FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Možnosti praktického využití technologie Blockchain
Student:	Dušan Trnka
Vedoucí:	Ing. Pavel Náplava
Studijní program:	Informatika
Studijní obor:	Informační systémy a management
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2018/19

Pokyny pro vypracování

Analyzujte možnosti praktického využití technologie Blockchain pro realizaci IT systémů. Zaměřte se především na srovnání různých typů technologie a vytvořte průvodce, který pomůže zájemcům vyhodnotit přínosnost technologie pro realizaci jejich IT projektu a vybrat odpovídající architekturu. Postupujte následovně:
1) Analyzujte a popište klíčové vlastnosti technologie Blockchain.
2) Analyzujte a popište odlišnosti od jiných, běžně používaných, technologií pro realizaci IT systémů.
3) Identifikujte a srovnejte různé typy technologie a architektury Blockchain.
4) Vytvořte interaktivního průvodce, který pomůže zájemcům o technologii identifikovat smysluplnost využití technologie a doporučit vhodnou architekturu technologie.
5) Průvodce demonstrujte na vybraných praktických příkladech (budou vybrány po dohodě s vedoucím práce).

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 10. ledna 2018

Poďakovanie

Chcel by som poďakovať vedúcemu Ing. Pavelovi Náplavovi, bez ktorého by som túto prácu pravdepodobne nedotiahol do konca. Takisto mojím kamarátom ktorý mi pomohli s korektúrou. A rovnako by som rád poďakoval vedeniu ČVUT za to, že môžem túto prácu písať v mojom rodnom jazyku.

Prehlásenie

Prehlasujem, že som predloženú prácu vypracoval(a) samostatne a že som uviedol(uviedla) všetky informačné zdroje v súlade s Metodickým pokynom o etickej príprave vysokoškolských záverečných prác.

Beriem na vedomie, že sa na moju prácu vzťahujú práva a povinnosti vyplývajúce zo zákona č. 121/2000 Sb., autorského zákona, v znení neskorších predpisov, a skutočnosť, že České vysoké učení technické v Praze má právo na uzavrenie licenčnej zmluvy o použití tejto práce ako školského diela podľa § 60 odst. 1 autorského zákona.

V Prahe 14. mája 2018 .....

Odkaz na túto prácu

Trnka, Dušan. *Možnosti praktického využitia technológie Blockchain.* Bakalárska práca. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2018.

Abstrakt

Blockchain je novovznikajúca technológia, ktorá prináša nový spôsob ako vytvoriť decentralizovanú a autonómnu databázu. Túto technológiu je možné zaregistrovať predovšetkým v súvislosti s kryptomenami, no blockchain prináša mnoho iných vylepšení ktoré sa dajú zužitkovať no pre ich komplexnosť ešte neboli centrom pozornosti pre širokú verejnosť. Najväčším prínosom sú takzvané smart kontrakty, kde sa jedná o záväzok, ktorý je vykonávaný autonómne podľa preddefinovaných pravidiel. Tieto smart kontrakty umožňujú vytvárať komplexnejšie decentralizované aplikácie (dApps) či autonómne organizácie (DAO), ktoré dokážu fungovať autonómne a bezpečne na blockchain technológii.

Svet blockchain technológie je veľmi dynamický a vo veľmi krátkom čase tu vznikla obrovská diverzita blockchain riešení, ktoré sú vhodné na veľmi rozličné prípady použitia. Cieľom tejto práce je predstaviť hlavných hráčov na scéne blockchain technológií, a ujasniť čitateľovi aké riešenia prinášajú. Následne je na základe tejto štúdie vytvorený sprievodca, ktorý ma pomôcť človeku určiť, či potrebuje blockchain poprípade akú architektúru a prečo. Fungovanie sprievodcu je vysvetlené na modelových prípadoch a jednotlivé otázky, detailne vysvetlené aby používateľ pochopil rozhodnutia, ktoré musí urobiť pri výbere blockchain architektúry.

Klíčová slova Blockchain, distribuovaná sieť, decentralizované hlasovacie mechanizmy, zmysluplnosť blockchainu, sprievodca blockchainu, analýza architektúry

Abstract

A blockchain is a newly quick developing technology, which brings a new way of thinking when building decentralized, autonomous databases. You might hear of this technology in association with cryptocurrencies, but the blockchain technology brings much more than just digital money. It advances the field of smart contracts from idea to actually working ecosystem. This smart contracts which are digitalized and autonomous form of normal contracts allow developers to build decentralized applications (dApps) and later we will see decentralized autonomous organizations (DAO). The number of people interested in the blockchain usage apart from cryptocurrency has been rapidly growing in a recent couple of months. We have gotten to the stage, where we have so many different blockchain systems that it is really hard to navigate through for people outside of this business. And new solutions are being developed every month.

The goal of this thesis is to explain main technical features of a blockchain and explain to the reader which architecture is suitable for what. According to this research, a decision guide has been created. Which will help the user determine whether to use blockchain for their problem and if yes which architecture and why. Decision guide is explained on various examples with a background for the question asked and decisions the user has to make.

Keywords Blockchain, distributed network, consensus mechanism, architecture analysis, decentralized consensus, decentralized network

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Blockchain, je takmer nemožné toto slovo v dnešnej dobre nezachytiť. Čítali ste príspevky o tom ako je blockchain revolučná technológia, ktorá zmení celý svet. Pozorne ste sledovali ako rastie cena Bitcoinu[1] a s ešte pozornejšie, keď začala prudko klesať. Neprešiel deň, kedy by ste neľutovali prečo ste tie Bitcoiny nenakúpili skôr. A možno ste ich kupovať vôbec nemali, kto vie. Táto práca je napísaná pre ľudí, ktorý chcú nazrieť do útrob technológie ktorá spôsobila toľký ošiaľ. Pokúsim sa demystifikovať túto technológiu, ktorú pôvodne čistú a revolučnú veľmi ovplyvňujú korporácie a ich tlak na rýchly vývoj. Ale takisto aj presvedčiť tých, ktorý neúnavne tvrdia, že blockchain je ďalšia bublina a netreba do nej investovať svoj čas.

Táto nová technológia sa veľmi dynamicky mení a vyvíja. Prvý krát sa objavila v roku 2008, keď bol publikovaný prvý odborno-technický návrh popisujúci bitcoin technológiu a jej pravidla fungovania. Bol to veľmi nadčasový a elegantne napísaný návrh tak ako celé prvotné riešenie bitcoin blockchainu. Jej autor žiaľ nie je známy. Pod prácu sa síce podpísal Satoshi Nakamoto, no netušíme kto sa skrýva pod týmto pseudonymom. Stále sa vedú špekulácie kto to mohol byť a pravdepodobne sa to nikdy nedozvieme.

Blockchain sa za takmer 10 rokov od publikovania prvého návrhu drasticky rozrástol, dnes už nikto nepochybuje, že táto technológia tu zostane a bude sa ďalej vyvíjať, pretože do vývoja blockchain technológia investovali najväčšie firmy sveta ako aj neskutočne množstvo nadšencov a vývojárov. Za úspechom tejto technológie stojí predovšetkým jej elegantnosť riešenia a prvotná jednoduchá myšlienka. Blockchain je prakticky distribuovaná databáza, ktorá využíva prvky modernej kryptografie a výpočtovej sily. Momentálne, už existuje niekoľko úplne odlišných implementácií blockchain technológie, ktoré v tejto práci priblížim a navzájom porovnám.

Vzhľadom na to, že blockchain terminológia nemá ustálené preklady do slovenčiny, budem sa tieto výrazy snažiť preložiť do slovenčiny ako najlepšie budem môcť. V prípade, že v slovenčine neexistuje adekvátny preklad budem používať anglický výraz. Rovnako sú všetky zdroje a literatúra z ktorej čerpám

v angličtine a preto je všetko preložené najlepším možným prekladom autorom tejto práce. Tieto preklady a hlavne citácie sa snažia čo najlepšie vystihnúť myšlienku autora zahraničnej literatúry.

