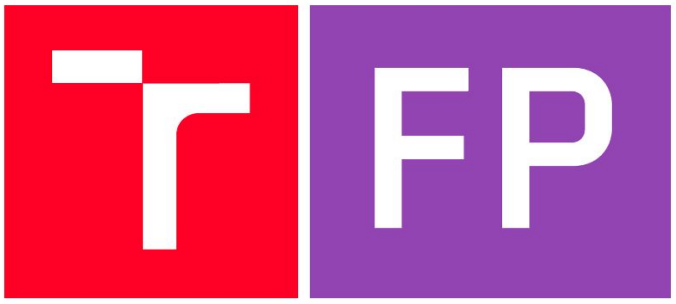
Semestrální projekt

Blockchain & Smart Contracts

Podnikové informační systémy 2

Řízení životního cyklu IS



Robert Albrecht

Daniel Vítek

Martin Kopec

2018

Obsah

1. Co je to Blockchain

1.1 Historie

1.1.1 Blockchain

První zmínky o blockchainu byly popsány pány Stuartem Haberem a W. Scottem Stornettou v článku pro Journal of Cryptology v lednu roku 1991. Tehdy se ještě nejednalo o blockchain jak ho známe nyní, ale základní princip byl stejný. Článek nesl název “How to time-stamp a digital document” a jak už vyplývá z názvu, tak autoři chtěli systém distribuovaných bloků využít pro podepisování digitálních dokumentů [8]. Hlavní slovo při rozšíření této myšlenky a její reálné implementaci měl však především Satoshi Nakamoto, když v roce 2008 vydal publikaci s názvem “Bitcoin: A Peer-to-Peer Electronic Cash System” [9].

1.1.2 Kryptoměny

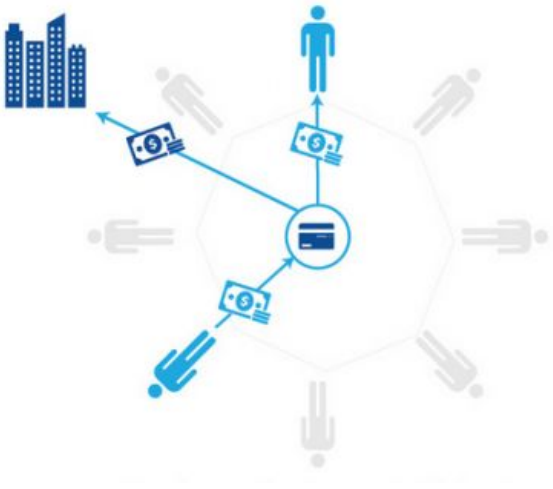
Vývoj a postupné proniknutí blockchainu ve známost veřejnosti je silně spojený se vznikem a vývojem kryptoměn. Ostatně, jak je zmíněno v předchozí kapitole, tak největší rozkvět blockchainu přišel právě se vznikem Bitcoinu. Ač Bitcoin může být průkopníkem ve světě kryptoměn, tak se ale rozhodně nejedná o první kryptoměnu. Již v devadesátých letech minulého století přišel David Chaum, počítačový specialista se zaměřením na kryptografii s koncepcí elektronických peněz [6]. Pod záštitou firmy DigiCash, jejímž byl zakladatelem se pokusil najít reálné využití této technologie, ale i přes nalezení několika klientů v bankovním sektoru se nepodařilo technologii dostatečně prosadit. Spotřebitelé radši dali přednost platebním kartám a společnostem s důvěryhodnějším principem placení jako byli Visa či MasterCard. Na konci roku 1998 ukončila firma podnikání [7]. V průběhu let pak postupně vznikaly a pokusily se prosadit další kryptoměny, jako např. B-Money nebo Bit Gold. Ale opravdu správný čas pro kryptoměny a jejich raketový vzestup přišel až s Bitcoinem.

1.1.2.1 Bitcoin

Po pár měsících od zveřejnění publikace “Bitcoin: A peer-to-peer Electronic Cash System” došlo k založení firmy. Získávání této měny bylo založeno pouze na tzn. těžení. O rok později pak mělo dojít k prvnímu obchodu, kde bylo směněno 10,000 ks za dvě pizzy *(Poznámka autora: tento fakt je zde uveden vzhledem k jeho zajímavosti, ale jeho průkaznost je mizivá. Informace pochází ze zdroje [10])*. Postupnému zpopularizování této digitální měny pomohlo dozajista i perfektní načasování jejího vzniku. Když v rámci celosvětové finanční krize v roce 2008 částečně padl systém bank, kterému měli lidé, jakožto koncový spotřebitelé, bezmezně věřit, otevřel se prostor pro diskuzi nad existencí systému jiného.

1.2 Princip fungování

Princip fungování si ukážeme na finančních transakcích, protože zde nalezneme nyní nejrozšířenější užití blockchainu. Koncept blockchainu je navržený tak, že při finančních transakcích není zapotřebí důvěryhodné třetí strany (banky). Jedná se tedy o decentralizovaný systém, kdy na ověření a schválení transakce se podílí všechny připojené jednotky, neboli uzly. Důvěryhodné třetí strany (banky) si v naprosté většině případů účtují malý poplatek za ověření a provedení transakce (převod mezi bankami) a samotný proces může trvat až několik dní. Při použití blockchainu nepotřebujeme třetí důvěryhodnou stranu, jelikož transakci ověřuje celá síť. V případě převodu kryptoměn poplatek placený odesílatelem není a samotný transfer je prakticky okamžitý.



Obrázek 1. Centralizované bankovní transakce [1]

1.2.1 Průhlednost díky otevřenému záznamu všech transakcí

Blockchain je zabezpečené a funkční řešení, které využívá konceptu otevřené účetní knihy (v angličtině “distributed ledger”). Jinými slovy naprosto všechny transakce jsou všemi zpětně dohledatelné. Každý uzel má u sebe kopii všech transakcí, které se kdy provedly, a nové se průběžně přidávají. K tomu, aby tento systém fungoval, musí docházet k pravidelné synchronizaci, aby všechny kopie byly identické a všichni měli aktuální verzi.

Obrázek 2. Decentralizované bitcoinové transakce [2]

1.2.2 Blok a blockchain

Při transakci v blockchainu se vytváří nový zápis neboli tzv. blok. Blok je složen ze tří částí: data, hash a hash předchozího bloku. Co obsahují data se liší s ohledem na užití daného blockchainu. Nejdůležitější informace jsou ale informace o tom kdo požádal o transakci, kdo je jejím příjemcem a co je podstatou transakce. Když se nový blok vytvoří, automaticky se vypočítá jeho hash, což je unikátní řetězec písmen a čísel, jinými slovy matematický obraz celého bloku. Při sebemenší modifikaci některé z těchto tří sekcí se výsledný hash bude lišit a takto tedy můžeme spolehlivě kontrolovat, zda se někdo nepokusil o podvodnou změnu. Tím, že bloky mají v sobě hash předchozího bloku vznikají řetězce, ve kterých se jednotlivé bloky nedají upravit, aniž by to bylo očividné.

