33.226%	29.356%	26.044%	23.182%	20.692%
38%	76%	64.691%	56.698%	50.421%	45.245%	40.854%	37.062%	33.743%	30.811%	28.201%
40%	80%	70.400%	63.488%	57.958%	53.314%	49.300%	45.769%	42.621%	39.787%	37.218%
42%	84%	76.205%	70.508%	65.882%	61.938%	58.480%	55.390%	52.595%	50.042%	47.692%
44%	88%	82.086%	77.715%	74.125%	71.028%	68.282%	65.801%	63.530%	61.431%	59.478%
46%	92%	88.026%	85.064%	82.612%	80.480%	78.573%	76.836%	75.234%	73.742%	72.342%
48%	96%	94.003%	92.508%	91.264%	90.177%	89.201%	88.307%	87.478%	86.703%	85.972%
50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Obrázek 2.17: Úspěšnost útoku dvojitého utracení [9]

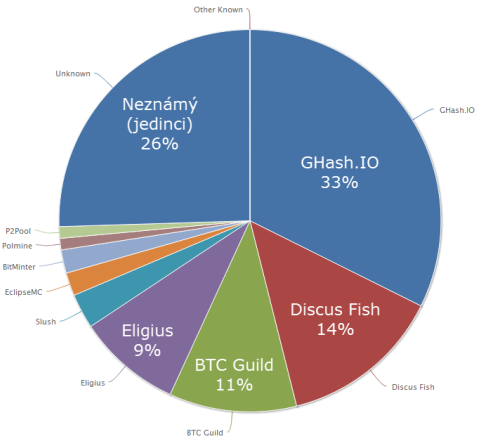
2.16.0.2 Pravděpodobnost úspěšností útoku

V Tabulce 2.17 vidíme úspěšnost proveditelnosti útoku, kde sloupec q značí kolik útočník (miner) má procentuálně výkonu celé sítě a sloupce s čísly značí počet potvrzení transakce (zanoření transakce pod novějšími bloky).

V předchozím ukázkovém příkladě 2.16.0.1 měl útočník superpočítač s 40% výkonu celé sítě. Když se koukneme na 40% podle Tabulky 2.17, tak pravděpodobnost, že útočník „vydrží“ tvořit bloky ve svém tajném řetězci rychleji než ostatní mineři (s 60% výkonem sítě) je pro první blok 80%. Pro další bloky se pravděpodobnost postupně zmenšuje.

Pokud útočník má méně než 50% výpočetního výkonu sítě, tak muže uspět v rychlejší tvorbě tajné větve jen krátkodobě. Pokud útočník má více než 50% výpočetního výkonu sítě, tak má 100% pravděpodobnost, že bude svou tajnou větev tvořit rychleji než zbytek sítě.

V praxi útočník jako jedinec má šanci uspět jen krátkodobě, protože výkon celé sítě je obrovský. Na světě se nenajde žádný superpočítač, který by mohl mít větší výpočetní výkon než 50% celkového výkonu sítě. Šanci mají jenom mining pooly. V dnešní době se bitcoiny těží především v mining poolu. Vlastník mining poolu určuje pravidla těžby nového bloku. Pokud by maining pool měl více než 50%, tak tento útok je reálný. Na Obrázku 2.18 vidíme aktuální rozdělení výpočetního výkonu sítě mezi mining pooly. Dlouhodobě mezi největší mining pooly patří GHash.IO, jehož výkon se pohybuje poslední dobou kolem 30% až 40%. Na začátku roku 2014 se jeho výkon pohyboval kolem 40% až 46%. Tento fakt ohrozil důvěru Bitcoinu, protože se zdál být reálný útok 50%. Na základě tohoto faktu majitelé zastavili registraci nových uživatelů a vydali prohlášení, že v případě dosáhnutí 50% výkonu nebudou tvořit tajný řetězec. Mineři z tohoto poolu rovněž sami dobrovolně vystoupili a přidali se k jiným poolům.



Obrázek 2.18: Rozdělení výpočetního výkonu sítě mezi minery [5]

2.16.1 Rekapitulace útoku

Kvůli tvorbě krátkodobých paralelních řetězců buď neúmyslně (kapitola 2, sekce 2.15) nebo úmyslně útokem dvojitého utracení obchodníci, kteří akceptují bitcoiny, musí čekat minimálně několik potvrzení (několik zanoření transakce pod bloky). Za bezpečné se považuje zanoření pod 6 bloky, což trvá přibližně 60 minut. V důsledku tohoto faktu nejsou bitcoiny vhodné pro okamžité platby. Obchodník může být okraden.

Tuto nepříjemnost validačního algoritmu PoW[21] banky chtějí vyřešit vlastním validačním algoritmem. Jeho logika bude popsána v další kapitole.

2.17 Úmyslné zahlcení celé sítě

Jedna se o útok, kdy útočník posílá hodně transakcí mezi svými adresami z jedné adresy na druhou. Fakticky naprogramuje robota, který produkuje miliony transakcí pro minery. Cílem této akce je zahltit platební system Bitcoinu. Toto je ošetřeno pomocí minimálního transakčního poplatku. Mineři můžou do bloku zahrnout maximálně 50 kB transakcí bez transakčních poplatků. Blok má maximální celkovou velikost 1 MB. Ostatní transakce musí mít minimální transakční poplatek. V případě, že se nevejdou do bloku, budou ve frontě v dalším bloku. Může se proto stát, že když uživatel pošle transakci bez transakčního poplatku, tak se bude potvrzovat klidně i tři dny. Počítá se s tím, že pokud útočník se rozhodne útočit transakcemi s minimálním transakčním poplatkem, tak mu bitcoiny rychle dojdou. Tento útok tedy není možný.

[21] Proof of Work

Kapitola 3

Blockchain technologie

V předchozích kapitolách jsem se zabýval decentralizovanými kryptoměnami obecně a hlavním reprezentantem decentralizovaných kryptoměn, jimž je Bitcoin. V této kapitole pracují s hlavním technologickým jádrem těchto kryptoměn, což je Blockchain.

V předchozí kapitole jsem rovněž řešil především technickou stránku Bitcoinu, na kterým je nový fenomen blockchain respektive distributed ledger stavěn. V této kapitole řeším především charakteristiky a aplikaci této technologie pro různé odvětví. Aplikace blockchainu pro tradiční finanční instituce se aktuálně vyvíjí.

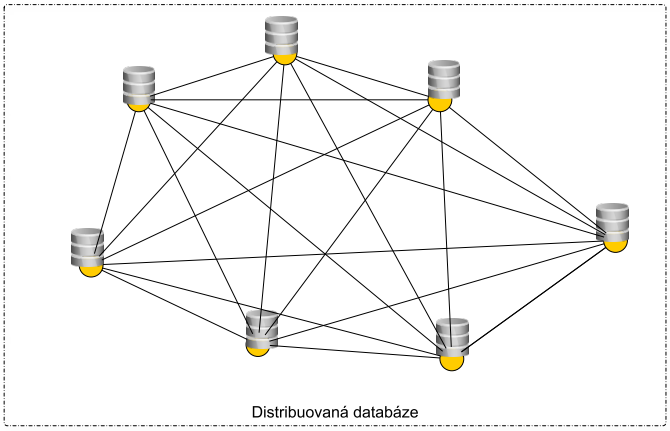
3.1 Blockchain technologie a literatura

V dnešní době pojem blockchain je distribuovaná a decentralizovaná databáze dat(ne jenom transakcí díky aplikaci v jiných odvětví). První blockchain byl implementovaný v Bitcoinu v roce 2009. Vznikl s několika stránkami dokumentace[22]. V literatuře kolem decentralizovaných kryptoměn dochází k významnému větvení výkladů a pojmu, jelikož nemají žádnou známou centrální autoritu, která by se starala o terminologií a k tomu rovněž přispívá rapidní vývoj samotných blockchainů. Blockchain téma je zkoumána paralelně velkým množstvím jednotlivců, komunitou, skupinami společností a tak dále. Nejdříve přišlo technické řešení a později terminologie jednotlivých technologických častí Bitcoinů, blockchainů. Články, dokumentace, analýzy o Bitcoinu, blockchainů na webových portálech byli napsané jednotlivci, komunitou. Později byli vydaný první knihy. Kvůli zájmu o komerční využití této technologie bankami a jinými společnostmi se začali zabývat jejich odbornici. Vytvářeli a tvořili nezávislé na sobě vlastní analýzy, zprávy, reporty, články, studie a tak dále. Autoři těchto děl se shodli v řadě pojmů, ale nebylo tomu tak úplně všude. Je potřeba tedy literaturu kolem blockchainů brát s rezervou. Kvůli

[22] https://bitcoin.org/bitcoin.pdf

aktuálnímu, rapidnímu vývoji blockchainů se některé věci rychle mění. Popisy vlastností, terminologie co jsou v jedné analýze nemusí byt stejné ve druhé.

V následujících kapitolách jsem především vycházel z různých analýz poradenských společností jako jsou Deloitte, Pwc, Accenture, Gartner a dalších. Rovněž jsem vycházel z různých analýz tradičních finanční instituci jako jsou UniCredit bank, Credit Suisse a dalších. Knihy kolem blockchain technologií bohužel nejsou vhodné, protože nedokáží zachytnout, tak rapidně rychlý vývoj blockchainů.