Štruktúra práce

Postupne vysvetlím prečo a ako blockchain technológia vznikla. Následne rozoberiem pôvodný Bitcoin white paper a vysvetlím základne ideály s ktorými vznikol prvý blockchain. V druhej kapitole predstavím rôzne typy blockchain architektúry ako aj rozdielne implementácie hlasovacích systémov. V tretej kapitole sa dostanem ku možným dopadom tejto technológie na bankový sektor a iné odvetvia. Na záver predstavím rozhodovací model zmysluplnosti použitia technológie blockchain na reálnych príkladoch.

Kapitola 1

Cieľ práce

Hlavným cieľom tejto práce je pomôcť čitateľovi odpovedať na otázku: či potrebujem blockchain technológiu? A ak áno akú architektúru. Vytvorením rozhodovacích stromov, ktoré užívateľa prevedú rozhodovacím procesom, zjednodušíme komplexnú literatúru na základné otázky na ktoré dokáže odpovedať aj človek ktorý sa veľmi nevyzná v blockchain technológiách. Následným umiestnením výsledku do rozdelenia blockchain technológie ukážeme používateľovi celkový pohľad na čo by sa mal zamerať a čo zvážiť. Celý tento rozhodovací proces bude prebiehať pomocou webovej aplikácie.

Kapitola 2

Princípy blockchainu

Slovo blockchain sa skladá z dvoch slov a to blok a chain. V preklade blok a reťaz, tieto pomenovania vymyslel Satoshi Nakamoto, keď vytváral prvý blockchain. Symbolizuje to skutočnosť, že sa jednotlivé transakcie uchovávajú v blokoch a tie bloky sa naväzujú na predošlý blok a vytvára to reťaz blokov. Blockchain je dynamicky meniaca sa technológia a práve preto si v prvej kapitole pripomenieme s akými princípmi vznikol prvý blockchain a ako sa tieto princípy dnes už mnohými implementáciami vôbec nedodržujú respektíve ignorujú. Nasledujúca kapitola teda rozoberá Bitcoin blockchain a vychádza hlavne z knižnej predlohy.[2]

2.1 Integrita siete

„Dôvera prichádza zvnútra nie z vonkajška.“[strana 30][2] Integrita je stav keď môžem veriť, že druhá strana vykoná, to čo sa od nej očakáva. Môže ísť o zmenu vlastníctva, urobiť správne rozhodnutie alebo napríklad vyvodiť následky. A táto skutočnosť v blockchain technológiách nezávisí na jedincovi alebo inštitúcii ale je kolektívne vyžadovaná sieťou ako celkom. Integrita je zakódovaná do každého kroku procesu a fungovania siete a následne táto integrita vytvára dôveru v sieť ako celku. Ak chce niekto tieto mechanizmy integrity obísť nemôže, pretože je to buď nemožné alebo je to pre neho časovo, finančne alebo inak nevýhodné.

Počítače sú užasne stroje, ktoré dokážu okrem iného dokonale replikovať všetky svoje digitálne dáta. Uveďme si príklad, že pošlete naraz rovnakú platbu subjektu A a zároveň subjektu B. V dnešnom svete Vám banka prvú platbu povolí a druhú zamietne, pretože nemáte dostatok prostriedkov. Celý dnešný platobný systém stojí na dôvere v banku teda centrálnu autoritu, ktorá autorizuje platby. Ak chceme dosiahnuť pravú integritu distribuovanej siete, nemôžeme mať centrálnu autoritu. A to nás opäť raz dostáva pred otázku ako vyriešime problém viacnásobného míňania, ktorý existencia centrálnej autority kompletne obchádza.

Túto otázku si položil aj Satoshi Nakamoto a vyriešil ju nečakane elegantne, keď spojil mechanizmus hlasovania (consensus mechanism) v distribuovaných sieťach a pokročilú kryptografiu. Použil princíp, kde sieť časovým údajom opečiatkuje prvé použitie daného aktíva a všetky nasledujúce odmietne (pokiaľ sa platba definitívne neuverejní na sieti). Príslušníci siete ktorý chcú a majú nato dostatočnú výpočtovú silu môžu overovať uskutočnené transakcie. Vždy si pozbierajú ešte nefinalizované transakcie, poukladajú ich do kontajneru ktorý voláme blok. Tento blok sa pripojí na reťaz predošlých blokov. Takýto proces sa opakuje v takmer pravidelnom intervale. Každý blok musí byť pripojený na reťaz predošlých blokov, aby bol platný. Ako náhle je blok pripojený na sekvenciu predošlých blokov, všetky transakcie sú definitívne a verejne zaznamenané a dohľadateľné.

Týmto procesom Satoshi dosiahol nielen prekonanie problému viacnásobného míňania ale aj potrebu mať centrálnu autoritu. Keďže sa účastníci môžu slobodne rozhodnúť, či sa budú podieľať na fungovaní siete. Kód ktorý si účastníci spúšťajú je open-source a môže ho používať každý. Satoshi chcel eliminovať rozdielne interpretácie pravdy a preto to prenechal na kód, ktorý je jednoznačný. Chcel aby sa sieť bola schopná dohodnúť sama so sebou, čo sa vlastne stalo a čo je pravda. Prenechal počítače aby sa algoritmický dohodli bez zásahu ľudského faktoru. Tento mechanizmus sa ukázal ako najkritickejšia časť celého blockchainu.

Satoshi použil takzvaný proof–of–work (PoW) mechanizmus. Vychádzal z toho, že sa nevieme spoľahnúť na identitu jednotlivých používateľov a preto ani nato, kto vytvorí ďalší blok. Preto namiesto toho každý blok predstavuje nejaký problém, ktorý je ťažké vyriešiť ale jednoduché overiť správnosť jeho riešenia. Účastníci sú dohodnutý, že kto nájde ako prvý riešenie problému tak môže vytvoriť nový blok. Vyriešenie takého problému je veľmi výpočtovo náročné a užívateľ musí spotrebovať značné množstvo výpočtovej sily, respektíve elektrickej energie. Za každý vytvorený blok dostáva jeho autor určitú finančnú odmenu vo forme bitcoin tokenov.

2.2 Distribúcia výpočtovej sily

Blockchain ako taký je distribuovaní v peer–to–peer sieti. To znamená, že ak vypadne nejaký užívateľ nijako to neovplyvní sieť. Žiadny jedinec nedokáže vypnúť sieť. Ak sa niekto pokúsi vypojiť jedinca alebo menšiu skupinu, sieť ako taká bude fungovať ďalej. Až do momentu, keď sa viac ako polovica užívateľov siete pokúsi prevládnuť menšinu, no v tom prípade budú všetci vidieť čo sa deje.

Od vzniku internetu sme svedkami toho ako veľké korporácie zneužívajú a snažia sa zarobiť na dôvere ľudí. Vo svete kde veľké korporácie zhromažďujú najrôznejšie informácie a vyhodnocujú ich, aby si zvýšili svoje zisky. Odovzdávajú informácie vládnym agentúram bez súhlasu používateľa alebo vykonávajú

plošné zmeny bez súhlasu používateľa. Je veľmi ťažké si predstaviť, že to takto nemusí byť.

Blockchain je vďaka svojej štruktúre chránený proti takýmto zásahom vyššej entity ako napríklad štátu, vládnej agentúry alebo nadnárodnej korporácie. Vďaka PoW mechanizmu, by takýto zásah potreboval neskutočne veľa výpočtovej sily a tým pádom aj elektrickej energie. Potencionálne finančné zisky útočníka by tým pádom nedokázali pokryť ani náklad na útok. Preto je to vysoko nepravdepodobné. Josh Fairfield to pomenoval, že *„neexistuje žiadny sprostredkovateľ po ktorom by sa mohlo ísť.“*[strana 34][2]Blockchain sa nachádza všade a užívatelia ho dobrovoľne udržujú online a prenajímajú mu svoju výpočtovú silu. Každá transakcia, ktorá je vysielaná do siete, prešla potrebnou validáciou a verifikáciou. Žiadna tretia strana si nič neuchováva a preto to nemôže ani zneužiť proti jedincovi.