Matematický výpočet hashe v dnešní době ale není náročný proces a při nekalé úpravě jednoho bloku by se téměř okamžitě daly vypočítat nové hashe pro každý další blok a tím skrýt stopy po útoku. Avšak technologie blockchainu nasazená pro transfer měn používá koncept proof-of-work (viz kapitola 1.3.1), kdy vytvoření jednoho bloku je matematicky navržené tak, aby trvalo určitou dobu (u Bitcoin blockchainu je to 10 minut), a proto tedy není možné změnit data v jednom bloku a rychle přepočítat nové heshe všech následujících. [12]

1.2.3 Průběh transakce a vytvoření nového bloku

Prvnímu blok v blockchainu vzniká automaticky, neobsahuje has předchozího bloku a říká se mu genesis blok. Praktický příklad použití blockchainu si vysvětlí na převodu

kryptomen. Při převodu virtuální měny mezi uzly A a B, nod A vytvoří nový blok s informacemi o transakci a vyšle jej všem ostatním uzlům v sítí, přičemž žádá o verifikaci a zařazení do blockchainu. K tomu, aby proběhla verifikace nového bloku, jsou v sítí přítomni mineři (anglicky miners). Mineři jsou uzly, které mají k dispozici dostatečný výpočetní výkon hardwaru a defacto zpracovávají tyto transakce. Transakce se zpracuje tak, že mineři mezi sebou začnou soutěžit o rozluštění unikátní šifry nového bloku, který někdo chce přidat do sítě. Předem není jasné, komu se to povede dříve a je to tedy celé postaveno na náhodě. Mineři dedikují výpočetní výkon svého hardwaru a energii pro rozluštění vždy unikátní šifry nového bloku a kdo ji jako první rozluští, verifikuje transakci a přidává ji do svého blockchainu. Kopie blockchainu minera, který tuto šifru rozluští je následně broadcastnuta do celé sítě. Ostatní uzly ověří správnost posledního bloku a vyluštěné šifry a přidají si tento blok do své vlastní kopie blockchainu. Veškeré snažení ostatních minerů se zastavuje a začínají zpracovávat další transakci. V případě Bitcoin blockchainu je odměnou za rozluštění šifry samotný bitcoin, poskytnutý sítí za provedenou práci. Tímto způsobem je nastavená odměna za poskytnutý výpočetní výkon (hashrate) pro potřeby sítě. [13]

1.3 Typy algoritmov

V tejto časti sa budeme venovať rôznym spôsobom, akým môžu byť transakcie a celé bloky v blockchaine spracovávané. Pôjde o algoritmy, ktoré zabezpečia náhodnosť v tom, kto bude daný blok (transakciu) spracovávať. Zároveň sú navrhnuté tak, aby sťažili potenciálnym útočníkom ovplyvniť spracovanie bloku (transakcie) v ich prospech.

1.3.1 Proof of work

Myšlienka bola prvý krát predstavená v roku 1993 na ochranu proti spamu a formálne nazvaná proof of work v roku 1997 [1]. Ochrana proti spamu bola založená na vypočítaní časovo relatívne náročného výpočtu pri odoslaní každého emailu. V prípade, že odosielateľ chce poslať niekoľko tisíc emailov, a teda rozoslať spam, stáva sa pre neho takéto konanie nerentabilné, pretože spočítanie danej funkcie (proof of work) pre taký počet emailov je časovo a teda aj ekonomicky nevýhodné.

Každý uzol v sieti, ktorý validuje nové bloky blockchainu sa označuje ako miner a proces, ktorý vykonáva sa nazýva mining. Proof of work je použitý na zabezpečenie siete Bitcoin, čo bola aj jeho prvá širšia aplikácia.

1.3.1.1 Princíp

Každý blok obsahuje, okrem hashu predchádzajúceho bloku a seba, ešte ďalšiu hodnotu, nazývanú nonce. Úlohou minera je overiť validitu dát, vypočítať hash a nonce nového bloku. Pod validáciu dát patrí napr. overenie, že odosielateľ (identifikovaný jedinečným kľúčom) má k dispozícií dané prostriedky, ktoré chce previesť inému užívateľovi.

V sekcií 1.2.2 bolo spomenuté, že výpočet hashu nie je v dnešnej dobe náročný proces. Preto sú definované určité pravidlá, ktoré hash vytvorený minerom musí spĺňať,viď nasledujúcu sekciu 1.3.1.2.

1.3.1.2 Príklad

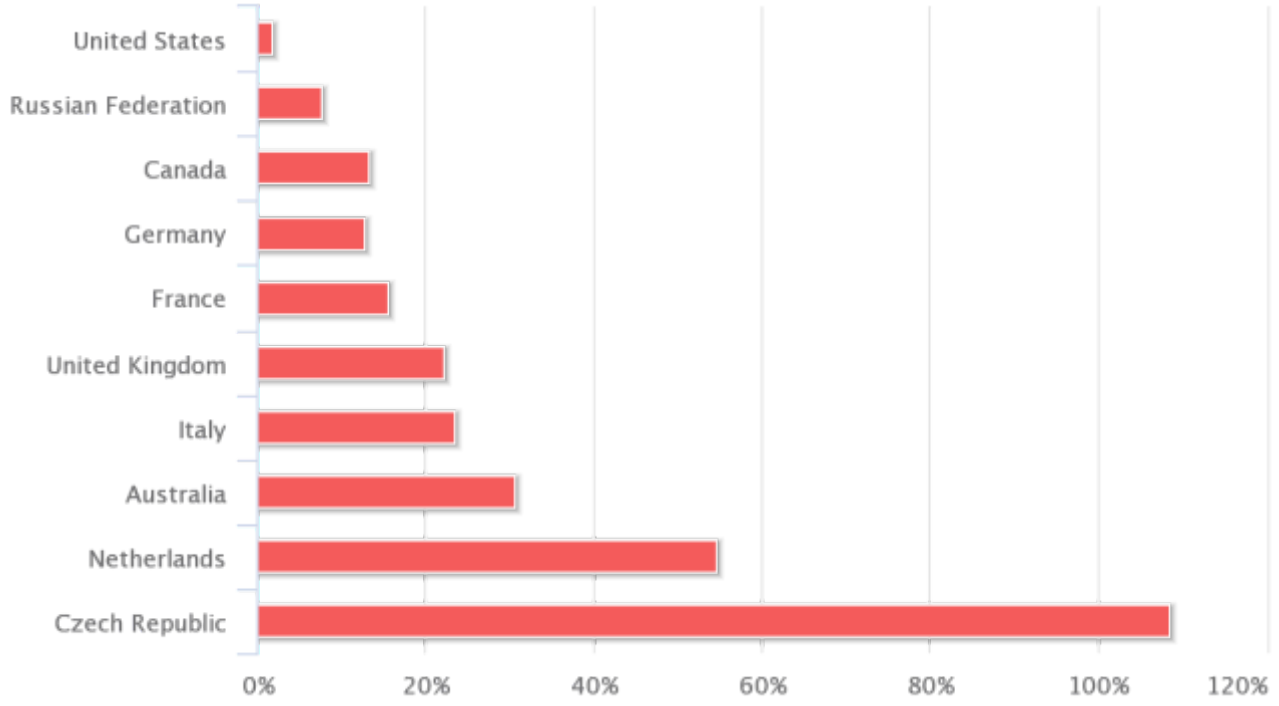
Stanovme si, že každý hash musí začínať štyrmi znakmi 0. To znamená, že miner vypočíta hash bloku a ak tento hash nespĺňa podmienku, miner musí vygenerovať nový hash. Aby dostal nový hash musí pozmeniť dáta v bloku na čo práve slúži nonce hodnota. Miner zmení túto hodnotu (napr. inkrementuje o 1) a znova vypočíta hash pre daný blok. Tento proces sa opakuje až do momentu, keď hash spĺňa podmienku a začína sa štyrmi znakmi 0. Získaný hash je následne odoslaný všetkým ostatným uzlom v sieti a dotyčný miner získava odmenu. Vďaka tomu, že ide o časovo náročný proces, je nemožné dopredu predpokladať, ktorý uzol bude prvý, čím sa zväčuje dôvera užívateľov v danú sieť.