Obrázek 3.1: Distribuovaná databáze v sití

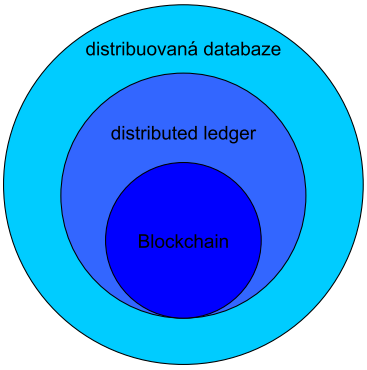
3.2 Distribuovaná databáze

V různých informačních zdrojích lze nalézt různé definice distribuované databáze. Obecně si lze představit distribuovanou databázi jako rozkopírovanou jednu a tutéž databázi o identickým obsahu dat, která je uložena na více výpočetních uzlech v počítačové síti. Na obrázku 3.1 je znázorněna distribuovaná databáze o 7 stejných instancích. Mezi výhody distribuované databáze například patří:

- Výkon
- Spolehlivost
- Škálovatelnost
- Dostupnost

Celý fenomen Blockchain vychází ze speciálního případu distribuované databáze. Blockchain se zabývá neřešitelným problémem u distribuovaných systému - „two generals' problem“. Je to v informatice teoretický myšlenkový

experiment, který dokazuje nedosažitelnou jistotu dvou subjektů domluvit se na společné akci přes nespolehlivý komunikační kanál. V případě blockchainu je tato akce validace či ověření transakce. Blockchain má díky objeveným validačním algoritmům vysokou odolnost proti chybám korektní domluvy či ověření transakce[23].



Obrázek 3.2: Blockchain je specifická distribuovaná databaze dat

3.3 Blockchain a Distributed ledger

Blockchain je distribuovaná a decentralizovaná databáze dat. V případě kryptoměn tato databáze obsahuje veškeré dosud provedené transakce v dané platební síti. Důvodem proč již nelze v dnešní době považovat pod pojmem blockchain pouze distribuovanou a decentralizovanou databázi transakci je ten, že se postupně nacházejí jiné možností aplikace této databáze(mimo finanční sektor). Potom tato databáze obsahuje jiná data než data o provedených transakcích v platební síti(viz. dále případy užíti blockchainu pro různé odvětví).

Z výše uvedeného důvodu se objevil nový pojem distributed ledger(někdy rovněž shared ledger), který je definován jako konsensus replikovaných, sdílených a synchronizovaných digitálních dat geograficky rozmístěných v různých místech, státech nebo institucí [25]. Blockchain je tedy podmnožinou distributed ledger viz. Obrázek 3.2. Distributed ledger je tedy pojmem konkretizovaného blockchainů pro bankovnictví obohacený o vlastností jako je možnost regulace a podobně. Banky ve svých studiích, analýzách používají oba dva termíny ve stejným kontextu. Můžeme tedy říci, že jsou si navzájem zaměnitelné. Pojem distributed ledger je nový a objevuje se v roce 2015 a 2016 v různých zprávách, analýzách apod. především od bank. Banky se snaží poměrně často prezentovat distributed ledger jako svůj privátní bankovní blockchain, ale není

[23]high byzantine fault tolerance

tomu vždy tak.

3.4 Historie vývoje Blockchain technologií

Vývoj blockchain technologií prošel určitými fázemi. Tyto jednotlivé fáze zde popíšu:

3.4.1 Blockchain 1.0 - Bitcoin

V roce 2009 vznikl Bitcoin a s tím spolu první blockchain. Postupně na bázi Bitcoinů vznikli další decentralizované kryptoměny altcoins[24] jako je Litecoin, Dogecoin a další. Všechny tyto decentralizované kryptoměny měli praktický stejné funkční vlastností, nebo-li respektive jejích technologické jádro - blockchain měl stejné vlastností. Tento blockchain dostal v literatuře přiřazenou verzi 1.0. Pod touto verzi se v literatuře blockchain představuje jako decentralizovaná kryptoměnová databáze transakcí se základními vlastnostmi blockchainů Bitcoin.

3.4.2 Blockchain 2.0 - Smart kontrakty

Postupem času vznikla v roce 2015 nová decentralizovaná kryptoměna Ethereum, která oproti předešlým kryptoměnam měla obohacený blockchain o smart kontrakty. Smart kontrakty[25] se považuje za revoluční benefit v blockchainu a proto tento blockchain dostal v literatuře přiřazenou verzi 2.0. Smart contracts budou popsány dále.

3.4.3 Blockchain 3.0 - Aplikace

Pod verzi blockchain 3.0 se považují aplikace této technologie, jak pro finanční sektor, tak i mimo finanční sektor. Blockchain totiž je distribuovaná databaze dat, do které jakmile se nová data přidají, tak nelze je změnit. Táto vlastnost má obrovský potenciál. Data totiž nemusí byt nutně transakce, ale můžou to byt například digitální občanské průkazy, volební lístky a podobně. Další případy užíti budou popsány dále.

Komerční společností, vlády a jiné subjekty se všimli fenomenu blockchain a jeho vlastností. Chtějí aplikovat blockchain pro své potřeby. Dochází zde k rozdělení blockchainů na permissioned a permissionless[26], které budou popsány dále.

[24] Alternate cryptocurrencies
[25] Český v překladu - „chytré kontakty“
[26] Český v překladu - „s oprávněním a bez oprávnění“

3.5 Smart kontrakty

3.5.1 historie

Smart kontrakt[27] byl objeven počítačovým vědcem Nickem Szabo již v roce 1994, ale plně praktického využíti se dočkal až v roce 2015 se vznikem decentralizované kryptoměny Ethereum. Tato vlastnost byla implementována v blockchainu kryptoměny Ethereum, která byla spuštěna v červnu roku 2015. Její prostředek finanční směny je ether.

3.5.2 definice podle Nicka Szabo

Smart contract je počítačový transakční protokol, který vykonává podmínky kontraktu(smlouvy). Obecným cílem je uspokojit běžné smluvní podmínky (například platební podmínky, zástavy, vymáhaní,..), minimalizovat výjimky jak zlomyslné, tak náhodné a minimalizovat potřebu důvěryhodných zprostředkovatelů kontraktu. Související ekonomické cíle zahrnují snížení ztráty kvůli podvodům, arbitráži, nákladu na vymáhání podle právních předpisů a ostatní transakční náklady.[26]

3.5.3 Princip fungováni smart contracts v Ethereum

Smart contract je reprezentován zdrojovým kódem[28], který se následně nahraje do blockchainu Ethereum kryptoměny a tím i speciálního virtuálního stroje, který vykoná kód. U tohoto kontraktu je garantováno výpočetní sítí kryptoměny, že bude proveden dle podmínek jeho zdrojového kódu, který je dostupný ve veřejným blockchainu.

3.5.4 Příklad smart kontraktu

Franta chce prodat notebook Pepovi poštou. Znají se mezi sebou na základě inzerce o prodeji notebooku. Franta chce za notebook 1000 etheru, zatímco Pepa chce od Franty funkční notebook. Definujeme tuto záležitost jako nezávislou transakci X.

Kontrakt umožní dvěma samostatným uživatelům vložit na účet kontraktu částku 5000 etherů, dohromady tedy 10000 etherů sloužících jako jistina. Tuto částku poté uživatelům vrátí pouze v případě, že oba potvrdí úspěšné uskutečnění na kontraktu nezávislé transakce X.

Poté co oba tuto částku uhradí na účet kontraktu, dá tento kontrakt oběma uživatelům vědět, že obdržel jistinu. Nyní mohou provést nezávislou transakci X.

[27] Český chytré(inteligentní) kontrakty, smlouvy

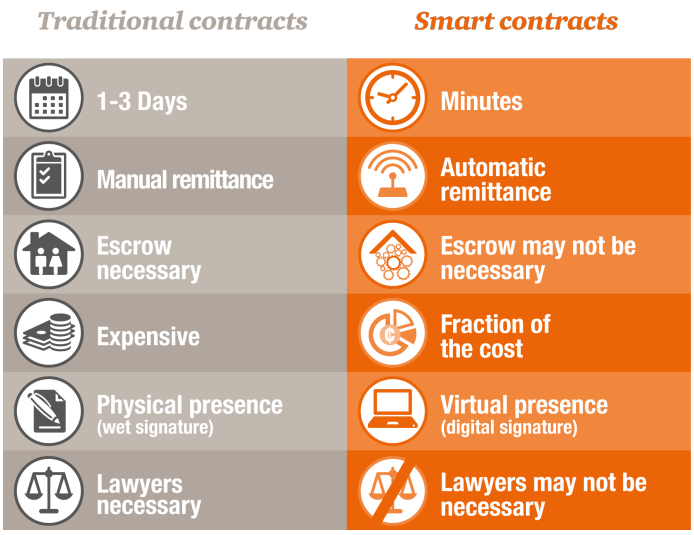
[28] Postup jak naprogramovat jednoduchý kontrakt je popsán zde: `https://www.ethereum.org/greeter`

Pokud nezávislá transakce X proběhne v pořádku, oba uživatelé dají kontraktu vědět, že transakce proběhla v pořádku. V tom případě jim oběma kontrakt vrátí vložené ethery, které byly předtím zaslány na jeho účet.

Jestliže však nezávislá transakce X proběhne špatně, například kupující se pokusí okrást prodávajícího, nebo naopak, kontrakt ethery nevyplatí a po nějaké době je převede na svůj speciální účet. Oba dva uživatelé tedy přijdou o veškeré vložené ethery do smart kontraktu.