Satoshi zašiel ešte ďalej a zviazal distribúciu nových tokenov (bitcoinov) s vznikom nového bloku. Počet týchto bitcoinov obmedzil na 21 miliónov BTC. Kde práve používatelia, ktorý pomáhajú sieti sú zato odmeňovaný. Týmto vyriešil problém distribúcie BTC. Neexistuje tu žiadna centrálna banka, európska banka alebo inštitúcia, ktorá by vydávala bitcoin. Rozdeľuje si ich sieť sama, tým ktorý sa o ňu starajú a spôsobom, že je ich počet fixný, nedá sa s tým nijak manipulovať. Podľa odhadov v roku 2140 sa odblokuje posledný bitcoin a po tom už nebudú dostávať ťažitelia žiadnu odmenu, ale iba províziu ktorú platia užívatelia za transakciu.[]

2.3 Správny stimul

Nemôžeme sa diviť, že v krajine, kde je každý navádzaný na to, aby klamal a podvádzal, každý klame a podvádza. Keďže, sa nejedná o počítačový model ale ľudskú psychológiu tieto poznatky z behaviorálnej psychológie sa dajú uplatniť aj na distribuovanú autonómnu transakčnú sieť akou je blockchain. Veľké svetové banky zneužívali systém pokiaľ sa nezlomil, pretože podľa Joseph-a Stinglitz-a *„hlavným stimulom pre väčšinu vrcholových manažérov boli krátkozraké ciele s veľkým ziskom, ktoré prinášali príliš veľké riskovanie pri požičiavaní peňazí“*. Načo doplácali hlavne tí najchudobnejší.[3]

Podľa Ernst & Young prieskumu, takmer tri štvrtiny manažérov priznali, že zhromažďovali dáta o svojich používateľoch aby zlepšili svoj biznis a takmer 80% z nich tvrdí, že si zvýšili svoje zisky na základe znalostí vyťažených z týchto dát. No problém nastáva, keď niekto hackne tieto firmy, pretože sú to zákazníci a majitelia ukradnutých kariet, ktorý musia všetko nanovo zariadiť aby sa vyhli zneužitiu ich účtu.[4]

Satoshi rozumel teórií hier a vedel ako naviesť používateľov, aby boli čestný a nepodvádzali. Pretože podvádzaním nedokázali získať viac ako tým, že boli čestný sa toto správanie úplne vytratilo. Satoshi napísal: „Podľa pravidla, prvá transakcie v bloku je špeciálna transakcia, ktorá vytvára nový token

ktorý dostane tvorca bloku. Takýto spôsobom pridáva pozitívny stimul pre užívateľov aby sieť podporovali“[1] Tým, že používateľ ktorý ako prvý vyťaží blok dostane odmenu v BTC, je v jeho záujme udržiavať túto sieť čo najdlhšie a preto bude prispievať k jej správnemu fungovaniu tým, že nebude podvádzať. Dokázal ľudské hodnoty presunúť z tých krátkodobých na dlhodobé, preto mnoho minerov investovalo do kvalitného hardware-u a hľadajú spôsoby ako to robiť čo najefektívnejšie. Pretože správne fungovanie siete je v záujme všetkých zúčastnených a preto vždy dokážu identifikovať toho kto podvádza. Napríklad v momente, keď sa vyťažia zároveň dva nové bloky v rovnakej úrovni, sieť sa musí rozhodnúť ktorý bude validný a začnú na ňom ťažiť nový blok. Väčšinou je to úplná náhoda, respektíve sa vyberá blok, ktorý ma najväčší potenciál byť validným. Nie je v nikoho záujme mať dve rovnako dlhé reťaze, pretože by museli rozdeliť svoju výpočtovú silu a validovať pre obidve reťaze pokiaľ sa jedna nestane aktuálnejšiu ako ta druhá. Pod aktuálnosťou sa myslí najmä dĺžka reťaze, pretože čím je reťaz dlhšia tým obsahuje viacej transakcií a keďže sa nové bloky pridávajú systémom reťazenia, dlhšia reťaz je tá aktuálnejšia.

2.4 Bezpečnosť

Všetky bezpečnostné prvky sú zakódované priamo do siete, neexistuje jediný bod zlyhania. Táto skutočnosť poskytuje sieti nielen rúško anonymity ale takisto aj dôveryhodnosť a overiteľnosť. Pretože každý kto sa chce pripojiť, musí používať kryptografiu.

Žijeme vo svete kde na používateľa internetu číha nebezpečie na každom kroku, či už sa bavíme o stiahnutí vírusu z nedôveryhodného zdroja, phishing e-mailoch alebo zhromažďovanie citlivých dát tretími stranami. Mnohé firmy, ktoré zhromažďujú citlivé informácie ako osobné údaje, bankové údaje, zdravotnú históriu a mnoho ďalších, sa nevenujú ich zabezpečeniu na plný úväzok.

IBM na základe štúdie zistila, že priemerná krádež dát stojí okradnutého približne 3.8 milióna dolárov.[5] Priemerné náklady na jedinca, ktorému ukradli zdravotnú históriu je približne 13,500 dolárov.[6] A nikto nedokáže predpovedať, kde sa udeje nasledujúca krádež. Firmy nedokážu bezpečne uchovávať citlivé informácie, ktoré im poskytujeme. A útoky sa neustále stupňujú, pretože sa z toho stal biznis.

Satoshi použil dobre známu infraštruktúru verejného-súkromného kľúča (PKI)[7]. A vyžaduje od všetkých účastníkov siete aby ho používali. PKI je pokročilý kryptografický systém dvoch kľúčov, ktoré sú kryptograficky spárované ale fyzicky sa od seba líšia, každý ma inú funkciu. Každý účastník má verejný kľúč, ktorý ako napovedá názov vedia všetci a súkromný kľúč, ktorý je potrebné si patrične chrániť pretože dokáže autorizovať platby.

2.5 Súkromie

Ľudia by mali vlastniť svoje údaje. Nielen preto, že je to základné ľudské právo a základný kameň slobodnej spoločnosti, ale aj preto, že firmy ukázali, že nevedia tieto údaje uchrániť pred krádežou. Dnes vlastní Vaše údaje, komukoľvek ich poskytnete a môže si s nimi robiť čo chce. Mnoho firiem využíva znalostí získané z big dáta na zlepšenie ich zisku a zvýšenie tržieb. Mnoho firiem neinvestuje do ochrany týchto dát dostatočne prostriedky.

Satoshi vytvoril systém, kde nepotrebujeme poznať reálnu identitu užívateľa. To znamená, že nikto nemusel udávať svoje meno, dátum narodenia alebo e-mail aby mohol bitcoin používať. Používajú sa iba verejné kľúče, ktoré sú síce jednoznačným identifikátorom v rámci blockchainu no pokiaľ ich nemá čo spojiť so skutočným svetom jedná sa o podstatne neidentifikovateľný údaj (existujú spôsoby ako sa dá zistiť identita používateľa, ktoré rozoberám v ďalšej kapitole). Preto skutočnosť, že všetky transakcie sú verejne prístupné a dohľadateľné nepredstavuje zásadný problém.