Zmienený proces je znázornený na obrázku č. 3, kde dáta v bloku predstavujú text “Hello, world!” doplnený o hodnotu nonce. Z obrázku vyplýva, že až na 4250-ty pokus sa minerovi podarilo vytvoriť hash, ktorý spĺňa danú podmienku [2].

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Obrázek 3. Ukážka hľadania správneho hashu [4].

Nevýhodou proof of work algoritmu je fakt, že hľadanie konkrétneho hashu vyžaduje silný vypočetný výkon a veľké množstvo elektrickej energie. Pre predstavu z obrázku 4 v prílohách vyplýva, že sieť Bitcoin spotrebuje viac elektrickej energie ako Česká republika [3].



Obrázek 4. Spotreba energie na ťaženie Bitcoinu v niektorých krajinách [5]

1.3.2 Proof of stake

Pri tomto type algoritmu sa uzol, ktorý sa podiela na validácií blokov nazýva validátor a proces minting alebo forging, čo si vo voľnom preklade môžme predstaviť ako pečiatkovanie. V prípade blockchainu peňažných transakcií, každý validátor dá do zástavy svoje finančné prostriedky. V prípade, že zvaliduje transakciu nesprávne (napr. snaží sa podsunúť falošné údaje), príde o svoje peniaze.

Pri tomto algoritme validuje nový blok len jeden uzol, uzly nesúperia medzi sebou, čo je hlavný rozdiel oproti PoW, kde každý blok validovali všetci. Vďaka tomu, že nie je potrebné počítať hash, ktorý spĺňa nejakú podmienku a faktu, že uzol nemusí byť najrýchlejší v celej sieti aby získal odmenu, nie je potrebný až tak výpočtovo silný hardware. Z toho vyplýva, že tento algoritmus nie je tak náročný na spotrebu elektrickej

energie ako PoW a taktiež prvotné náklady na hardware každého uzlu sú nižšie, vďaka čomu sa validátorom môže stať prakticky akékoľvek zariadenie.

Na druhú stranu, PoS prináša viac risku ako PoW, pretože musíme tiež riešiť situáciu, kedy zvolený validátor nevykoná svoju prácu. V takomto prípade sú zvolení náhradní validátori daného bloku. Ďalším problémom je náhodné vyberanie validátorov, pretože validátor môže spracovávať len transakcie, ktorých výška je nižšia ako výška jeho stávky, peniaze ktorými ručí za správnosť overenia daného bloku. Z toho vyplýva, že validátor, ktorý vložil do stávky 2-krát viac peňazí ako iný, má tiež 2-krát vyššiu pravdepodobnosť, že bude vybratý na validovanie nového bloku.

1.4 Výhody a nevýhody

Za předpokladu, že technologii blockchain považujeme obecně za přínos, tak se sluší začít výhodami.

V první řadě je na místě zmínit tu nejčastěji zmiňovanou výhodu a to je **decentralizace**. V podstatě se jedná do jisté míry o **nezávislost**. Jelikož je blockchain založený na peer-to-peer síti a nepotřebuje žádný centrální prvek, tak nám odpadají starosti s tím, jestli je daný centrální prvek dostatečně spolehlivý a důvěryhodný a také jestli bude dostupný když potřebujeme.

S tím jde ruku v ruce další výhoda a to je **rychlost**. Pokud se budeme bavit o blockchainu v pojetí jeho využití pro bankovní transakce, tak banky fungují typicky na principu spíše dní než hodin nebo dokonce minut. Pokud máme tu smůlu, že je zrovna víkend, tak si opravdu můžeme počkat při převodu do cizí banky i tři dny. Blockchain je v tomto omezený pouze ve smyslu jeho zabezpečení. Pokud pro tento příklad vezmeme kryptoměnu Bitcoin, tak vytvoření nového bloku je opatřeno ochranným mechanismem, který ho nepovoluje vytvořit dříve než za 10 minut.

Jako poslední bych zmínil **transparentnost**. Ta jde opět ruku v ruce se systémem decentralizace. Celý systém transakcí je kompletně transparentní a závislí na této transparentnosti. Každý uživatel má k dispozici kompletní přehled o všech transakcích a podílí se na jejich ověřování.

První nevýhodu, kterou bych zmínil, je v případě PoS rozhodně **potřebný výkon**. Každý nový blok musí mít vygenerovaný hash a validitu tohoto hashe musí ověřit ostatní uživatelé sítě.

S tím je úzce spojená další nevýhoda a tou je **redundace** dat. Každý člen sítě drží kopii “databáze” u sebe, právě z toho důvodu, aby byl schopný ověřovat jeho validitu. Tím pádem místo toho aby byla data jen na jednom místě, tak jsou zduplikována tolikrát, kolik je členů sítě, kteří zajišťují její běh.

Poslední nevýhodou, kterou bych zmínil je samotný princip blockchainu, který je silně **závislý** na počtu uživatelů, resp. “minerů”. Pokud nikdo nepropůjčí svůj výkon k tvorbě a ověřování nových bloků, tak celý síť ztrácí svůj primární účel. Zároveň při malém množství uživatelů nebo jejch shromáždění v poolech, může dojít k tzv. 51% útoku (více viz kapitola 51% útok).