Pokud je vložená částka do smart kontraktu větší, než předpokládaná hodnota nezávislé transakce X, oba jsou ekonomicky motivováni transakci provést korektně. Tím je zajištěna sebe-vymahatelnost kontraktu. Kontrakt navíc sponzoruje Ethereum, nebot' v případě propadnutí, tak ethery jdou znovu do oběhu.

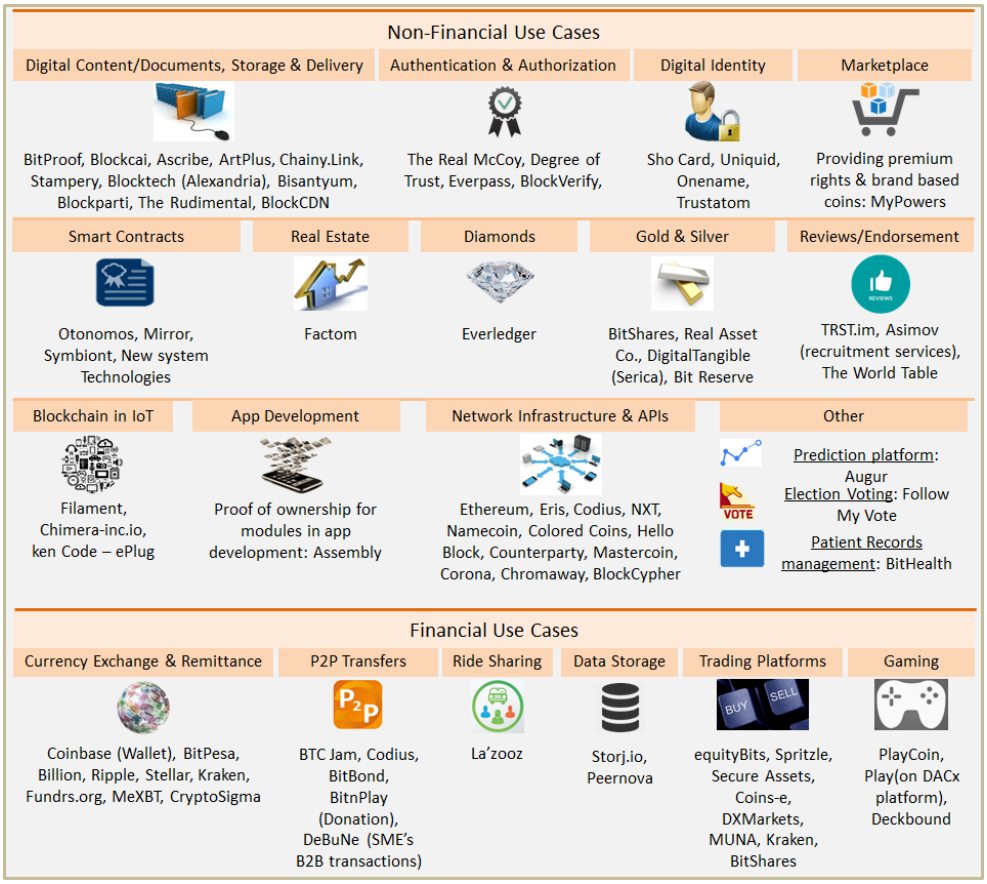
Výše uvedený kontrakt se dá chápat jako nástroj k navázání důvěry ve výši složené částky, mezi jinak nedůvěryhodnými stranami v nedůvěryhodném prostředí. Každá ze stran může důvěřovat do úrovně složené částky, že druhá strana má zájem transakci korektně dokončit a získat zpět záruku, kterou poskytla na korektní provedení transakce.



Obrázek 3.3: Shrnutí výhod smart kontraktu oproti tradičním kontraktum[10]

3.5.5 Výhody smart kontraktu

Na Obrázku 3.3 vidíme řadu hlavních výhod smart kontraktu oproti tradičním. Především je to minimalizace právních tahanic a s tím spojené snížení nákladu na právní kancelář a další výhody.



Obrázek 3.4: Přehled případu užití blockchain technologií ve finančním i mimo finanční sektor[1]

3.6 Případy užíti blockchain technologie[1]

V posledních letech se objevilo poměrně hodně nových případu užití blockchain technologií napříč různými obory. Některé jsou již zrealizované jiné čekají na realizací. Na Obrázku 3.4 můžeme vidět některé případy užití blockchainů. Případy užití blockchainů jsou v prvé řadě rozvinuté ve finančním sektoru. V poslední době dochází k intenzivnímu rozvoji i v případech užití mimo finanční sektor. Aplikaci blockchainu mimo finanční sektor se především zabývají startupy[29] ve FinTech[30] sféře. Celé „kouzlo“ blockchainu spočívá v tom, že používá decentralizovanou a distribuovanou databází s validačním(konsensus) algoritmem. Pokud validatoří ověří nějaký nový kus dat(např. transakce, do-

[29]podnikatelský subjekt, typicky popsán jako nově založená či začínající společnost a rychle se vyvíjející a měnící společnost. V současné době neexistuje jedna ucelená, mezinárodně uznávaná definice startupu. Kolem blockchainů vzniká spousta nových startupu, které chtějí aplikovat tuto technologií především ve finančním sektoru, ale i ostatních odvětvích.

[30]Financial technology

kumenty, a tak dále) validačním algoritmem v síti, tak tento kus dat zůstane natrvalo v blockchainu respektive v každé instanci distribuované databáze v síti. Typy validačních algoritmu jsou popsaný dále v sekci „Základní druhy blockchainů“.

Popíšu, zde krátce některé aplikace blockchainů:

3.6.1 Everledger - diamanty

Společnost poskytuje blockchain pro identifikaci diamantu a ověřování transakcí pro různé zainteresované strany (od pojišťoven až k různých bezpečnostních firmám kolem diamantu).

3.6.2 Factom - správa dat databázi

Factom používá blockchain pro správu databazi a datových statistik k podpoře různých aplikaci.

3.6.3 The Real Asset company - komodity

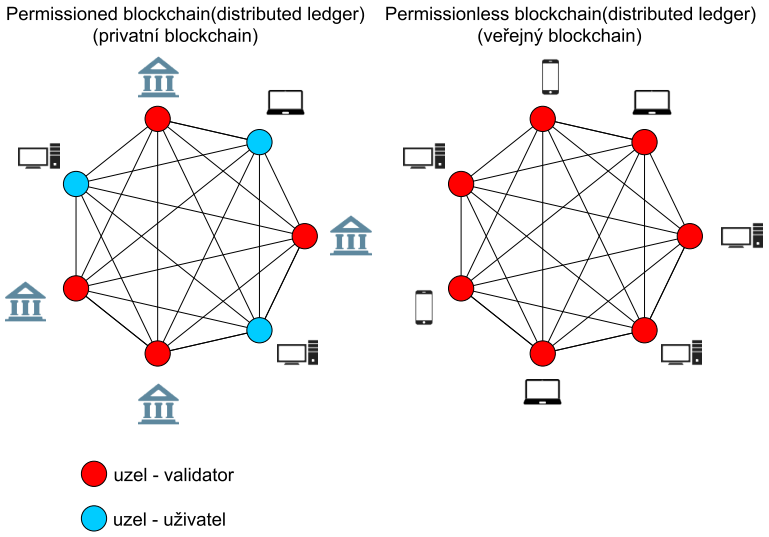
The Real Asset company poskytuje úspory komodit pomocí blockchainu.

3.6.4 Blockchain and digital content

Ascribe pomáhá umělcům a tvůrcům přisuzovat digitálního umění pomocí svého blockchainu.

3.6.5 Komentář k případu užití

Dalo by se říci, že blockchainy ve finančním sektoru validují především finanční prostředky, transakce. Naopak mimo finanční sektor je to především validace digitální identity, statistických dat a jiných důležitých dat(digitální hlasovací lístky pro volby a podobně).



Obrázek 3.5: Permissioned a Permissionless blockchain(distributed ledger)

3.7 Základní druhy blockchainů

Aktuálně blockchainy můžeme rozdělit na dva základní typy podle toho, kdo může provádět validaci(ověřovaní) transakcí v sítí:

- **Permissionless blockchain** - provádět či přispět k validačnímu procesu může kdokoliv v síti
- **Permissioned blockchain** - provádět validaci můžou pouze předem vybraní uzly v sítí(podsit' jako centrální autorita)

Na Obrázku 3.5 máme znázorněny oba dva zmíněné blockchainy. U permissioned blockchainu vidíme podsíť, která tvoří centrální autoritu. Mají především právo validace transakce, ale můžou mít i další práva.

Další rozdělení je podle toho, kdo může číst a vytvořit transakcí v blockchainu:

- **Veřejný blockchain** - číst a vytvořit transakcí v blockchainu může kdokoliv
- **Privatní blockchain** - číst a vytvořit transakcí v blockchainu můžou jen vlastnící tohoto blockchainu(podsit' jako centrální autorita)

V literatuře je toto rozdělení poměrně často zmatené. Někteří píšou o permissioned blockchainů jako by byl automaticky veřejný a podobně. Je tedy nutno toto rozdělení brát s rezervou. Nejdůležitějším rozdělením je jistě to první, které krátce rozebereme dále.