2.6 Zachovanie práv

Každý z vás si už určite niekedy zadarmo stiahol svoju obľúbenú pesničku z internetu alebo nebodaj film ktorý sa práve premieta v kinách. Problém pirátstva je celosvetový aj, keď sa s ním veľa krajín snažilo vysporiadať, nie vždy sa to konkrétne podarilo. Hlavným argumentom týchto lobistických skupín bolo, že ľudia si nelegálne kopírujú ich diela, pretože nechcú za ne platiť. Opak bol pravdou a ukázalo sa to časom, keď nastúpili streamovacie služby. S príchodom Spotify investori a lobovacie skupiny pochopili, že ľudia sú ochotný platiť ale musí to byť jednoduché a prístupné a transparentné. Tak to bolo aj so Spotify, kde sme si všetci mysleli ako začne táto služba odmeňovať tvorcov za ich diela. Lenže ako to už v biznise chodí s globálnou expanziou a narastajucími platiacimi užívateľmi sa biznis plány zmenili. Dnes síce Spotify odmeňuje tvorcov, ale nikdy sme sa nedozvedeli koľko im teda vlastne dávajú z predplatného zákazníkov. Tvorcovia ako Taylor Swift to aj verejne priznali a bojkotovali túto službu stiahnutím všetkých svojich skladieb.[8] Nespokojnosť na oboch stranách a prostredník sa snaží nájsť nejaký kompromis. Aj v tejto sfére je perspektíva blockchainu veľmi optimistická, pretože má možnosť odstrániť prostredníka nielen v finančnej sfére, ale aj v tej hudobnej alebo filmovej.

Predstavte si, že by ste platili za pesničku priamo jej autorovi. Žiadny prostredník iba vy a vaše peniaze a na druhej strane tvorca a jeho tvorba. S časovými pečiatkami troškou najnovšej kryptografie a nezmeniteľným registrom všetkých diel, to už neznie ako sen ale ako riešenie a plán. Elimináciou prostredníka by sa dosiahla konečne trvajúca spokojnosť na oboch stranách. Tvorcov by to motivovalo vytvárať lepšie diela, keby boli za ich čas adekvátne

zaplatený. Určite sa pýtate v čom je tento systém iný ako napríklad klasické CD nosiče. V jednom a zásadnom bode, naše zvyky a spôsob ako počúvame napríklad hudbu sa zásadne zmenili. Všetci chceme mať hudbu pri sebe a možnosť pustiť si ju kedykoľvek a bezdrôtovo do svojich zatiaľ ešte „slúchadiel“, a pretože, nám presne toto umožňujú smartfóny musíme hudbu a eventuálne aj vlastníctvo digitálnych diel presunúť do digitálnej podoby a formy.

2.7 Inklúzia

Ekonomika funguje najlepšie, keď funguje pre všetkých. Ľudia v mnohých kútoch sveta nie sú súčasťou globálnej ekonomiky, 2 miliardy ľudí v rozvinutých krajinách nemajú ani účet v banke.[9] Internet a globalizácia priniesla veľký pokrok pre rozvojové krajiny, či už podpora ekonomiky vytváraním pracovných miest v týchto krajinách alebo vytváraním prostredia pre budúcich podnikateľov. No však nie je dosť, treba vyriešiť to aby mal každý človek prístup k finančným inštitúciám. Mnoho ľudí si nemôže dovoliť otvoriť účet pretože, potrebujú nejaký minimálny vklad, takisto minimálna cena za transakciu je veľký limitujúci faktor. V krajinách kde ľudia žijú s 2 dolármi na deň je naša hodnota peňazí mylná.

Systém ktorý je prístupný pre všetkých a nemá žiadne počiatočne náklady by mohol byť riešením, pre krajiny kde je lokálna mena príliš nestabilná alebo cez národnú banku ju ovládajú mnohokrát skorumpovaný a neodvolateľný úradníci. Blockchain technológia predstavuje spôsob, kde by nebola potrebná žiadna verifikácia občana, bydliska alebo majetku, kde by mohol ktokoľvek poslať komukoľvek platbu aj cez hranice a nezaplatil by pritom obrovské poplatky. Presne tieto možnosti prináša blockchain v prípade, že sa rozrastie do globálnej platformy. Možnosti pripojiť rozvíjajúce sa krajiny do svetovej ekonomiky a globálneho finančného trhu. Pretože blockchain má byť pre všetkých a slúžiť všetkým. Taká bola prvotná filozofia pri vzniku prvého blockchainu (Bitcoin).

2.8 Zhrnutie

V tejto kapitole som vysvetlil základné princípy na ktorých bol postavený prvý blockchain. Tieto princípy sa dnes nie vždy dodržiavajú. Predovšetkým distribúcia výpočtovej sily je veľmi zložitý problém, ktorý sa mnohé spoločnosti rozhodli zjednodušiť obmedzením, kto môže overovať transakcie. Čitateľ si z tejto kapitoly odniesol predovšetkým porozumenie čo všetko dokáže blockchain vyriešiť. V nasledujúcej kapitole sa budú rozoberať rôzne implementácie blockchain technológie.

Kapitola 3

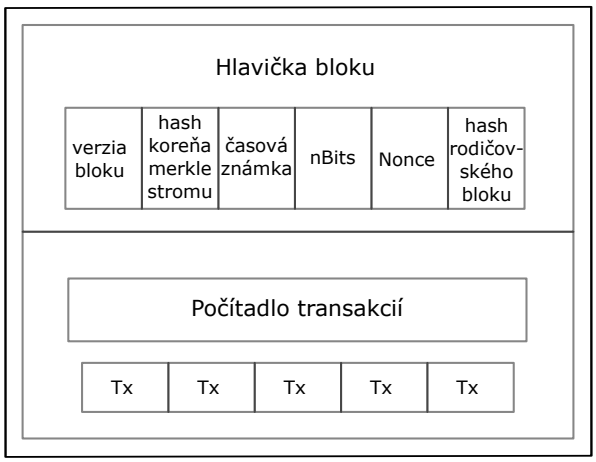
Blockchain architektúra

Blockchain alebo inak reťaz blokov sú za sebou usporiadané jednotlivé bloky, ktoré mimo iné obsahujú transakcie. Tieto bloky sú kryptograficky previazané a nemôžu byť usporiadané v inom poradí. Táto štruktúra je dosiahnutá tým, že hash predošlého bloku je použitý pri hashovaní toho nasledujúceho. Základnou stavebnou jednotkou je teda blok.

3.0.1 Blok

Ako môžete vidieť na obrázku 3.1 blok obsahuje niekoľko súčasti a to konkrétne:

- verzia bloku - jedná o určenie verzie pravidiel, ktoré má blok dodržiavať
- hash koreňa merkle stromu - jedná sa o jednoznačne určenie dátového obsahu bloku, merkle strom rozoberiem nižšie



Obr. 3.1: Ukážka štruktúry jednotlivého bloku [10].

- časová známka - určuje presný čas kedy bol blok vytvorený
- nBits - tento údaj určuje náročnosť hashu, ktorý musel tento blok splniť
- nounce - 4–bajtové číslo ktoré sa pridáva k hashu pri vytváraní bloku
- hash rodičovského bloku - 256–bitový hash predošlého bloku
- transakčná časť - táto časť obsahuje počítadlo transakcii a jednotlivé transakcie [10]

3.0.2 Merkle strom

Jedná sa o dátovú štruktúru, ktorá sa používa princíp binárneho stromu a hashovania oboch potomkov do rodiča. Pomocou tejto dátovej štruktúry sme schopný veľmi rýchlo overiť integritu dát bez toho aby sme ich museli všetky jednotlivo kontrolovať. Blockchain používa túto technológiu, aby zmenšil veľkosť bloku ktorý sa posiela všetkým účastníkom siete a zjednodušil overovanie integrity dát. V bloku sa nachádza hlavný koreň merkle stromu (obrázok 3.2), ktorý zaručuje integritu transakcií, ktoré daný blok reprezentuje. Každý si ho vie overiť a stačí si porovnať koreňový hash a človek ihneď vidí, či sa s danými dátami manipulovalo.