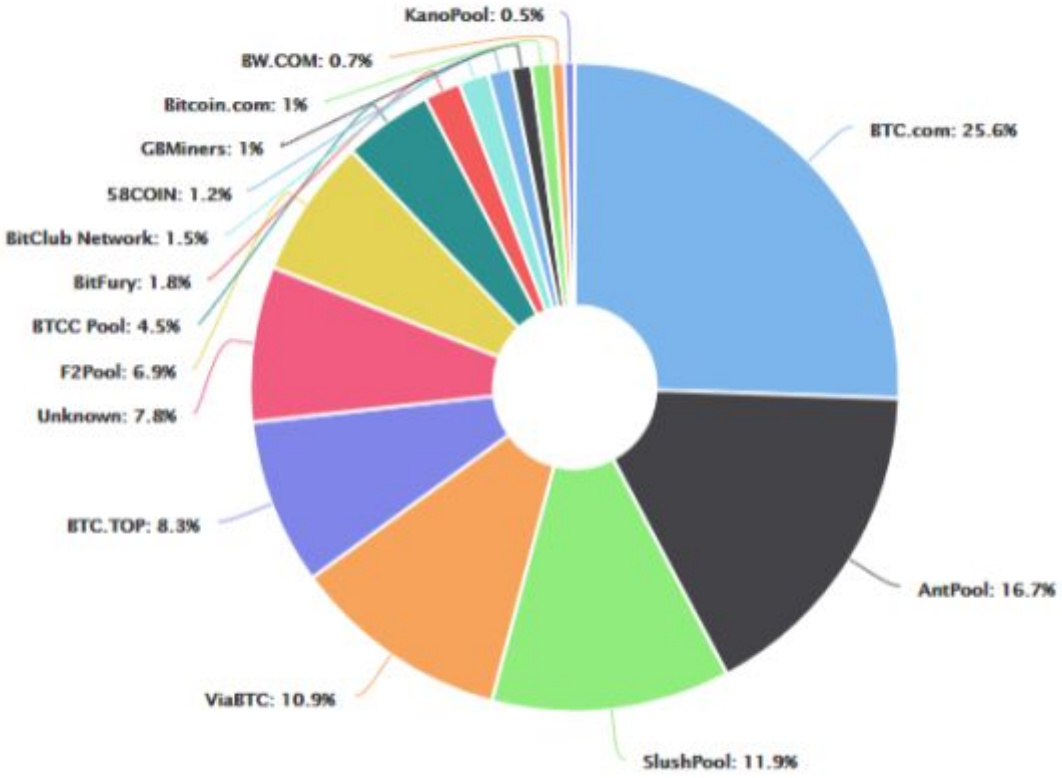
1.4.1 51% útok

Prvý krát bolo na tento útok poukázané ako hrozba PoW algoritmu. Ide o útok kde jeden miner alebo skupina minerov získa väčšinovú silu, tzn. hashing power v prípade PoW alebo väčšinový podiel stávky v prípade PoS algoritmu. V takom prípade tento miner/skupina minerov môžu schvalovať svoje transakcie, čím klesá dôvera v sieť a celý systém prestáva fungovať.

Ráta sa s tým, že v prípade veľkých sietí je tento typ útoku veľmi nepraktický. Pre príklad si zoberme kryptomenu Dash, ktorá používa PoS. V októbri 2018 bol jej trhový objem v hodnote takmer 1,3 miliardy amerických dolárov [5]. V prípade, že by chcel niekto uskutočniť útok 51%, musel by nahromadiť Dash v hodnote 650 miliónov dolárov. V takom prípade by bol útočník schopný podvrhnúť svoje bloky, pretože by bola vysoká šanca, že bude kvôli vysokej stávke vybratý práve on na zvalidovanie bloku. Avšak nemá 100% istotu, že bude vybratý práve on na tomto alebo akomkoľvek nasledujúcom bloku. Ak bude vybratý niekto iný, je možné, že si pravdepodobne všimne chybné bloky a sieť stratí dôveru, čím útočník príde o svoje peniaze - celú stávku, ktorá by v tomto prípade bola rovná 650 miliónom dolárov.

Blockchain, ako už bolo spomínané, je decentralizovaná sieť, avšak, v prípade PoW mineri priniesli časť centralizácie tým, že sa spájajú do tzv. mining pools. Robia tak z dôvodu, že ako skupina disponujú vyšším výpočtovým výkonom, takže keď ťažia spolu, síce sa delia o zisk ale majú vyššiu šancu vyťažiť nový blok skôr ako niekto iný. Obrázok č. 2 zobrazuje percentuálny podiel poolov z celého výpočtového výkonu, ktorý je použitý na mining akéhokoľvek Bitcoinu. Z grafu na obrázku č. 5 vyplýva, že ak by sa spojili 3 najväčšie pooly, disponovali by viac ako 50% podielom výpočtového výkonu celej siete, čo

by spôsobilo stratu dôvery v sieť a jej zánik. Z tohto dôvodu je 51% útok viac pravdepodobný pri PoW ako pri PoS.



Obrázek 5. Percentuálny podiel Bitcoin mining poolov [7]

2. Použití blockchainu

2.1 Jak se blockchain aktuálně používá

2.1.1 Účetní kniha

Vzhledem k faktu, že za zpopularizováním této technologie stojí hlavně Bitcoin se blockchain popisuje u velkého množství zdrojů jako účetní kniha. Pravdou však je, že to je pouze jedno z možných využití blockchainu. O jeho potenciálu a alternativních možnostech využití je více popsáno v následující kapitole. Dnes tedy známe blockchain hlavně jako účetní knihu. Co to ale znamená? To znamená, že v jednotlivých blocích jsou zaznamenány informace o transakcích, které probíhají v návaznosti na některou z kryptoměn. Každá transakce, která se uskuteční, představuje nově vzniklý blok, který se připojí do sdílené databáze, čímž vzniká právě tento “ledger” neboli účetní kniha.

2.1.2 Co dalšího

Jak jsem naznačil v předchozí kapitole, tak blockchain má dnes využití hlavně v kryptoměnách. Spekulací o tom, jak by se tato technologie dala dále efektivně využívat je velké množství a některé příklady z těchto možných aplikací blockchainu jsou zmíněny v následující kapitole. Je tedy ale blockchain využíván i jinak než u kryptoměn? Existuje už reálně jiná implementace této technologie? Několik příkladů využití blockchainu je popsáno níže následováno obrázkem znázorňujícím další projekty založené na této technologii.