3.7.1 Permissionless blockchain

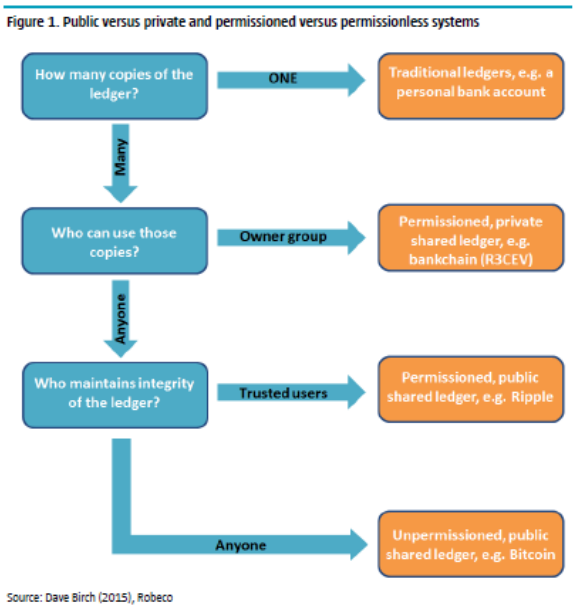
Permissioneless blockchain je používaný ve většině dnešních svobodných kryptoměnach jako je Bitcoin, Litecoin, Ethereum a spousta dalších. Většina sítě validuje či ověřuje transakce. Každý má právo se podílet na validaci. V minulé kapitole 2 jsem podrobně popsal jak tento blockchain běží na Bitcoinu. Všechny tyto blockchainy jsou veřejné, nebot' pro zakladatelé každé takové svobodné kryptoměny je důležitá důvěra a ta vzniká díky svobodnému prohlížení obsahu blockchainů.

3.7.2 Permissioned blockchain

Permssioned blockchain je novější druh blockchainů, který pravě cílí především na bankovnictví a aplikace u komerčních firem. Tyto blockchainy jsou požadovány spíše jako privátní, aby obsah mohli vidět jenom autorizované subjekty. Z prvních kryptoměn s permissioned blockchainem lze považovat Ripple. Aktuálně probíhá intenzivní výzkum těchto blockchainu. Poptávka po permissioned blockchainu vznikla na základě požadavku od tradičních finančních společností, které nemohli byt uspokojeny předchozím permissionless blockchainem.

3.7.3 Rekapitulace rozdělení blockchainů

Na Obrázku 3.6 vidíme přehledně situaci kolem rozdělení blockchainů.



Obrázek 3.6: Kombinace privatních, veřejných, permissioned, permissionless blockchainů v praxi[11]

3.8 Srovnání vlastností permissioned a permissionless blockchainu

V této sekci srovnávám základní rozdílné charakteristiky permissioned a permissionless blockchainu, které jsou přehledně v tabulce 3.1

	Permissioned blockchain	**Permissionless blockchain**
Přístup	autorizovaný	volný
Regulace	ano	není
Validator	podsít'	kdokoliv
Identita	identifikovaná	pseudoanonymní
Rychlost potvrzení	rychlá	pomalá
Algortimus validace	vlastní	PoW, PoS
příklady blockchainů	Ripple, R3 Corda,..	Bitcoin, Litecoin,..

Tabulka 3.1: Přehled zakladních rozdilných vlastností permissioned a permissionless blockchainu

3.8.1 Přistup

Permissionless blockchainy jsou téměř všechny veřejné. Každý může vytvořit transakcí v peněžence a odeslat jí do sítě a rovněž prohlédnout si obsah blockchainu.

Zatímco permissioned blockchainy jsou požadovaný spíše naopak privátní, a to kvůli legislativě, ochrany osobních udaju a podobně. V případě u tradičních bank jsou to přísné regulace od centrálních bank.

3.8.2 Regulace

Bankovní regulace jako je například AML[31] a KYC[32] jsou praktický neproveditelné u stávajících permissionless blockchainů.

Centrální banky se staví pozitivněji k privátním permissioned blockchainům, u kterých se regulace dají lepé splnit.[27]. Popíšu tyto základní regulace:

3.8.2.1 Know your customer - KYC

Pojem „Know your customer“, nebo-li česky „poznej svého klienta“ se vyskytuje u finančních instituci, které nakládají s finančními prostředky svých klientu. Především se tento termín tyká regulace u bank.Každá banka má povinnost dostatečně identifikovat svého klienta před prováděním finanční operace klienta.

[31] Anti-money Laundering
[32] Know your customer

„Povinnost zjišťovat totožnost osob, se kterými banka vstupuje do smluvních vztahů, je dána legislativně. Základní právní normou je zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti. Dohled nad dodržováním stanovených pravidel provádí regulátor, tedy Česká národní banka.“[28]

3.8.2.2 Anti money laundering - AML

Pojem „Anti money laundering“, nebo-li česky „praní špinavých peněz“ se jedná o regulační pojem u bank. AML je definováno jako jednání sledující zastření nezákonného původu peněz s cílem vzbudit dojem, že se jedná o peníze nabyté legálně.[28]

3.8.3 Identita

Identita v permissionless blockchainech je pseudoanonymní, jelikož jsou aktuálně všechny tyto blockachiny veřejné. Každý se může podívat na obsah jakékoliv adresy či učtu v blockchainu. Například na zůstatek, provedené transakce adresou a podobně. Sice adresa nemá žádné uvedené iniciály, ale můžou si určitým způsobem vystopovat. Příklad jsem popsal v minule kapitole 2 v sekci 2.12. První zcela anonymní permissionless blockchain lze považovat u kryptoměny zCash, která byla vytvořena v listopadu 2016.

Banky u vlastního permissioned blockchainů musí zajistit, aby každý klient byl u blockchainu jednoznačně identifikován kvůli legislativě, regulacím. Zároveň by měli taky zajistit, aby se identita nedostala k neautorizovaným osobám.

3.8.4 Rychlost potvrzení

Aktuálně mezibankovní potvrzení transakce trvají u tradičních bank i několik dní. U permissionless blockchainu, který je například implementovaný v Bitcoinu trvá potvrzení transakce 60 minut viz. předchozí kapitola 2 sekce 2.15.1. Jsou již permissionless blockchainy, které mají rychlejší algoritmus validace.

U permissioned blockainů se očekavá ještě rychlejší potvrzení transakce díky velikosti menší validační podsítě a vlastního naimplementovaného algoritmu validace. Očekává se blesková rychlost potvrzení transakce.

3.8.5 Algortimus validace

Algoritmus validace, nebo-li také konsensus algoritmus je algoritmus, který řeší ověření transakce, tak aby nedošlo k dvojitému utracení finančních prostředku v blockchainů. Permissionless blockchainy mají dva základní algoritmy:

- Proof of Work
- Proof of Stake

Zatímco permissioned blockchain má vlastní naimplementovaný algoritmus. Všechny tyto algoritmy jsou zde zmíněny:

3.8.5.1 Proof of Work

Tento algoritmus je implementovaný v blockchainu u Bitcoinu a v řadě dalších permissionless blockchainů. Podrobně jsem jej popsal v minulé kapitole 2 sekci 2.14.

Validace(ověření) transakce proběhne na základě prokázaného vlastnictví výpočetního výkonu v platební sítí.

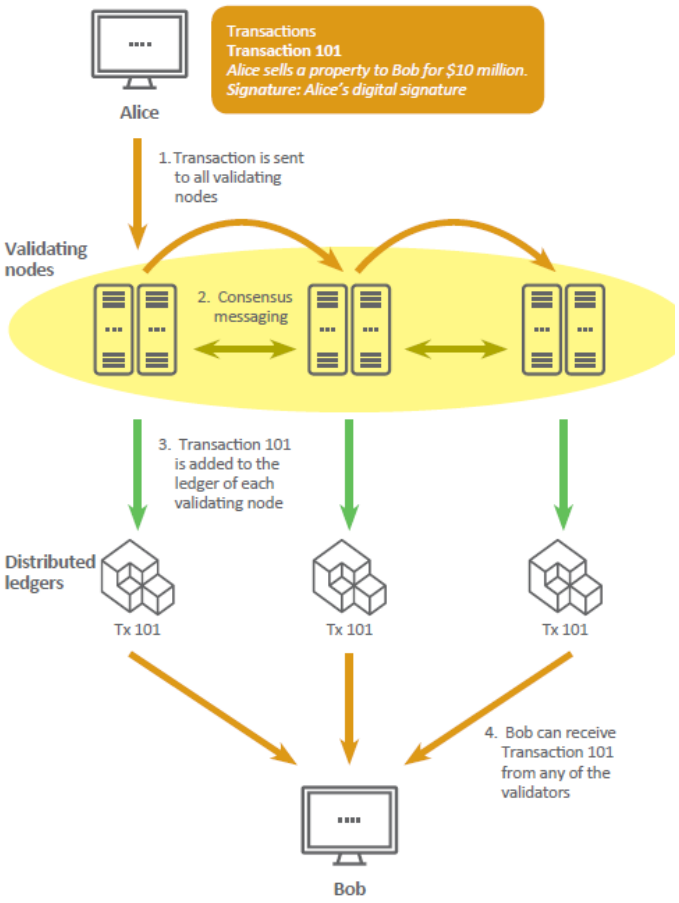
3.8.5.2 Proof of Stake

Tento algoritmus je implementovaný například v Peercoinu. Validace(ověření) transakce proběhne na základě prokázání vlastnictví podílu kryptoměny.

3.8.5.3 Vlastní algoritmus validace

U obou předchozích algoritmu může dojít k takzvanému 51% útoku, kdy vlastník vlastní víc jak 51% kryptoměny či výpočetního výkonu získává možnost falšovat či upravovat transakce.