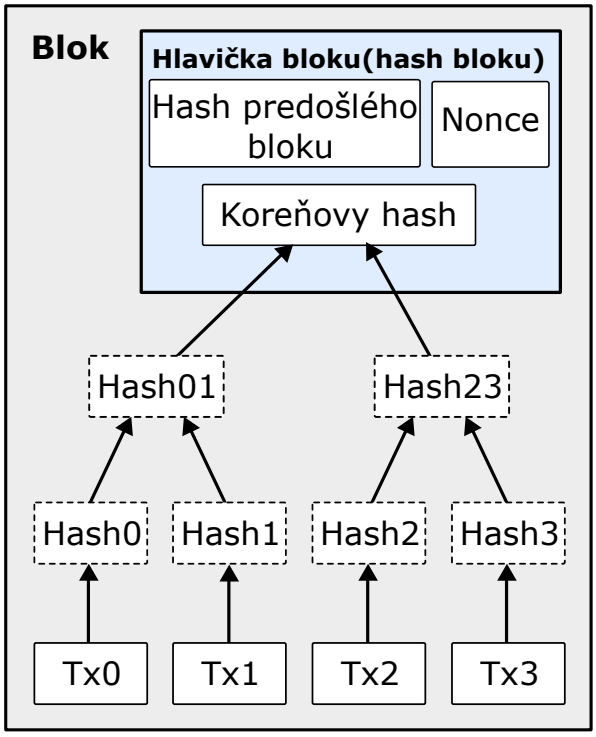
3.0.3 Fork blockchainu

Fork alebo rozdvojenie blockchainovej reťaze nastáva, ak sa príjmu nové pravidlá alebo parametre nastavenia blockchainu. Tento jav sa deje pomerne zriedka a sú to dopredu plánované akcie. Rozpoznávame dva typy forku:

- Hard fork - V prípade rozdvojenia hard forkom sa vždy ponechá stará reťaz a vytvorí sa nová v dohodnutom bode. Stará reťaz pokračuje ako keby sa nič nestalo a ta nová už aplikuje nové pravidlá, a je odteraz navždy oddelená od tej starej. Takmer každý väčší blockchain si prešiel nejakým forkom.
- Soft fork - Jedná o menšiu zmenu pravidiel, ako napríklad veľkosť bloku alebo frekvencie vytvorenia nového bloku. Kde si nová reťaz zachováva spätnú kompatibilitu pre transakcie pred forkom. Pri soft forku väčšinou prejde takmer celá sieť na nové pravidlá a tie staré sa už prestanú používať.

3.1 Základné rozdelenie

Blockchain architektúru rozdeľujeme na dve veľké základné skupiny a to permissonless a permissioned. Tieto dva pojmy sa vzťahujú na existenciu nadradených užívateľov v sieti. Permissionless je najčastejšie spájaný s verejným



Obr. 3.2: Ukážka fungovania merkle stromu v jednotlivom bloku. Transakcie sú hashované a postupne vytvárajú koreňový hash, vďaka ktorému je jednoduché overiť obsah transakcií. [1]

Vlastnosť	Verejný blockchain	Konzorcium blockchain	Súkromný blockchain
Overovatelia transakcií	Všetci používatelia	Malá skupina používateľov	Jedna organizácia
Viditeľnosť transakcií	Všetci vidia všetko	Môže byť obmedzená alebo zakázaná	Môže byť obmedzená alebo zakázaná
Nemeniteľnosť	Takmer nemožné niečo zmeniť	Dáta môžu byť manipulované	Dáta môžu byť manipulované
Efektívita	Nízka	Vysoká	Vysoká
Centralizácia	Nie	Čiastočna	Áno
Hlasovaní mechanizmus	Permissionless, Permissioned	Permissioned	Permissioned
Dopad na trh	Prevratný	Zníženie nákladov	Zníženie nákladov

Tabuľka 3.1: Porovnanie rôznych typov architektúr blockchainu z pohľadu správy systému

blockchainom, pretože tam neexistujú nadradený užívatelia a všetci si sú rovný. Permissioned je často spájaný so súkromným blockchainom alebo konzorciom. Je potrebné si tieto pojmy nespájať so súvislosťou nad tým, či dokáže človek čítať údaje na blockchaine. Pri permissionless platí, že musí byť zoznam všetkých transakcií vždy verejný a prístupný komukoľvek. Aj napriek tomu, že sa nedá žiadny účastník alebo transakcia priamo identifikovať, existujú spôsoby [11] ako sledovať peniaze a určiť konečného používateľa alebo identifikovať niekoho na základe všetkých jeho transakcií.

V prípade permissioned to už neplatí, existujú prípady použitia kedy nie je vhodné aby si mohol ktokoľvek čítať transakcie ako napríklad bankovníctvo, ale existujú aj prípady permissioned blockchainu kde je zoznam transakcií verejný. Mnohé veľké firmy vyvíjajú riešenia prevažne na premissioned blockchaine, ktorý je menej obmedzujúci a dokážu ho mimo iné lepšie riadiť. To však hneď neznamená, že je zoznam transakcií neverejný. Vedie sa ale obrovská diskusia, či sú vlastne permissioned blockchain stále blockchain aplikácie a nie skôr distribuované databázy.

3.1.1 Permissonless

V tomto prípade sa jedná o architektúru bez centrálnej autority, žiadna skupina ľudí nemá viac práv ako ostatné. Ktokoľvek môže prísť a odísť kedykoľvek sa mu zachce. Blockchain je verejný a otvorený, každý ma právo overovať a hlasovať za transakcie. Najlepší príklad verejného blockchainu je Bitcoin alebo Etherneum [12].

Permisionless implementácia blockchainu prináša mnoho prekážok ale aj výhod. Medzi jeho hlavné výhody patrí predovšetkým spôsob ako chrániť užívateľov systému pred vývojármi ustanovením, že existujú určité veci, nad ktorými nemajú ani samotný vývojári kontrolu a žiadnu autoritu ich zmeniť. Môže to pripadať naivné, že prečo by dobrovoľne vzdali práva ovládať veci na ich aplikácií. No pri hlbšej ekonomickej analýze prídeme k záveru, že ak sa explicitne vzdám práva ovládať určite veci, ľudia budú viacej veriť systému a používať ho intenzívnejšie, pretože budú veriť že t sa im tieto určité veci stanú zriedkavejšie. Druhá výhoda je, že ak sa niekto pokúsi akokoľvek prinútiť vývojárov aby niečo zmenili vedia povedať *„Nemám nad tým žiadnu kontrolu a moc“*. Toto je predovšetkým účinné, pretože to odradí od potencionálneho nátlaku. Pre bežných užívateľov to implikuje, že žiadna cenzúra nebude môcť byť zavedená na príklad od vlády, alebo inej inštitúcie [13]

Nevýhody sú napríklad:

- Vysoká cena za uskutočnenie transakcie, pokiaľ sa sieť dostatočne nerozrastie
- Približne 3x dlhší čas než sa sieť dohodne na dokončení(finalite) transakcií

- Spotreba energie a environmentálna záťaž
- Obmedzené možnosti robiť zásadné zmeny po spustení blockchainu
- Všetky transakcie sú nenávratné
- Škálovacie problémy kvôli pomalej rýchlosť konvergencie siete

3.1.2 Permissioned

Za permissioned sa považuje kompletne súkromný blockchain, čiže presný opak verejného blockchainu, ale aj konzorcium blockchain. Existuje tu hlavná autorita, či už centralizovaná alebo decentralizovaná nezáleží na tom. Táto hlavná autorita, niečo ako vláda má jediné právo overovať transakcie a rozhodovať o udávaní smeru a jeho dodržiavania. Tento typ architektúry vyvíjajú hlavne banky a finančné inštitúcie pre interné potreby poprípade enterprise aplikácie. Veľmi dobrým príklad je napríklad Corda[14] alebo Juno(JPMorgan).