2.1.2.1 E-estonia

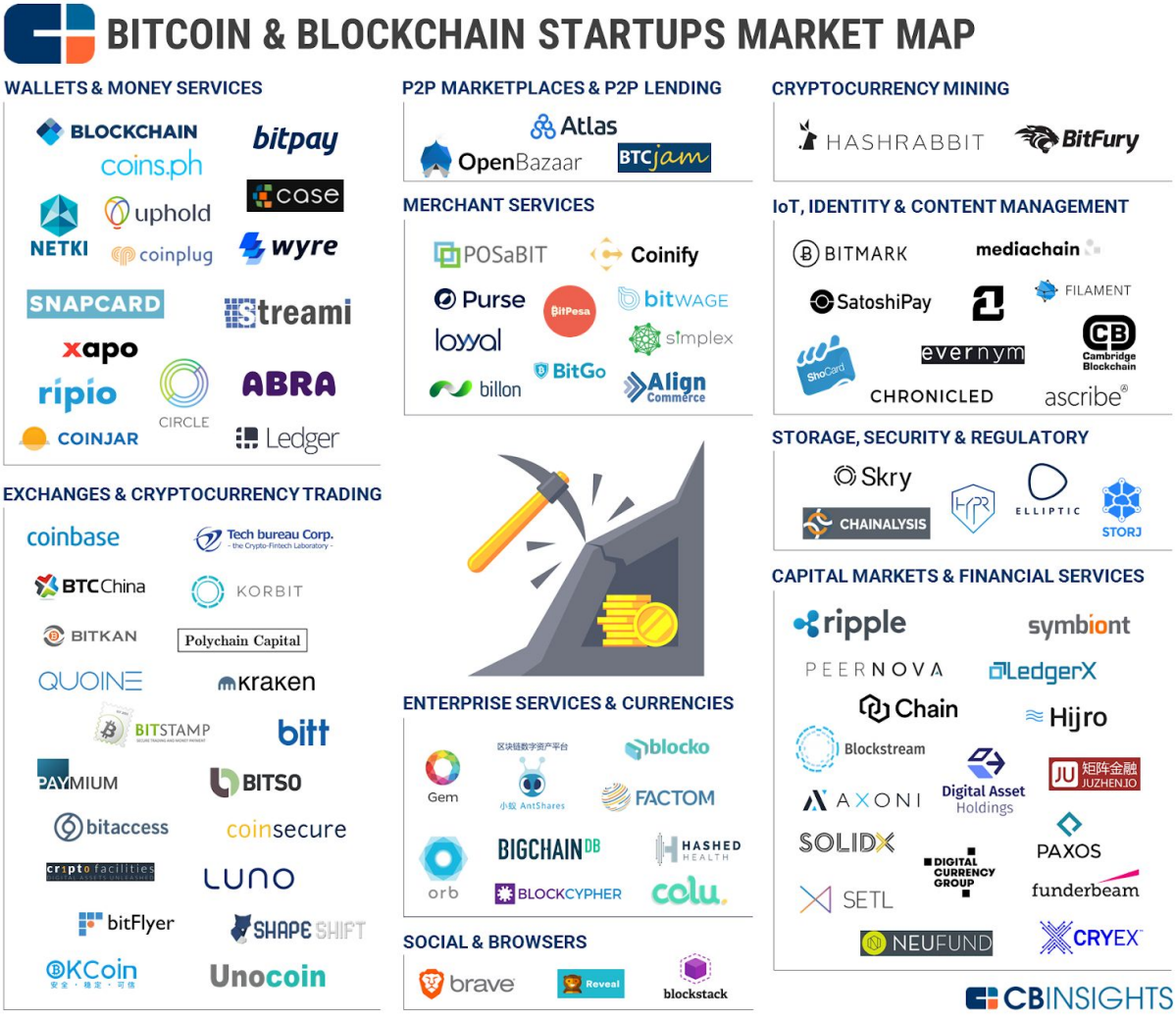
Estonsko a jeho dlouholetý projekt E-estonia se snaží zajistit, že stát, resp. vláda Estonské republiky takzvaně půjde s dobou. Od přelomu tisíciletí již implementovali několik větších projektů v oblasti informačních technologií, jako jsou např. e-Tax (elektronické daně) či i-Voting (elektronické volby). Od roku 2008 se začali zajímat o samotnou technologii blockchainu a v od roku 2012 je blockchain využíván ve veřejných registrech v oblasti zdravotnictví či legislativy [11].

2.1.2.2 Followmyvote.com

Follow my vote je projekt elektronických voleb. Jedná se o open source řešení a je postavený právě na technologii blockchain.

2.1.2.3 Bitgive

Dalším využitím blockchainu je Bitgive. Jedá se o financování dobročinných projektů. Použití blockchainu dává v tomto sektoru smysl především z důvodu jeho transparentnosti.



Obrázek 6. Seznam projektů, které využívají bitcoin a blockchain [6]

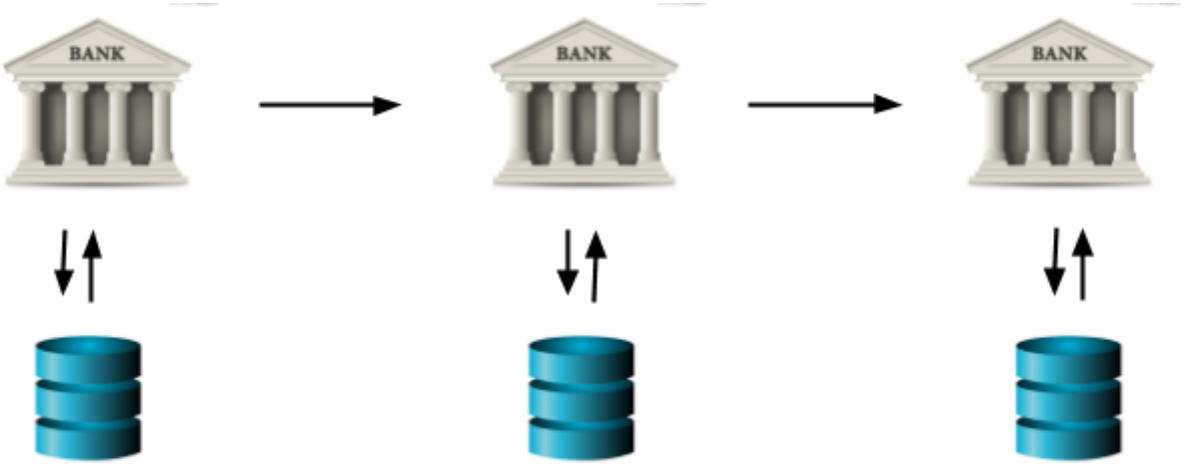
2.2 Ako využiť blockchain

Ako sme spomenuli v sekcií 1.2.1, blockchain je v podstate zdielaná databáza, medzi viacerými stranami, ktoré spolu spolupracujú bez nevyhnutnosti dôvery jeden v druhého. Takže táto technológia je naozaj dobrá v 3 veciach a to transparentnosť, autenticita a auditing.

V tejto kapitole popíšeme kde môže byť ešte blockchain využitý a aké problémy v danom prostredí môže vyriešiť.

2.2.1 Bankový systém

Predstavme si ako príklad prevody peňazí do zahraničia, korešpondenčné bankovníctvo[1].

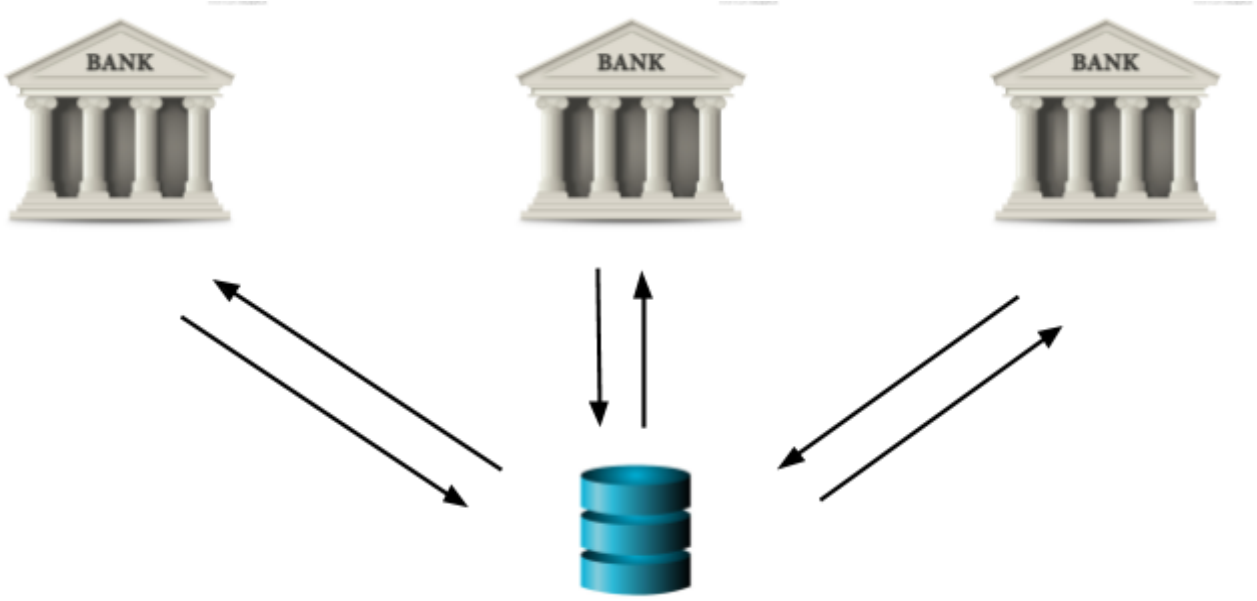


Obrázek 7. Centralizované korešpondenčné bankovníctvo [3][10]