Permissioned blockchain bude mít vlastní algoritmus validace, kde ověřovat transakce bude podsít' validačních uzlu, která bude tvořit určitou centralizaci. Každý tento uzel bude vlastnit důvěryhodná autorita. Aktuálně tento algoritmus je implementovaný u komerční kryptoměny Ripple. Na obrázku 4.5 vidíme znázorněný princip, jak by to mohlo fungovat u bankovních blockchainů.



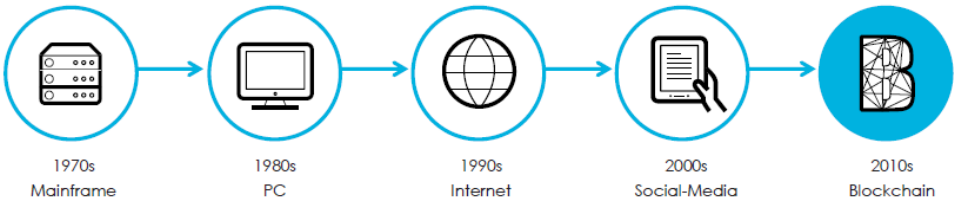
Obrázek 3.7: Vlastní algoritmus validace u permissioned blockchainů[12]

Kapitola 4

Blockchain v bankovnictví

V minulé kapitole jsem popsal revoluční technologický fenomén blockchain, který zasahuje do mnoha finančních i nefinančních oboru. Některé aplikace blockchainu byli již zrealizovaný, ale spousta dalších ještě realizace nenabyla a nacházejí se další potenciální aplikace.

V této kapitole se zabývám konkretní aplikaci blockchainů, a to pro bankovnictví. Jedná se především o architekturu privátních permissioned blockchainů se smart kontrakty.

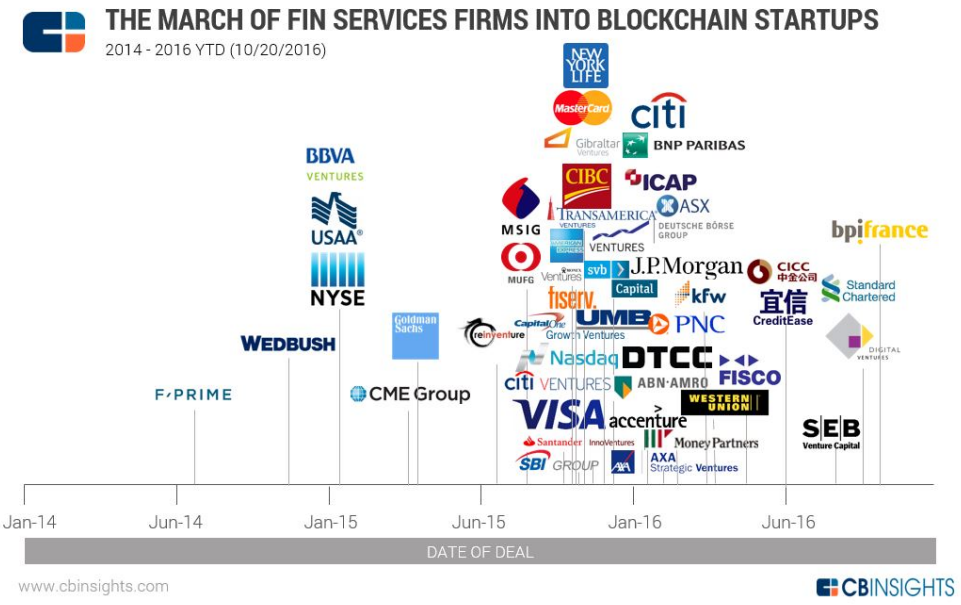


Obrázek 4.1: Disruptive technogies, které změnili svět[13]

4.1 Bankovnictví a technologie

Vynález telegrafů a železnice způsobil revoluci obchodu v 19. století. Následně komunikační a dopravní systémy se stále vyvíjely a společně dělali svět menší a menší rok co rokem. Finanční svět využil přínos rozvíjející se technologie a obchodování se stalo rychlejším a jednodušším než kdy bylo předtím. V 70 letech 19.století proběhla revoluce počítačů a obchodní platformy a účetní systémy se prudce posunuli od postupů na papíru, které se prováděli od dob, kdy byl papír vynalezen.
Někdo by si myslel, že vývoj komunikačních systémů dosáhl pravě svého vrcholu, kdy se mobilní telefony začaly objevovat v ulicích na začátku 90 let 20

století. Internet změnil společnost, včetně finančních systémů a obchodování takovým způsobem, který nebylo možné předpovídat jen před několika desetiletími. Nyní blockchainy nabírají své první kroky, které by mohly skončit působením dramatických změn v každodenním životě lidí a fungování finančních trhů.
Finanční instituce předpokládají, že utratí více než 1 bilion dolarů do blockchain projektů v roce 2017. [29] Tímto krokem by udělali jeden z nejrychlejších se rozvíjejících podnikového softwaru všech dob. Znamená to, že se něco děje. Možná, že se nejvíce ambiciózní scénáře nestanou realitou, ale zdá se pravděpodobně, že uvidíme mnoho zlepšení v efektivnosti trhů a obchodování, stejně tak, jako nové služby poskytované zákazníkům, a to díky blockchainům.
Na Obrázku 4.1 vidíme přehled některých disruptive technology[33]



Obrázek 4.2: Investice do blockchain technologií[14]

4.2 Investice a vývoj bankovních blockchainů

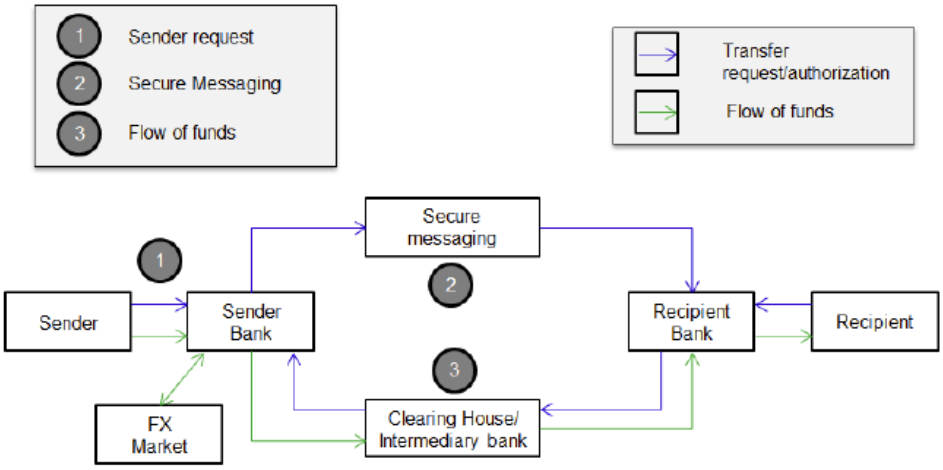
Aktuálně bankovní blockchainy vyvíjejí interně jednak banky a dále FinTech[34] společností, kde se většinou jedna o technologické startupy[35]. Banky mají bo-

[33]Distruptive technologie je technologie, která vytěsňuje zavedené technologie a vytváří zcela nové průmyslové odvětví.

[34]Financial technology - fintech je akronym pro Financial technology. Jedna se průmyslové odvětví věnující se inovacím ve finančním sektoru.

[35] podnikatelský subjekt, typicky popsán jako nově založená či začínající společnost a rychle se vyvíjející a měnící společnost. V současné době neexistuje jedna ucelená, meziná-

haté zkušeností s legislativou, regulacemi kolem financí a mají potřebný kapitál pro rozjezd vývoje, zatímco startupy mají především silné zázemí technologické kryté odborníky. Vzniká tedy spolupráce mezi bankami a FinTech startupy, protože každý si navzájem může něco nabídnout.
Investice finančních instituci do Blockchain startupu v roce 2016 se odhadují na více než 1 bilion amerických dolaru.[29] Na Obrázku 4.2 vidíme jednotlivé finanční instituce, které investují do startupu kolem blockchain technologií podle časové osy.
Největším projektem kolem bankovních blockchainů je R3 Corda blockchain, který bude popsán později.



Obrázek 4.3: Aktuální transakční systémy u tradičních bank[15]

4.3 Jak fungují mezibankovní transakce dnes?

Pro lepší pochopení potenciálu blockchainu pro bankovnictví je nejlépe se prvně zaměřit na stávající situaci mezibankovních plateb u tradičních bank. Na Obrázku 4.3 vidíme názorně jak to funguje dnes. Z tohoto obrázku je patrné, že banky spoléhají na zprostředkovatele jako je například Česká centrální banka v případě vnitrostátních transakcí v ČR nebo SWIFT[36].[15]. Provedení zúčtování probíhá v řadu dnů a musí byt rovněž zaplaceno zprostředkovatelům, což jsou negativa, která vytváří řadu dalších negativ. Popíšu krátce dva zmíněné subjekty v rámci zprostředkovaní plateb:

rodně uznávaná definice startupu. Kolem blockchainů vzniká spousta nových startupu, které chtějí aplikovat tuto technologií především ve finančním sektoru, ale i ostatních odvětvích.