Konzorcium blockchain, je zase v mnohom podobný tomu verejnému, ale existujú tu privilegované skupiny ktoré sú poverené overovaním transakcií. Je to taký mix, ktorý s snaží nájsť rovnováhu niekde v strede týchto rôznych architektúr. Všetci sa môžu pripojiť a skúsiť overovať transakcie, no musí sa zhodnúť väčšina privilegovaných aby sa našla zhoda na sieti. Táto skupina privilegovaných je určená vývojármi a môže sa časom meniť. Typickým príkladom tejto architektúry je Hyperledger Fabric [15],[12].

Súkromný a konzorcium blockchain môžeme zaradiť do triedy permissioned blockchain. Pretože sa rozlišujú iba v tom ako veľmi zasahujú so fungovania systému centrálne autority. Hlavnými výhodami permissioned blockchainu sú:

- Konzorcium alebo firma ktorá spravuje blockchain, dokáže jednoducho zmeniť pravidla blockchainu, vrátiť transakcie, meniť stavy na účtoch atď.
- Overovatelia transakcii sú verejne známy, preto je nemožné spôsobiť sybil útok alebo 51% útok.
- Transakcie sú lacnejšie, pretože ich overujú iba niektorý účastníci ktorý nato majú privilégium. Môžeme predpokladať, že títo účastníci budú mať najlepšiu techniku a preto sa zníži aj cena za overenie jednej transakcie.
- Transakcie sú rýchlejšie uverejnené na blockchain, pretože potrebujeme nájsť zhodu na jednotlivom bloku iba u privilegovaných jednotlivcov a nie na celej sieti ako v prípade verejných blockchain systémov.

Nevýhodou týchto systémov je samozrejme vkladanie dôvery do rúk niekomu inému. A je len na skupine ľudí ktorý spravujú daný blockchain, či túto dôveru nezneužijú. Aj keď je očividné, že tieto permissioned systémy porušujú

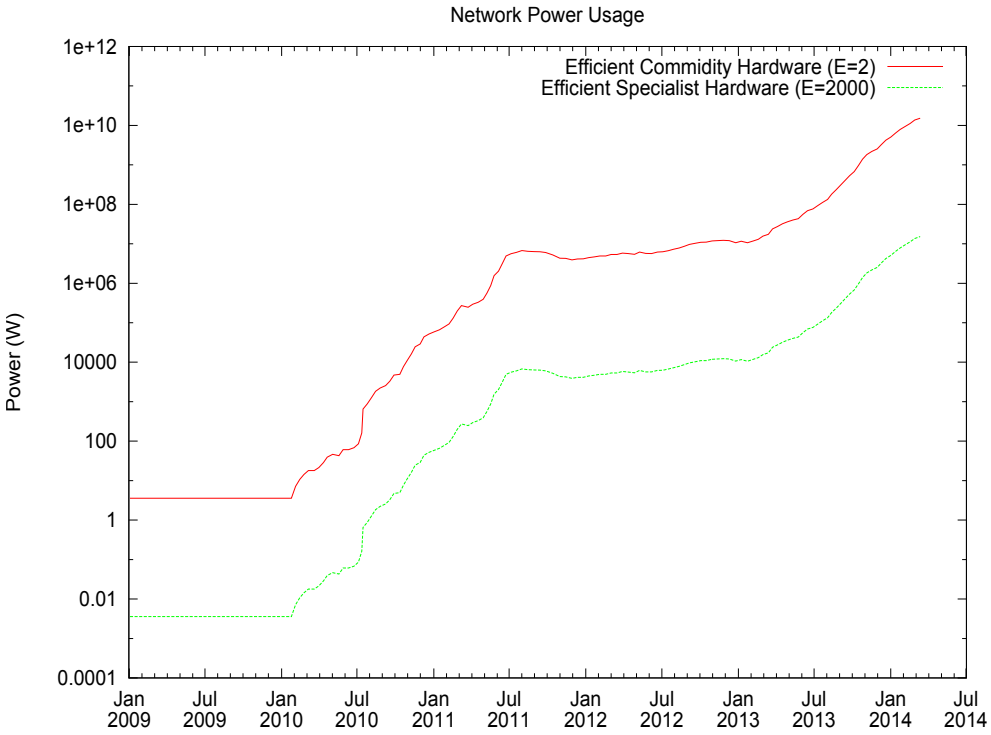
základne princípy blockchainu, ktoré položil Satoshi Nakamoto, nemusí to byť až také zlé. V mnohých prípadoch by bolo nemožné použiť verejný blockchain a preto trh reagoval zjednodušením si podmienok.

3.2 Hlasovací mechanizmus

Ako sme si už predstavili v predošlých kapitolách, hlasovací mechanizmus je jadro akéhokoľvek blockchainu, pretože hlasovací mechanizmus predstavuje systém ako sú nové bloky vytvárané, overené sieťou a pridané do blockchainu. Najväčšiu výzvu predstavuje predovšetkým u verejného permissionless blockchainu. Kde nastávajú problémy najmä pri škálovaní na väčšiu skupinu používateľov. V prípade PoW, ktorý sme si predstavili ako príklad, je spotreba elektrickej energie a rýchlosť overenia transakcie najväčší problém. Jednotlivé problémy musia byť dostatočne náročné aby nevznikali okamžite, no akonáhle sa táto sieť začne zväčšovať stávajú sa tieto celkové energetické nároky príliš veľké. Určiť presnú spotrebu je veľmi ťažké, pretože ceny elektriny a spotreba jednotlivých hardvérových komponentov sa môže líšiť, no v roku 2014 spotreboval bitcoin blockchain odhadom toľko ako celé Írsko [16]. A má tendenciu naďalej stúpať ako môžte vidieť na grafe 3.3, pretože náročnosť výpočtu neustále rastie a takisto aj počet používateľov ktorý aktívne ťažia nové bloky.

Rôzne skupiny sa pokúšajú tento problém vyriešiť a nie vždy sa zhodnú, napríklad Hyperledger skupina vytvorila spôsob ako si tieto mechanizmy efektívne zamieňať a preniesli ich na modulárny systém, kde si môže tvorca blockchainu vybrať ktorý mu najviac vyhovuje. Nápadov na nové hlasovacie mechanizmy je niekoľko, ale zatiaľ žiaden nebol plne funkčne implementovaný. Cesta za lepším mechanizmom pre verejný blockchain nie je jednoduchá, keďže musí spĺňať niekoľko kritérií.

1. Decentralizované riadenie - Nemôže existovať centrálna autorita, ktorá určuje finalitu transakcií.
2. Štruktúra kvóra - Jednotlivý účastníci hlasovania musia komunikovať preddefinovaným spôsobom, ktorý môže mať niekoľko vrstiev
3. Autentifikácia - Potreba jednoznačne identifikovať účastníkov.
4. Integrita - Musí byť zachovaná integrita všetkých transakcii, napríklad pomocou kryptografie.
5. Odvolateľnosť - Potrebné na zachovanie istoty, že odosielateľ naozaj poslal transakciu.
6. Súkromie - Zaručuje, že iba zamýšľaný príjemca si môže prečítať správu.
7. Odolnosť voči chybám - systém dokáže fungovať efektívne a rýchlo aj napriek nejakým chybám v sieti (zlyhanie pripojenia, dlhá odozva)



Obr. 3.3: Odhadovaná spotreba energie bitcoin sieťou

8. Výkon - Riešenie musí byť škálovatelné, dostatočne rýchle, zvládať náhlu záťaž a nesmie mať dlhú odozvu [17].

Tieto rozsiahle kritéria nie je jednoduché naplniť, no máme k dispozícií niekoľko existujúcich riešení a nové vznikajú rýchlo. Okrem toho, že by tieto riešenia mali spĺňať formálne požiadavky, musia ešte efektívne vyriešiť problém komunikácie v distribuovanej sieti. Jedna z najpodstatnejších metrík blockchainu je odolnosť voči byzantským chybám.