Pre banku nie je uskutočniteľné a pravdepodobne ani výhodné posielať peniaze hocijakej banke v zahraničí z dôvodu rôznych poplatkov, zmlúv a dohôd. Preto v prípade zahraničných prevodov idú peniaze z jednej banky do druhej, odtiaľ do tretej, do štvrtej až do n-tej. Každá z týchto bánk má svoju vlastnú databázu transakcií, do ktorej je potrebné túto transakciu znova vložiť a ktorú je potrebné pravidelne synchronizovať s ostatnými bankami. Takže jednoduchý prevod peňazí do zahraničia je v podstate drahý a pomalý proces.

[1] poskytovanie služieb v mene inej banky

Predstavme si, že všetky banky na svete pripojíme do jednej zdieľanej databázy. Táto databáza by samozrejme nebola verejná ako sú databázy kryptomien, bola by zdieľaná len medzi bankami. V takomto prípade by sa banka odosielateľa mohla priamo spojiť s bankou príjímateľa a proces prevodu by bol rýchlejší a teda aj lacnejší.



Obrázek 8. Decentralizované korešpondenčné bankovníctvo [3][10]

Toto bola len jedna oblasť z bankového sveta, kde by sa blockchain dal využiť. Ďalšími príkladmi by mohli byť napr. viď sekciu 2.2.2.

2.2.2 Sledovanie životného cyklu produktu

Ako už bolo spomínané, každý užívateľ blockchainu vystupuje pod svojím verejným kľúčom, ktorého vlastníctvo dokazuje svojím skúkromným kľúčom, ktorý drží v tajnosti.
Keď výrobca produkt vyrobí, vytvorí transakciu s uníkátnym číslom produktu. Keď ho predá dealerovi, znova prebehne medzi nimi transakcia, podobne ako ked sa posielajú peniaze, len namiesto peňazí sa presúva vlastníctvo produktu. Na základe toho by sme vedeli, kto produkt vyrobil, cez koho bol distribuovaný a kedy sa tomu tak stalo. Uveďme si dva príklady.

2.2.2.1 Lieky

Keď kupujeme v lekárni liek, ako vieme, že daný liek je pravý, že to nie je falošný, pašovaný liek? Ako vieme overiť, že bol naozaj vyrobený certifikovaným výrobcom? Nevieme. Takéto niečo by bolo veľmi ťažko overiteľné, pretože dovoz toho lieku od výrobcu až ku spotrebiteľovi nie je transparentný. Nevieme určiť cez aké medzičlánky daný liek prešiel.

Avšak ak by sme celý proces distribúcie vložili do blockchainu a každá zo zúčastnených strán, ktorá sa podieľa na jeho distribúcií by vytvorila novú transakciu so stranou komu liek ďalej predáva (výrobca - dodávateľ, dodávateľ - predajca), celý životný cyklus daného lieku by bol plne transparentný a jednoducho spätne dohladateľný.

2.2.2.2 Automobily

Keď kupujeme ojazdené auto, vieme so 100% istotou určiť v ktorej krajine bolo auto vyrobené? Koľko majiteľov malo? V akých krajinách bolo jazdené? A asi to najdôležitejšie, vieme koľko má najazdených kilometrov? Odpoveď na tieto otázky pravdepodobne vieme, ale to len preto lebo veríme tomu danému predajcovi, že hovorí pravdu. Znova ide o centralizovaný systém, ktorému chýba transparentnosť.
Tomuto príkladu sa venujeme viac v kapitole 3. Praktické využití blockchainu.

2.3 Smart contracts

Vysvětlení pojmu smart contracts si vysvětlíme na blockchainu, který používá virtuální měna Ethereum. Jak už víme z kapitoly *1.2 Princip fungování*, blockchainová síť obsahuje uzly, kterými jsou samotní uživatelé sítě nebo mineři zpracovávající verifikace transakcí. Smart contracts jsou naprogramované kusy kódu, které provedou nějakou akci, pokud se splní naprogramované podmínky. V síti smart contracts mohou být vytvořené účty (respektive uzly), ke kterým nemá nikdo přístup a po jejich vytvoření je nikdo nemůže upravit. V případě Ethereum blockchainu, smart contract mají stejná práva v síti jako ostatní uživatelé a to odesílání a přijímání Ethereum měny. Smart contract je tedy účet, který je spravován kódem a nikoliv uživatelem.

2.3.1 Crowdfunding smart contract

Příklad smart contractu si ukážeme na způsobu, jakým crowdfundingové portál zprostředkovavají službu startupům a firmám. Představme si, že firma potřebuje 100 000 $ na započetí výroby svého produktu. Lidem se tento produkt líbí a začnou firmě skrz portál přispívat dokud se nenashromáždí požadovaný finanční obnos. Nyní odstraníme z tohoto modelu webový portál, nahradíme ho smart contractem a místo dolarů budeme používat virtuální měnu ethereum. Jednotlivé uzly v síti posílají ethereum smart contractu (uzlu) na sítí. Ten bude mít ve svém kódu napsáno, že pokud se do 14 dní vybere dostatečné množství ethereum, všechny tyto prostředky převede na účet firmy, která bude takto zafinancována. V případě, že se do 14 dní nevybere dostatečné množství ethereum, smart contract automaticky vrátí prostředky všem uzlům (uživatelům), které přispěly. [14]

2.3.2 Co řeší smart contracts

Smart contracts přidávají novou vrstvu automatizace do blockchainu. Jedná se o naprogramované kusy kódu, které provádí operace a převody podle zadaných logických podmínek. S jejich pomocí jsme schopni vytvořit nezávislé a důvěryhodné prostředníky, jakými jsou například v dnešní době právníci a banky. Při prodeji nemovitosti se využívá nezaujaté třetí strany, která zadrží finance za nemovitost na dostatečně dlouho dobu, než je nemovitost převedena na nového majitele. Pokud se nemovitost převede na nového majitele, je prodejci vyplacena smluvní částka. Pokud k převodu nedojde, peníze kupující nikdy neuvidí. Stejným způsobem fungují smart contracts a jejich využití může být mnohem rozsáhlejší.

Užitím smart contracts se odstraní lidská chybovost a zamezí se nežádoucímu chování. To jak se smart contract chová určuje jeho kód a po jeho vytvoření se nedá změnit. Smart contracty se dají seskupovat dohromady a mohou mezi sebou komunikovat. Tohle řešení je vhodné složitějších úkoly, kdy užití pouze jednoho smart contractu by bylo nedostačující.