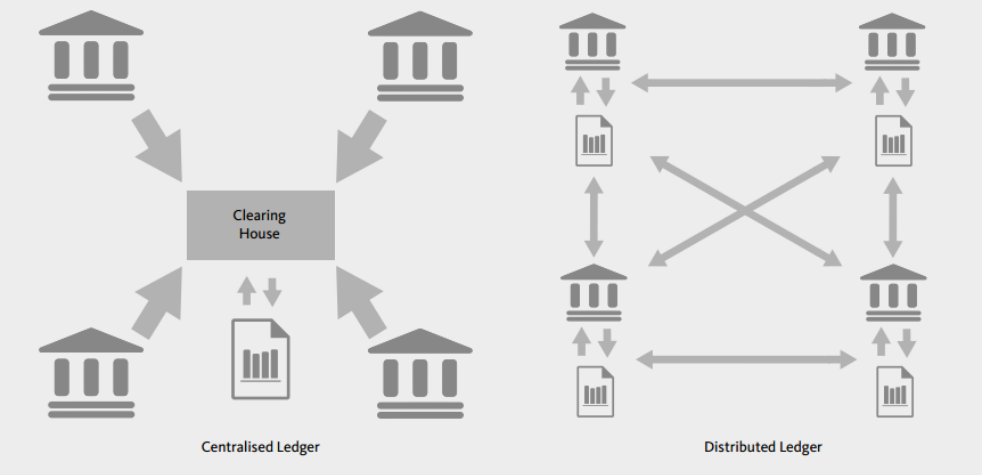
[36]Society for Worldwide Interbank Financial Telecommunication

4.3.1 Česká centrální banka

„Jediným systémem mezibankovního platebního styku v České republice, který zpracovává mezibankovní platby v českých korunách, je systém CERTIS (Czech Express Real Time Interbank Gross Settlement system). CERTIS zahájil provoz v rámci zúčtovacího centra SBČS v bývalém Československu 8. března 1992. Po rozdělení Československa počátkem roku 1993 bylo na Slovensku vytvořeno nové zúčtovací centrum, zatímco bývalé federální zúčtovací centrum zůstalo v ČNB.“[30].
Na Obrázku 4.3 je označen jako „Clearing house“.

4.3.2 SWIFT

„Společnost pro celosvětovou mezibankovní finanční komunikaci) slouží zejména k mezinárodnímu platebnímu styku. V rámci SWIFTu má každá zúčastněná banka svůj jedinečný kód(BIC), kterým se identifikuje. Tento systém běží od roku 1973.“[30]
Na Obrázku 4.3 je označen jako „Secure messaging“.



Obrázek 4.4: Srovnání dnešního a budoucího stavu platební sítě bank[16]

4.4 Budoucnost mezibankovních plateb

Budoucnost mezibankovních plateb banky vidí především v privátních, permissioned blockchainech, kde centrální autorita bude tvořena jako podsíť tradičních bank validátoru, ale případně i dalších finančních institucí. Obrázek 4.4 znázorňuje vizi bank.

Dále se zabývám SWOT analýzou privátního, permissioned blockchainu se smart kontrakty pro bankovnictví z pohledu, co všechno přinese pro toto odvětví oproti současnému tradičnímu bankovnímu systému.

4.4.1 Co je to SWOT analýza?

„SWOT analýza je univerzální analytická technika zaměřená na zhodnocení vnitřních a vnějších faktorů ovlivňujících úspěšnost organizace nebo nějakého konkrétního záměru (například nového produktu či služby).“[31]

Obrázek 4.5: SWOT analýza permissioned blockchainu pro bankovnictví

4.4.2 Silné stránky

Banky nebudou mít zprostředkovatele v rámci směny, což nese řadu pozitiv. Například nebudou muset spoléhat na důvěru cizích služeb zprostředkovatele. Ušetří na transakčních poplatcích a tím rovněž svým klientům. Rychlost transakcí bude blesková díky technologií blockchainu. Zároveň v síti budou moci použít smart kontrakty, které budou zajišťovat vymahatelnost a tím rovněž ušetří na právních sporech. Nebudou mít „single point of failure“[37] a tím tedy bude větší odolnost proti například DoS útokům. Blockchain nabídne bankám vysokou kvalitu dat, kterou nepůjde jednoduše zfalšovat.

4.4.3 Příležitostí

Permissioned blockchain může nabídnout v bankovnictví naopak lepší mechanismy v boji proti praní špinavých peněz a podobně. Centrální banky naopak

[37] Jedná se o část systému, který propojuje v něm všechny subjekty. Když spadne, tak se zhroutí celý tento systém

se staví permissioned oproti permissionless blockchainu pozitivně.[27]

4.4.4 Slabé stránky

Banky můžou vytvářet díky blockchainů monopol, což je jedna z forem nedokonalé konkurence. Ostatní banky, kteří nebudou mít přistup do blockchainů z nějakých důvodu budou v nevyhodě.

Banka bude muset dodržovat pravidla většiny sítě validátoru.

4.4.5 Hrozby

Hrozbami jsou obrovské investiční náklady do blockchain technologií, které zatím stále nejsou zrealizovaný.

Blockchain je nová technologie. Je tu riziko, že se může něco v praxi pokazit.

4.5 První bankovní blockchainy v praxi

Obrázek 4.6: R3 Corda blockchain a jeho validatoří[17]

4.5.1 R3 consortium

Jedna se o konsorcium finančních institucí, které bylo založeno v roce 2014 Davidem Rutterem. K datu březen 2016 se skládálo z 42 předních finančních instituci (převážně bank) viz. Obrázek **??**. Cílem tohoto konsorcia je výzkum a vývoj Blockchainové technologie. Dne 3. března 2016 bylo provedené první větší testovaní Blockchainu se zapojením všech účastníku konsorcia.[17]

4.6 Vyjádření významných členu R3

Každý člen konsorcia R3 si slibuje velké přínosy od Blockchain technologie. Zde shrnu několik veřejných vyjádření k Blockchainu od několika vyznaných členu tohoto konsorcia.

4.6.1 Goldman Sachs

„„Co když bychom vám řekli, že bitcoin jen otevírá něco dalšího... jen přivádí blockchain do centra pozornosti," uvedla v prosincové poznámce investiční banka Goldman Sachs a dodala, že by tato technologie mohla „změnit všechno." Goldman Sachs také vyjmenovala řadu průmyslových odvětví, které by blockchain mohly používat – ať už jde o hlasovací systémy, registraci vozidel, poplatky, kontroly zbraní či katalogizaci vlastnictví uměleckých děl. „Odstraní se potřeba prostředníka, což snižuje potenciální bezpečnostní obavy, ale také částečně ničí korupční prostředí. Urychluje manuální procesy, které jsou zastaralé a trvají příliš dlouho," dodala investiční banka."[32]

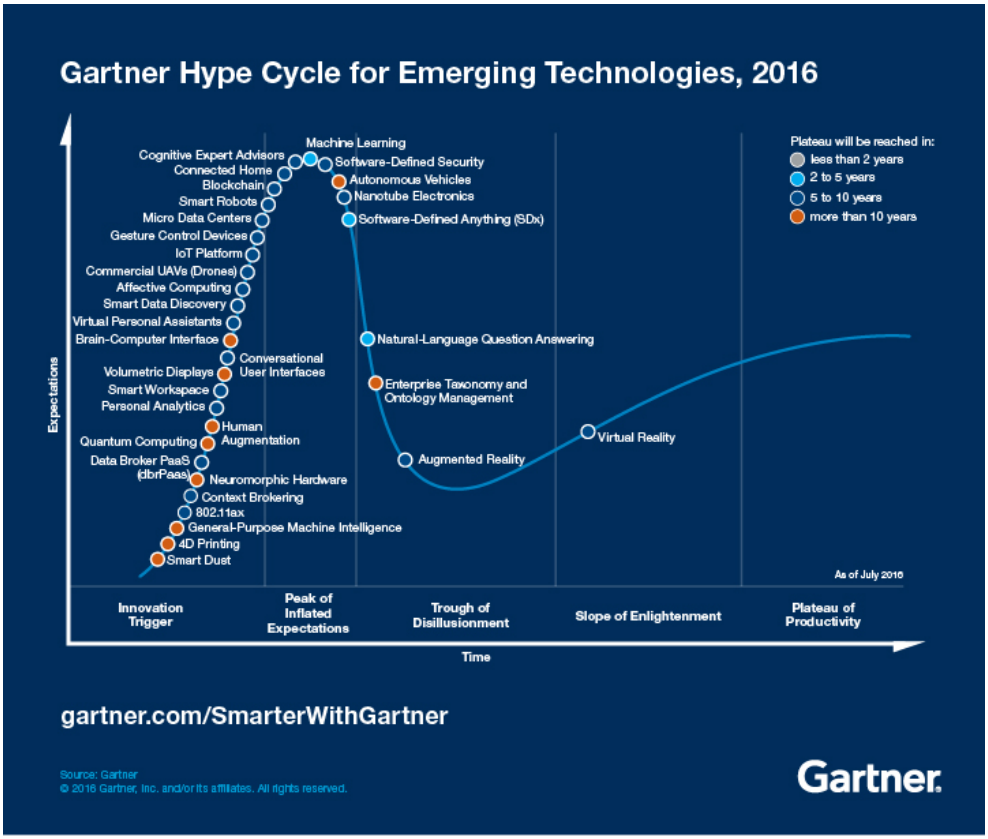
4.6.2 JPMorgan

„JPMorgan v loňském roce investovala do technologií asi 9 miliard dolarů, zejména s důrazem na blockchain. Daniel Pinto, ředitel korporátní a investiční banky JPMorgan, poznamenal, že finanční gigant zřídil speciální týmy, který se budou zaměřovat na blockchain, ale i další technologické oblasti, jako například robotiku."[32]

4.6.3 UBS

„UBS je jednou z nejotevřenějších bank, co se plánů s technologií blockchain týká. Pod názvem „Crypto 2,0" provádí výzkum této technologie. Švýcarská investiční banka uvedla, že prozkoumala více než 20 možností využití blockchain a inkubuje nejlepší nápady. Jedním z těchto nápadů je využití v oblasti vydávání dluhopisů, výpočtu úroků, kupónových plateb atd. UBS dodává, že v tomto scénáři není třeba zprostředkovatele obchodu. Software by byl specificky konfigurován a automaticky by zpracovával tok informací a peněz mezi vydavatelem a kupujícím."[32]

4.7 Prognózy poradenských společností



Obrázek 4.7: Hype Cycle for Emerging Technologies 2016[18]

4.7.1 Gartner Hype Cycle

Gartner je uznávaná společnost, která se věnuje poradenství v oblastí IT služeb. Každý rok aktualizuje křivku „Hype cycle“. Jedna se o křivku, která popisuje životní cestu technologie. Křivka má pět stadii zralosti viz. obrázek 4.7. Podle této křivky se technologie narodí za 5 až 10 let(Plateau of produktivity). Bude tedy zrát(vyvíjet) ještě 5 - 10 let.