3.2.1 Byzantine Fault Tolerance (BFT)

Byzantine fault tolerance je charakteristika, ktorá určuje mieru dovolenej chybovosti v systéme ktorý dovoľuje triedu chýb, ktoré patria pod problém dvoch armád (Two Generals problem[poznamka nazývaný aj The Byzantine Generals Problem]). Byzantská chyba (Byzantine Fault) je najťažšie zachytiteľná trieda zlyhania jednotlivých používateľov distribuovanej siete, pretože neimplikuje žiadne reštrikcie alebo domnienky o chybnom správaní ktoré môže používateľ mať. Byzantská chyba je veľmi závažný problém, ktorý je potrebné riešiť napríklad v motoroch lietadiel, nukleárnych elektrárňach či v akomkoľvek inom systéme, kde sa spracúvajú údaje z veľkého množstva senzorov, ktoré môžu byť

	Energetícka efektívnosť	Overovanie identity	Finalita transakcií	Tolerovaná sila záškodníka	Príklad systému
Proof of work (PoW)	nízka	žiadne	pomalá	<25% výpočtovej sily	Bitcoin
Proof of stake (PoS)	čiastočná	žiadne	stredná	<51% stávky	Peercoin
Delegated proof of stake (DPoS)	čiastočná	žiadne	rýchla	<51% overovateľov	Bitshares
Proof of elapsed time (PoET)	vysoká	áno	rýchla	nemožný útok	Hyperledger Sawtooth
Practical byzantine fault tolerance (PBFT)	vysoká	áno	rýchla	<33,3 % chybných replík	Hyperledger Fabric
Federated byzantine agreement (FBA)	vysoká	áno	rýchla	<20% chybných serverov v prípade Ripple	Ripple

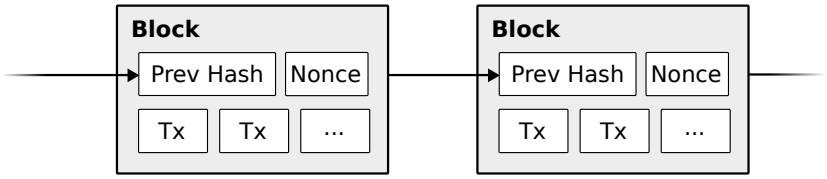
Tabuľka 3.2: Porovnanie rôznych hlasovacích systémov

pokazené alebo vracať chybné dáta. Dokonca aj SpaceX uvažuje nad potrebou mať takýto systém v ich raketách [18]. Tento problém sa týka samozrejme aj distribuovaných sieti ako blockchain. Pretože jednotlivé uzly (používatelia) môžu svojím podvodným správaním ovplyvňovať sieť až ju celú paralyzovať.

3.2.2 Proof of work

Jedným z prvých riešení ktoré človeka napadnú je Proof of Work, je to dlho používané riešenie proti DDoS útokom a BFT. Jedná sa o princíp, kde je cieľom vytvoriť krátke dáta, ktoré sú náročne na vytvorenie ale jednoduché na overenie inými používateľmi. Vytvoriť takéto dáta je mnohokrát proces pokusu a omylu s nízkou pravdepodobnosťou správneho výsledku. Tento termín v roku 1999 prvý krát použil Jakobsson Markus a Ari Juels [19]. Tento systém ma mnoho implementácii, no pre našu debatu sú potrebné iba tie ktoré majú implementáciu v blockchain svete.

- Hashcash (Bitcoin) jedná sa o proof of work algoritmus, ktorý mal slúžiť na minimalizovanie spamu v mailovej komunikácie. Funguje to na základe generovania hashu (SHA-1) ktorý sa potom pridá ku hlavičke správy. Vytvorenie tohto hashu má prísne dané pravidlá, a predstavuje čas, ktorý musel odosielateľ správy vynaložiť nato aby mohol správu poslať. Hash musel mať prvých 20 bitov nulu, ak ich neobsahoval musel sa zvýšiť nounce (počítadlo) a vytvoriť tento hash znovu pokiaľ nenašiel nejaký platný.Toto malo za cieľ, znížiť počet e-mailov, ktoré mohli užívatelia poslať a tým minimalizovať spam [20] Ako sme si už spomenuli v prvých kapitolách, Satoshi Nakamoto prebral túto technológiu a čiastočne si ju upravil pre potreby blockchainu. Začal používať novšiu hashovaciú



Obr. 3.4: Ukážka naviazovania hashov na predošlé bloky v prípade proof of work

funkciu SHA-256 a jasne definoval vstup do hashovacej funkcie ako hash predošlého bloku. Preto sa dá jednoznačne vytvoriť postupnosť blokov, pretože každý nový blok musí nasledovať za tým predošlým. Overovatelia transakcií vezmú hash posledného bloku a pridávajú ku nemu nounce. Ak tento výsledný hash splní práve aktuálny potrebný počet núl na začiatku, tak overovateľ práve vyťažil nový blok. Ak nie tak skúsi pridať iné číslo na koniec. Zmena čo i len o jedno číslo zmení kompletne celý výsledný hash, v novembri 2015 bolo na každý blok potreba vyskúšať približne 350 quintrilion(2 na 18) hashov. To samozrejme spotrebováva veľa energie a preto sa mnohý snažia tento mechanizmus nahradiť iným, ktorý by nemal také negatívne účinky na životné prostredie.

Vytvorenie nového bloku v prípade PoW znamená vyskúšať tisícky hashov pokiaľ nenájdem taký, ktorý ma potrebný počet 0 na začiatku. Je dôležité podotknúť, že tento počet nie je pevne daný a môže sa meniť. Toto kritérium sa prepočítava každých 2016 blokov, je to približne raz za dva týždne ak počítame optimálnu tvorbu bloku každých 10 minút. Toto aktualizovanie náročnosti problému zaručí, že sa bloky netvoria príliš rýchlo ani príliš pomaly. Následne po vytvorení bloku, musí tento blok overiť nadpolovičná väčšina uživateľov.

- Ethash

  Tento špeciálny algoritmus vznikol kombináciou algoritmov Hashimoto a Dagger [21]. Jeho hlavnou podstatou náročnosti sú čítacie operácie z RAM pamäti. Kde sa spolieha nato, že sa rýchlosť random-access čítacích operácií zásadne v budúcnosti nezmení. Tento algoritmus používa SHA-3 s 64 iteráciami hashovania, kde každá iterácia musí prečítať náhodných 128 bajtov v súbore s veľkou veľkosťou (viac ako 1GB). Ak výsledný hash na konci nemá požadované vlastnosti, musí sa tento algoritmus opakovať znova. Tento mechanizmus zaručuje pamäťovú náročnosť. Dagger algoritmus, ktorý je súčasťou Ethash zabezpečuje súbor ktorý sa číta a používa pri hashovaní. Tento súbor sa pravidelne mení a nanovo sa generuje každých 30 000 blokov (približne každých 5 dní).

Tento algoritmus aktuálne používa Etherneum 1.0, no očakáva sa, že sa vo verzií Etherneum 1.1 prejde na nový algoritmus Casper, ktorý je značne modifikovaná verzia PoS algoritmu.

3.2.3 Proof of Stake (PoS)

Tento kategorický rozdielny hlasovací mechanizmus vznikol v roku 2012. Jeho hlavným presadzovateľom je Vitalik Buterin zakladateľ Etherneum blockchainu, ktorý sa usiluje o prechod Etherneum z PoW na PoS. Medzi jeho hlavné výhody patrí malá spotreba energie, vysoká rýchlosť a zníženie rizika centralizácie.