Potencionální nasazení smart contracts

- crowdfunding
- prodej nemovitostí
- vyplacení pojištění

- vyplacení spoření
- poplatky za elektřinu a plyn

2.3.3 Kde běží smart contracts

Smart contracts jsou obsluhovaný podobně jako verifikace transakcí v blockchainu. Každé provedení nějakého smart contractu znamená spuštění kódu za ním. V reálném světe to znamená, že čím delší je kód smart contractu, tím více se zaplatí minerovi, který jej na svém stroji spustí. Uživatelé tedy platí velmi malé procento z částky kterou převedou pomocí smart contractu.

3. Praktické využití blockchainu

Po představení blockchainu, nastínění toho, co umí a kde se používá nebo může používat, jsme se rozhodli rozvést jedno z teoreticky možných využití podrobněji. V kapitole “Jak využít blockchain” bylo ve zkratce zmíněno, že je možné ho využít při prodeji a sledování automobilů. V této kapitole tento příklad trochu rozebereme.

Představme si, že by tento decentralizovaný systém sloužil tedy pro sledování vozidel. Co všechno by to zahrnovalo? Jednoduše řečeno, celou historii vozidla. Jak detailní historie by to byla, to už by záleželo na rozsahu daného projektu.

3.1 Typy užívateľov

Užívateľov by sme vedeli rozdeliť do dvoch skupín:

1. spotrebiteľ (majiteľ auta)
2. ostatní (výrobcovia, certifikované servisy, STK, notári/banky, ...)

Každý kto bude chcieť uskutočniť transakciu v tomto blockchaine (výroba, kúpa, predaj, kontrola automobilu) musí disponovať kľúčom. Rovnako ako je to v súčasnosti pri obchodovaní s kryptomenami.

Pre užívateľa typu 1. bude tento kľúč vydávať polícia, ktorá bude uchovávať osobné údaje človeka, ktorému kľúč vydala. Rovnako ako je to aj dnes.

Užívateľ typu 2. je užívateľ s nejakým obchodným zámerom (výrobca automobilov, dealer, STK). Preto bude kľúče týmto užívateľom vydávať regulátorský úrad v danej krajine, ktorý si bude uchovávať ich osobné informácie. Ďalej bude úrad spravovať webovú stránku na ktorej bude uvedená príslušnosť verejných kľúčov konkrétnym obchodným

subjektom. Vďaka tomu si môže užívateľ typu 1. zistiť napr. od ktorého dealera jeho auto pochádza.

Aby užívatelia typu 2. boli dostatočne demotivovaní podvádzať, pri výdaji kľúča budú musieť zložiť stávku, povedzme určitá suma peňazí o ktorú automaticky prídu aj s kľúčom a právom naďalej prevádzkovať svoju činnosť v prípade odhalenia podvodu.

3.2 Výrobce

Řekněme, že by to začínalo u výrobce vozidla. Výrobce by vůz, po jeho vyrobení, zadal do systému. Rozsah informací, které by byly v bloku uložené je variabilní, nicméně by zde byly uloženy při nejmenším informace, které by vedly k přesné identifikaci vozidla. Dále se vozidlo dostane k dealerovi vozidel.

3.3 Dealer

Dealer jako takový by do blockchainu zřejmě nijak nezasahoval až do doby, dokud by vůz neprodal. K prodeji vozu by bylo možné využít smart contrat. Prodej by se do databáze zaznamenal, aby byla uložena informace o počtu vlastníků vozidla. Zde by samozřejmě byli uloženy pouze nekonkrétní informace aby se nejednalo o narušení soukromí jednotlivých stran. Pro kupujícího by uvedení citlivých informací znamenalo hrozbu jejich zneužití, ale i pro prodávajícího by existovalo riziko a to únik informací a tudíž narušení konkurenčního boje. Nicméně nám postačí informace, že by auto změnilo majitele. Při prodeji vozu by se mohli zaznamenat rovnou najeté kilometry, protože to právě bude jedna z velkých výhod decentralizovaného transparentního systému. Pokud budeme pravidelně zaznamenávat najeté kilometry, tak snížíme riziko přetočení tachometru a podvodu vůči kupujícímu na minimum.

3.4 STK

Když jsme se dostali právě k problematice přetáčení tachometrů, tak to rovnou můžeme dále rozvést. Pokud chceme efektivně kontrolovat, zda nebyl tachometr přetočený, tak je potřeba informaci o stavu zaznamenávat co nejčastěji. Už jsme uvedli, že by se informace mohla ukládat pokaždé, když auto změní majitele.

Další, kdy by se zaznamenával stav ujetých kilometrů, by bylo při technické kontrole vozidla. Pravidelné technické kontroly jsou povinné a tudíž by se snížil interval na

zadávání stavu na jeden až čtyři roky, podle typu vozidla. Na technické kontrole by pak samozřejmě zaznamenali i informace o stavu vozidla, takže bychom získali další informace o tom, v jakém stavu se vozidlo nacházelo v minulosti.

3.5 Servis

Samozřejmě by bylo velice výhodné, kdyby informace o vozidle museli zaznamenávat i autoservisy a pneuservisy. Tím bychom se ovšem už dostali na úroveň velikosti projektu, který by se vyrovnal EET. Pro servisy by to znamenalo velké množství administrativy navíc, což by představovalo i vyšší náklady a tedy i vyšší ceny. Finanční stránku věci, ale rozebereme v dalších kapitolách.

3.6 Prodej vozu

Predávajúci a kupujúci (identifikovaní svojimi kľúčmi) vytvoria smart contract. Tento smart contract musí niekto potvrdiť - potvrdiť, že daná logická podmienka, ktorá triggeruje prevod auta nastala. Mohlo by ísť o banku alebo aj inú oficiálnu stranu ako napr. notár. Táto strana bude regulovaná úradom, čo znamená, že táto strana opäť (rovnako ako v prípade STK) od daného úradu obdrží kľúč, ktorým bude vytvárať transakcie v našom blockchaine a potvrdzovať contracty.

V prípade, že užívateľ nechce tento smart contract vytvárať sám, čo by sa mohlo stávať hlavne zo začiatku spustenia systému, môže prísť na úrad, kde ho vytvoria, rovnakým spôsobom a cez rovnaké rozhranie ako by to spravil on sám.

3.7 Vláda a úřady

Úrady, ktoré by sa podielali na prevádzke tohto systému:

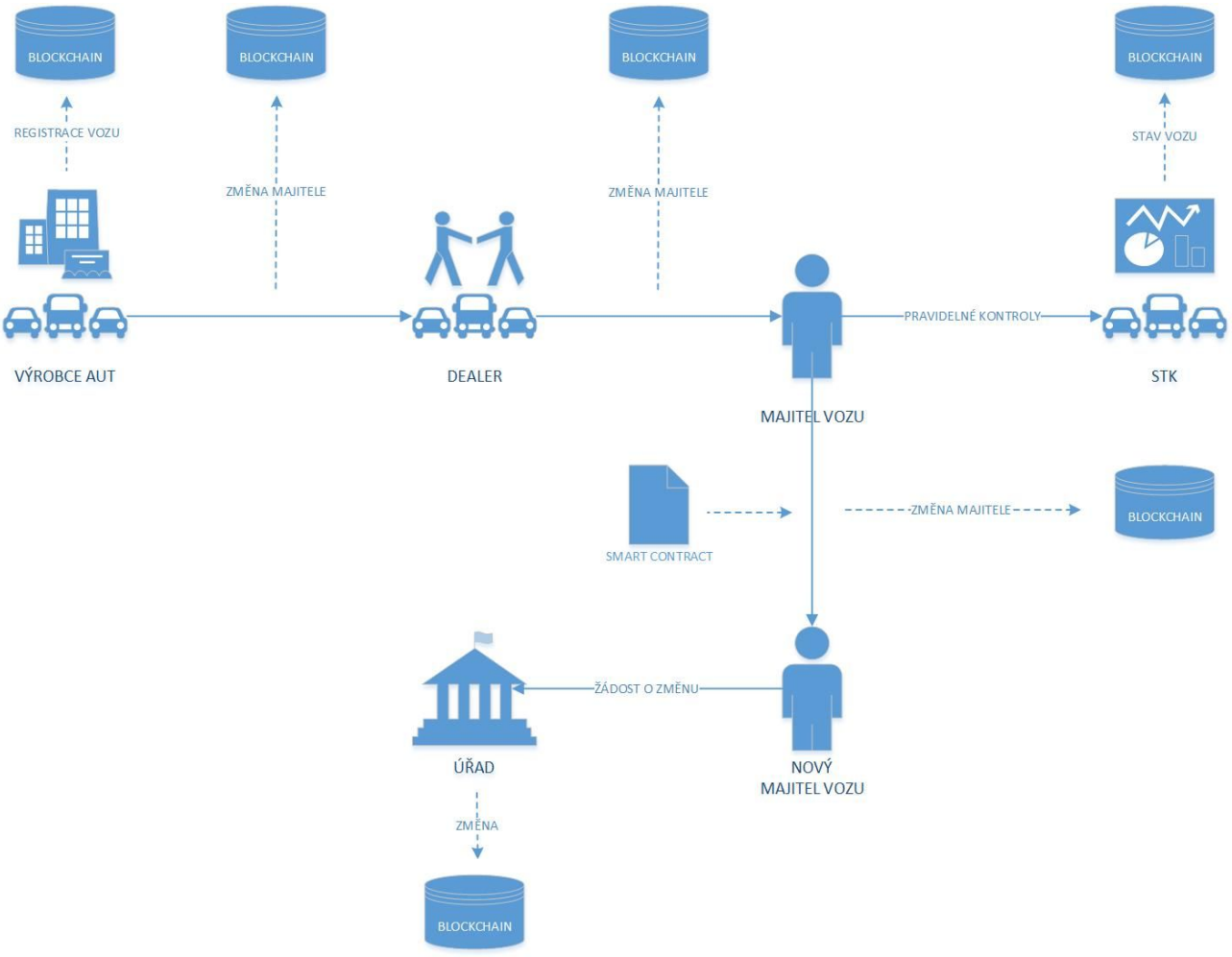
- polícia (vydávanie kľúčov, registrácia osobných údajov)
    - tento orgán by aj naďalej spolupracoval pri činnostiach ako:
        - schvalovanie technických zmien na vozidle
        - sprostredkovanie zániku vozidla
        - a.i.
- regulátorský úrad (nejaký zo súčastných úradov pri prevzal kontrolu) pre regulovanie užívateľov typu 2., viď sekcia 3.1.

3.8 Policajná kontrola

Policajt oskenuje/prepíše EČV, zistí verejný kľúč majiteľa (verejná info z blockchainu) a v policajnej databáze nájde osobné informácie daného človeka (policajné orgány ich majú, lebo tie kľúče vydávajú, viď 3.1) - táto info je už privátna, len polícia môže zistiť kto sa naozaj "skrýva" za daným kľúčom.

3.9 Proces

Přístupů, jak tento projekt uchopit a jak přesně nastavit proces je velké množství. Výše byl postupně popsán jeden z možných scénářů, ale rozhodně není nikde řečeno, že je to ten nejlepší. Níže se můžete podívat na grafické znázornění procesu, který je nastíněn v průběhu kapitoly tři.



Obrázek 9. Jeden z možných procesů při použití blockchainu k sledování vozidel.

3.10 Výhody

V prípade naimplementovania takéhoto riešenia registra vozidiel by majitelia áut:

- získali prehľad nad históriou vozidla (z akej krajiny pochádza, koľko má najazdených kilometrov, …)
- nepotrebovali žiadať o nové EČV pri prepise vozidla. Auto by malo jedno EČV po celý svoj život.
- nepotrebovali žiadať o nový technický preukaz pri prepise vozdila. Všetky informácie sú uvedené v blockchaine.
- nemuseli chodiť na úrady, strácať svoj čas a podstupovať veľa-krát zbytočne byrokratický proces.

Na základe hore zmieneného by majitelia áut ušetrili čas, peniaze a získali istotu, že vedia aký automobil v skutočnosti vlastnia.

Dané riešenie je aj ekologicky čistejšie, vďaka menšiemu papierovaniu a zastaveniu výroby nových a nových EČV.

4. Závěr

Cílem této práce bylo objasnění technologie blockchainu, představení jeho aktuálního nasazení a potenciální využití do budoucna, kde tato technologie dáva smysl. Teoreticky jsme probrali princip fungování a typy algoritmů, které blockchain může využívat, popsali jsme jak probíhají transakce, jaké typy uzlů v síti jsou a proces vytvoření blockchainu a samotných bloků. Následně jsme zmínili projekty, kde je blockchain využíván, uvedli jsme kde by se dal využít a probrali jsme rozšíření blockchainu o tzv. smart contracts. Poslední kapitola obsahuje detailnější nasazení pro námi zvolenou problematiku, kde by podle nás stálo zato blockchain nasadit. Tato práce dává čtenáři solidní teoretický základ a pochopení celkového fungování popsané technologie a předává nutný předpoklad pro vytvoření praktické aplikace pro zvolenou problematiku v poslední kapitole.

5. SEZNAM POUŽITÝCH ZDROJŮ

[1] https://en.bitcoin.it/wiki/Hashcash

[2] https://en.bitcoin.it/wiki/Proof_of_work

[3] https://digiconomist.net/bitcoin-energy-consumption

[4] https://coinscage.com/best-bitcoin-mining-pools/

[5] https://coinmarketcap.com/currencies/dash/

[6] https://bit.ly/SHRAgK

[7] https://www.forbes.com/forbes/1999/1101/6411390a.html#23e5b5cf715f

[8] https://www.anf.es/pdf/Haber_Stornetta.pdf

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

[10] https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin…

[11] https://e-estonia.com/

[12] https://www.youtube.com/watch?v=93E_GzvpMA0

[13] https://www.youtube.com/watch?v=SSo_EIwHSd4&t=8s

[14] https://www.youtube.com/watch?v=w9WLo33KfCY

6. SEZNAM POUŽITÝCH ILUSTRACÍ

[1] https://steemitimages.com/0x0/http://i.imgur.com/znMDcKR.png

[2] https://blockgeeks.com/wp-content/uploads/2016/09/image-4-276x300.png

[3] https://goo.gl/images/WhkMLU

[4] https://en.bitcoin.it/wiki/Proof_of_work

[5] https://digiconomist.net/bitcoin-energy-consumption

[6] https://cbi-blog.s3.amazonaws.com/blog/wp-content/uploads/…

[7] https://coinscage.com/best-bitcoin-mining-pools/

[10] http://www.panama-offshore-services.com/wp-content/uploads/panama-bank.jpg