4.8 Shrnutí potenciálů blockchainu v bankovnictví

Na základě získaných poznatku můžu dospět, že blockchain technologie má sama o sobě velký potenciál a přinejmenším v některých částech trhu způsobí revoluci ve fungování stávajícího finančního světa. Mezi hlavní výhody této technologie patří zvýšená efektivita, úspory nákladů, bezpečnost a příležitost pro lepší monitoring trhů s regulačními úřady v případě permissioned blockchainů. „Smart kontrakty“ mohou poskytnout automatizované řešení v situacích, kde je menší potřeba mít důvěru mezi protistranami, což znamená snížení rizika protistrany a umožňuje nový typ služeb v různých oblastech.

Všichni investoři se zdají být pozitivní o potenciálu blockchainů, ačkoliv je pozorovatelný významný rozdíl v názorech u tradičních finančních institucí a fintech společností. Banky jsou jednotní v názoru, že nelze použít permissionless blockchainy jako je Bitcoin na finančních trzích. Jako správnou volbu vidí ve vybudovaní soukromých blockchainů, kde budou jednoznačně identifikovaní všichni účastnicí tohoto blockchainů. R3 konsorcium tvořené z největších bank na světě je zřejmě nejviditelnějším příkladem pokusu vytvořit mezibankovní blockchain.

Fintech oblast má hodně různorodých společnosti a mezi nimi existuje cela řada různých postojů o budoucnosti blockchainů. Existuje rovněž mezi nimi několik různých druhu implementace této technologie. Každopádně společností v této oblastí jsou příznivější k permissionless blockchainům jako je Bitcoin než jak tomu je u bank. Zde není příliš kladená pozornost na právní otázky či nevýhody permissionless blockchainů. Namísto toho se zdá, že počítají s tím, že technologie a legislativa se bude rozvíjet a tyto otázky budou úspěšně řešeny v budoucnu. Startupy se především soustřeďují na Bitcoin a další permissionless blockchainy, což umožňuje implementaci technologie rychleji a ekonomický efektivněji.

Aktuálně banky mají šanci na úspěch pouze s permissioned blockchainy. Je to odůvodněné zejména skutečností, že je lze snadněji integrovat do nynějších stávajících systému. Zejména právní otázky spojené s regulacemi AML, KYC hovoří ve prospěch permissioned blockchainu. Finanční instituce poukazují na to, že přinejmenším v první době blockchainy by měly být použity pouze na některé trhy. Zejména tam, kde jsou objemy nižší a počet zúčastněných stran je omezen. Pohledem bank je, že tato technologie funguje nejlépe v odvětvích, kde je důvěra mezi stranami nízká, tam jsou tedy zbytečné zprostředkovatelé, přeshraniční platy nebo jiné překážky pro efektivitu. Obchodní finance, trhy s deriváty jsou příklady oblastí, kde banky se zdají mít největší pozornost pro tuto chvíli.

Fintech společnosti, chtějí především vyvíjet aplikace blockchainů pro všechny druhy trhu. Mají výrazně odlišný postoj než banky. Je snadné získat dojem, že mnoho z těchto společností mají pozitivní pohled, že blockchain by mohl znamenat revoluci pro všechny druhy trhů. Banky se zaměřují především na nejslibnější případy užití, kde nová technologie by mohla poskytnout úsporu

nákladů a zvýšení efektivity již v krátkodobém horizontu. Banky neradi utrácejí prostředky na projekty, které nejsou ziskové v krátkodobým horizontu 3-5 let.

Banky si uvědomili, že digitalizace a vývoj technologie blockchainů může představovat hrozbu pro tradičního bankovnictví. Fintech společnosti by mohli být schopni vytáhnout zisk bank díky technologií k sobě. Benefity blockchain technologie by mohly eliminovat potřebu centrálních autorit v provádění transakcí.

Bylo vidět v minulosti, že dominantní hráči na trhu ztratily své pozice na nové, menší účastníky. Došlo k tomu zejména v průběhu digitalizace. Dotklo se to některých segmentů bankovního podnikání, např. půjček a platebních služeb. Pokud banky nedokážou brát fenomen blockchain vážně a nebudou vyvíjet tuto technologií, tak totéž by se mohlo stát i na finančních trzích. Blockchain technologie by mohla rozhodovat o budoucností přežíti bank. Pokud totiž nějaká technologie se rozvíjí vysokým tempem, tak nikdo by si nemohl představit co s ní bude za několik let.

Banky si myslí, že tradiční finanční instituce mají konkurenční výhodu při vývoji blockchainů na finančních trzích. Existují racionální argumenty na podporu tohoto názoru. Banky mají významnou roli ve fungování společnosti. Jejich vztahy s klienty a regulátory jim dávají dobrou pozici k vytváření a vývoji blockchain technologií.

Na druhé straně revoluční řešení často pocházejí z prostředí, kde hráči mají ambiciózní cíle, a proto banky by měli sledovat, co fintech společností dělají. Spolupráce s menšími společnostmi je důležitá a banky již začaly získávat slibné startupy. To je známkou toho, že banky připouštějí, že by mohlo být lepší řešení vycházející ze sektoru fintech a že banky samy o sobě nejsou největší odborníci, pokud jde o technickou stránku blockchain technologie.

Naopak, banky mají dobré znalosti o tom, jak fungují finanční trhy, a proto se získáním fintech společností mají reálnou šanci uspět při vytváření dominantních finančních platforem. Skutečnost, že banky mají dobré postavení ve společnosti a mají finanční prostředky potřebné k financovaní začínající firmy je hlavním důvodem proč mají konkurenční výhodu. Pokud banky budou investovat do odborníku a využijí této odborné pracovní síly, kterou získali, je potom snadné vidět, jak uspějí ve vytváření platforem na blockchain bázi. Tyto platformy potom budou standardem na mnoha finančních trzích. Bankovní sektor bude efektivnější a banky mohou vytvářet nové zisky z inovací uskutečněných blockchain technologií. Vyžaduje to samozřejmě spolupráci v bankovnictví, ale průmysl se probudil na potřebu spolupráce a vytvořilo se již několik skupin pro mezibankovní řešení.

V případě, že banky nebudou brát vstup nových implementátorů technologie vážně nebo selžou ve snaze o vytvoření standardních řešení pro bankovnictví, potom je pravděpodobné, že ztratí nějakou část své činnosti a tím pádem i zisk. Blockchain technologie se vyvíjí vysokou rychlostí a například zapojením centrálních bank do kryptoměn, že by například vydávali vlastní kryptoměnu

by ještě usnadnilo process vývoje blockchainů, ale zatím tato vize je daleko. Centrální banka, která by vydávala kryptoměnu, potom by zejména usnadnila zavádění nových řešení poskytovaných malými fintech společnostmi, což by nastolilo větší důvěru k menším hráčům této technologie.

Některé z největších překážek při zavadění nových technologií jsou právní a vládní záležitosti. Nedostatek legislativy komplikuje vývoj. Regulátoří nemají negativní postoj k nové technologií. Pokud stabilita, bezpečnost a fungování trhů bude zajištěna, tak regulátoři pravděpodobně nebudou branit v šíření blockchainů. Zajištění ovladatelnosti a možnost dohlížet na trhy, bude pro ně rozhodující.

Závěr

Blockchain technologie, respektive distributed ledger technologie jsou poměrně novým fenomenem ve finančním světě, avšak aktuálně velmi intenzivně a rapidně se vyvíjejícím. Získal jsem hodně znalosti při psaní tohoto tématu a věřím, že tyto znalosti mi budou přínosem do budoucna. Je pro mě poctou, že při psáni tohoto tématu jsem mohl uplatnit předchozí získané znalostí o Bitcoinu, kryptoměnách, kterým jsem se věnoval v posledních letech. Tyto znalostí mi pomohli se lepé chopit tématu, nebot' technologie blockchain či distributed ledger vychází především z Bitcoinu. Rád jsem rovněž navštívil přednášku o blockchainech v bankovnictví, kterou organizovala technologická pobočka britské banky Barclays v Praze.

Kolem blockchain se aktuálně děje hodně věci a tradiční finanční instituce investují vysoké částky do výzkumu a vývoje svých systémů. Je třeba vyčkat, zda blockchainy budou zcela novým druhem finančních řešení, či spíše budou mít doplňkovou úlohu ve stávajících systémech. Můžeme nyní bezpečné říci, že uslyšíme ještě hodně o blockchainech v budoucnosti. Vývoj nové technologie pravě nabral své první kroky v bankovnictví. Vzhledem vysokému potenciálu této technologie můžeme očekávat, že uvidíme úspěch mnohem rychleji, než si myslíme.

Literatura

[1] Let's Talk Payments (LTP): *Know more about blockchain: overview, technology, application areas and use cases[online].* [cit. 2016-12-20]. Dostupné z: https://letstalkpayments.com/an-overview-of-blockchain-technology/

[2] Paralelní polis: *Paralelní polis[online].* [cit. 2016-10-15]. Dostupné z: https://www.paralelnipolis.cz/o-nas/

[3] Bitcoin community: *Promotional graphics [online].* [cit. 2016-10-11]. Dostupné z: https://en.bitcoin.it/wiki/Promotional_graphics

[4] Wikimedia Foundation: *Bitcoin [online].* [cit. 2016-09-10]. Dostupné z: http://en.wikipedia.org/wiki/Bitcoin

[5] Blockchain: *Bitcoin Charts [online].* [cit. 2016-10-22]. Dostupné z: https://blockchain.info/charts/

[6] HardwareWallets.com: *Trezor [online].* [cit. 2016-04-03]. Dostupné z: http://www.hardwarewallets.com/

[7] Bitcoin community: *Offline Address [online].* [cit. 2016-03-10]. Dostupné z: https://en.bitcoin.it/wiki/OfflineAddress

[8] *Bitcoin difficulty [online].* [cit. 2016-03-15]. Dostupné z: http://bitcoindifficulty.com/

[9] Rosenfeld, M.: *Analysis of hashrate-based double-spending [online].* [cit. 2016-07-04]. Dostupné z: https://bitcoil.co.il/Doublespend.pdf

[10] Morrison, A.: *Blockchain and smart contract automation: How smart contracts automate digital business[online].* [cit. 2016-11-30]. Dostupné z: http://www.pwc.com/us/en/technology-forecast/blockchain/digital-business.html

[11] Robeco: *Distributed ledger technology for the financial industry[online].* [cit. 2016-11-28]. Dostupné z: https://www.robeco.com/images/201605-distributed-ledger-technology-for-the-financial-industry.pdf

[12] Hong Kong Monetary Authority: *Whitepaper on distributed ledger technology[online].* [cit. 2016-12-26]. Dostupné z: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf

[13] Evry: *Blockchain: Powering the Internet of Value[online].* [cit. 2016-12-28]. Dostupné z: https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf

[14] CB insights: *The March Of Financial Services Giants Into Bitcoin And Blockchain Startups In One Chart[online].* [cit. 2016-11-10]. Dostupné z: https://www.cbinsights.com/blog/financial-services-corporate-blockchain-investments/

[15] UniCredit bank: *Blockchain Technology and Applications from a Financial Perspective[online].* [cit. 2017-1-6]. Dostupné z: https://www.scribd.com/doc/303933279/

[16] Santander: *Rebooting financial services[online].* [cit. 2016-12-23]. Dostupné z: http://santanderinnoventures.com/fintech2/

[17] company: *Distributed Ledger Technology[online].* [cit. 2016-11-13]. Dostupné z: http://www.chyp.com/wp-content/uploads/2015/03/R3-and-Corda-Richard-G-Brown-Tomorrows-Transactions-Final.pdf

[18] Gartner: *Hype Cycle for Emerging Technologies[online].* [cit. 2016-10-15]. Dostupné z: http://www.gartner.com/smarterwithgartner/3-trends-appear-in-the-gartner-hype-cycle-for-emerging-technologies-2016/

[19] Bradbury, D.: *Is Bitcoin a Digital Currency or a Virtual One? [online].* [cit. 2016-11-22]. Dostupné z: http://www.coindesk.com/bitcoin-digital-currency-virtual-one/

[20] Inc., J. I.: *What does Cryptocurrency mean? [online].* [cit. 2016-12-22]. Dostupné z: http://www.techopedia.com/definition/27531/cryptocurrency/

[21] Chaum, D.: *Blind signatures for untraceable payments [online].* [cit. 2016-10-15]. Dostupné z: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

[22] CoinMarketCap: *Crypto-Currency Market Capitalizations [online].* [cit. 2016-11-15]. Dostupné z: http://http://coinmarketcap.com/all.html

[23] Lorenz, R.: *RSA, problém faktorizace. Kryptografie s veřejným klíčem, ElGamalův algoritmus, DSA [online].* [cit. 2016-10-15]. Dostupné z: https://edux.fit.cvut.cz/courses/BI-BEZ/

[24] Bitcoin community: *History Bitcoin [online].* [cit. 2016-03-10]. Dostupné z: https://en.bitcoin.it/wiki/History

[25] BlockchainTechnologies.com: *Blockchain Technology Explained[online].* [cit. 2016-10-15]. Dostupné z: http://www.blockchaintechnologies.com/blockchain-definition

[26] Don Tapscott, A. T.: *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.(2016).* Portfolio Penguin, první vydání, ISBN 978-0670069972.

[27] European central bank: *Distributed ledger technologies in securities post-trading[online].* [cit. 2016-12-23]. Dostupné z: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf

[28] Finance.cz: *Musí banky znát své klienty tolik?[online].* [cit. 2016-10-18]. Dostupné z: http://www.finance.cz/zpravy/finance/249649-musi-banky-znat-sve-klienty-tolik/

[29] Redman, J.: *1.4 Billion Invested in Blockchain, says PwC Executive[online].* [cit. 2016-10-20]. Dostupné z: https://news.bitcoin.com/1-4-billion-invested-blockchain-pwc/

[30] Česká narodní banka: *Popis systému CERTIS[online].* [cit. 2016-11-10]. Dostupné z: https://www.cnb.cz/cs/platebni_styk/certis/certis_popis.html

[31] Management mania: *SWOT analýza[online].* [cit. 2016-12-23]. Dostupné z: https://managementmania.com/cs/swot-analyza

[32] Roklen24: *Co znamená technologie za bitcoinem pro velké banky?[online].* [cit. 2016-11-15]. Dostupné z: http://roklen24.cz/a/ipTHG/co-znamena-technologie-za-bitcoinem-pro-velke-banky

Příloha A

Seznam použitých zkratek

ČVUT České vysoké učení technické v Praze

ČR Česká republika

BTC Bitcoin mince

XBT Bitcoin mince nový akronym

mBTC Jedna tisícina BTC

GUI Graphical User Interface

P2P Peer-to-peer sít'

DSA Digital Signature Algorithm

ECDSA the Elliptic Curve Digital Signature Algorithm

SHA Secure Hash Algorithm

DP Diplomová práce

KYC Know your customer

ECB Evropská centrální banka

AML Anti money laundering

SWIFT Society for Worldwide Interbank Financial Telecommunication

FinTech Financial technology

Příloha B

Slovník použitých pojmů

- **Bitcoin** – Platební system Bitcoin
- **bitcoin - BTC** – Digitální peněžní měna platebního systému nebo rovněž prostředek směny Bitcoinu.
- **klient** – Typ používané aplikace, která je na každém uzlu sítě. Klienti komunikují mezi sebou pomoci implementovaného protokolu.
- **Bitcoind** – Oficiální implementovaný protokol v klientech. Určuje komunikaci klientů mezi sebou.
- **satoshi** – Nejmenší jednotka jednotka platebního prostředku Bitcoinu. 1 BTC = 1000 000 satoshi. Komunita Bitcoinu zvolila tento název na počest zakladatele Bitcoinu Satoshi Nakamoto.
- **Satoshi klient** – Název oficiálního klienta Bitcoinu.
- **adresa** – Adresa učtu Bitcoinu, která se skládá z 27 až 34 alfanumerických znaku. První znak adresy je 1 až 3.
- **peněženka** – Typ klienta, který generuje a uschovává kryptografické klíče, které prokazují vlastnictví Bitcoin minci v distribuované databázi.
- **distribuovaná databáze** – Je abstraktně účetní knihou, která uschovává veškeré záznamy o proběhlých transakcích za celou dobu existence platební sítě. Je tvořena řetězcem bloku.
- **Know your customer - KYC** – (český: Poznej svého klienta). Jedná se o pojem u regulaci bank. Každá banka má povinnost mít dostatek informací o svých klientech. Musí vědět, s jakými osobami vstupují do smluvního vztahu, kdo bude oprávněn manipulovat s peněžními prostředky a jaké jsou záměry těchto osob.

- **Anti money laundering - AML** – (český: Praní špinavých peněz). Jedná se o pojem u regulaci bank. Jednání sledující zastření nezákonného původu peněz s cílem vzbudit dojem, že se jedná o peníze nabyté legálně.
- **Startup** – podnikatelský subjekt, typicky popsán jako nově založená či začínající společnost a rychle se vyvíjející a měnící společnost. V současné době neexistuje jedna ucelená, mezinárodně uznávaná definice startupu. Kolem blockchainů vzniká spousta nových startupu, které chtějí aplikovat tuto technologií především ve finančním sektoru, ale i ostatních odvětvích.
- **Financial technology - Fintech** – Fintech je označení pro obor Financial Technology - "finanční technologie". Fintech představuje různé inovace ve finančních službách. Označuje se tak pomyslné propojení moderních technologií se světem financí. Respektivě způsoby, jak moderní technologie zefektivňují přístup k financím. Příkladem jsou online bankovnictví, crowdfundingové portály, peer to peer půjčky, kryptoměny, blockchainy a podobně.

Příloha C

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `DP_Rendla_Michal.pdf` ..... text práce ve formátu PDF