Podstata tohto riešenia pochádza z predpokladu, že ak chce niekto podvádzať malo by ho to stať viac ako môže získať. Blockchain si udržiava množinu všetkých ľudí ktorý chcú overovať transakcie. Do tejto množiny môže vstúpiť každý, stačí že pošle špeciálnu transakciu ktorá zablokuje ich sumu ako depozit zato, že budú môcť overovať transakcie. Overovatelia transakcií ručia za správnosť transakcii svojím depozitom alebo stávkou. Za každý overený blok sú jednotlivý užívatelia odmeňovaný takisto dvoma zložkami a to fixnou odmenou za vytvorený blok (slúži ako distribúcia nových tokenov) a poplatkami, ktoré zaplatili ľudia čo vytvorili transakcie. Táto odmena je podielovo delená na základe výšky depozitu jednotlivca a celkového súčtu depozitov zúčastnených jedincov čo sa podieľali na hlasovaní a vytváraní daného bloku.

Tento mechanizmus má mnoho rôznych implementácií no z algoritmického hľadiska existujú dva hlavné spôsoby ho uskutočniť:

- Chain-based proof of stake je spôsob kde blockchain pseudonáhodné vyberie účastníka, ktorý môže v danom časovom okne (napríklad 10 sekúnd) vytvoriť jeden blok, ktorý musí byť pripojený na nejaký predošlý blok (väčšinou je to posledný blok v reťazi). Tieto bloky následne konvergujú do jednej dlhej reťaze (blockchainu).

- BFT - style proof of stake kde sú overovatelia náhodne vybraní aby predložili blok a následne sa v niekoľkých kolách hlasuje o predložených blokoch. V každom kole musí každý dostupný overovateľ poslať hlas jednému špecifickému bloku a na konci sa všetci overovatelia zhodnú, či bude výsledný blok s najviac hlasmi permanentne pridaný do reťaze alebo nie.

Problémy tohto mechanizmu sú že sa časom stáva viac a viac centralizovaný, ak odmenu dostávajú tí ktorý hlasujú a najväčší hlas majú tí čo najviac vlastnia. Je to rovnaký problém ako v prípade proof-of-work, kde sa centralizujú výpočtové skupiny a spôsobujú kartelizáciu celého ekosystému. Preto Vitalik presadzuje Casper[link na casper] verziu PoS, kde môžu všetci účastníci hlasovať o potrestaní nejakého jednotlivca. V prípade, že jednotlivec spraví falošnú transakciu alebo inak poškodí sieti, môže väčšina odhlasovať stratu

jeho depozitu. Casper PoS mechanizmus nebol v čase písanie tejto práce ešte implementovaný, preto sa mu nebudeme venovať.

3.2.4 Proof of Elapsed Time (PoET)

Intel prišiel so svojou implementáciou hlasovacieho algoritmu využili pri tom svoje dlhoročné skúsenosti s výrobou a architektúrou procesorov. Tento systém je veľmi jednoduchý a spočíta v tom, že si účastník za pomoci Intel SGX vygeneruje čas, ktorý musí čakať. Ten kto si vygeneruje najkratší čas vytvorí nový blok. Aby sa predišlo podvádzaniu a zasahovania do generovania času používa sa Intel SGX. Je to systém, ktorý spúšťa kód na procesore v chránenom režime, aby sa nedal ovplyvniť akýmkoľvek spôsobom. Tento kód vygeneruje čas a potvrdenie, že tento čas bol naozaj vygenerovaný. Následne po uplynutí času sa toto potvrdenie zdieľa do siete, a kto ako prvý za zdieľa toto potvrdenie môže vytvoriť nový blok.

Jedná sa o permissoned blockchain, kde každý účastník musí poskytnúť svoju reálnu identitu. Tento systém je stále v začiatkoch no Intel do neho investuje veľa času a patrí pod platformu Hyperledger. Jediným príkladom tohto hlasovacieho algoritmu je Hyperledger Sawtooth.

3.2.5 Delegated proof of stake (DPoS)

Tento mechanizmus vychádza z proof of stake ale je podstatne odlišný v spôsobe ako sa riadi a vyberajú skupiny ktoré ho riadia. Snaží sa byť čo najrýchlejší a stále si udržať decentralizáciu. Má často prívlastok ako najdemokratickejší mechanizmus a jedná sa o elektronickú implementáciu reprezentatívnej demokracie. Medzi úspešne implementácie patrí napríklad Steem alebo BitShares či Graphene. Najzákladnejší princíp vychádza z toho, že používatelia si volia svojich reprezentantov demokratickým princípom, kde každý môže hlasovať ale silu hlasu rozhoduje majetok ktorým jednotlivec disponuje. Toto zariadi, že budú zvolení jednotlivci ktorý budú prospievať sieti ako celku, pretože bude v záujme ľudí zveľaďovať svoj majetok.V prípade, že porušia pravidlá alebo inak poškodia sieť, je možnosť ich jednoducho odstrániť stiahnutím hlasu [22].

- Svedok (Witness) - je rola ktorá má právomoc transakcie zbierať a zaznamenávať do blokov, ktoré potom vytvára a pridáva do reťaze. Odmeňovanie svedkov za vytvorenie bloku závisí od implementácie v BitShares je odmeňovaný každý kto vytvorí blok ale počet svedkov je obmedzený majoritou hlasov. V prípade Steem je to iba 20 svedkov, ktorý majú najviac hlasov a počet svedkov nie je nijak obmedzený. Obmedzenie na iba tých najlepších vytvára obrovský tlak na konkurenciu a perfektnosť fungovania jednotlivých strojov [23]. Každý svedok má možnosť vytvoriť nový blok iba určitom časovom intervale, kde po tom ako mali šancu

všetci aktívny svedkovia sa znova poradie náhodne zamieša. Každý užívateľ môže sledovať zdravosť novo vytvorených blokov aj koľko vytvoril ktorý svedok blokov. V prípade BitShares sú svedkovia určený raz za deň.

- Delegáti - sú volený rovnako ako svedkovia majú však inú úlohu. Každý delegát s platným mandátom je zároveň zapísaný v genesis bloku. A sú mu pridelené špeciálne volebné práva o zmenách v blockchaine. Ukázalo sa, že časom je vždy potrebné niečo zmeniť poprípade upraviť. Tieto drobné úpravy ako napríklad cena transakcie, veľkosť bloku, odmena pre svedkov, či interval jednotlivých blokov pripadajú práve na delegátoch. V prípade BitShares platí, že ak sa väčšina delegátov zhodne na zmene, je uzákonená a naberá platnosť za dva týždne, kde počas tých dvoch týždňov môže väčšina užívateľov zahlasovať za odmietnutie úpravy poprípade vymeniť delegátov. Táto čakacia lehota je podstatná, aby sa predišlo nátlaku na delegátov poprípade zmenám proti prosperite siete. Delegáti nie sú platený a majú plnú autoritu hlasovať o akýchkoľvek zmenách [22].

Jednou z najčastejšie spomínanou nevýhodou tohto mechanizmu je, že postupne konverguje ku centralizácií moci. Vedie sa veľká debata o tom či je lepší Casper PoS alebo BitShares implementácia DPoS.

3.2.6 Practical Byzanzine Fault Tolerance (PBFT)

V tomto prípade sa jedná o replikačný algoritmus stavového automatu, ktorý toleruje byzantské chyby. Používa sa, pretože dokáže zvládnuť až jednu tretinu siete ako chybnú. Nové bloky sú vytvárané v kolách, kde v každom kole sa vyberie hlavný vykonávateľ podľa definovaných pravidiel, ktorý je potom zodpovedný za zoradenie transakcií. Celý proces by sa dal rozdeliť na 3 časti:

- pred-spracovanie
- spracovanie
- commit [10]

V každej fáze, overovateľ postúpi do ďalšej fázy v prípade, že dostane hlasy od viac ako $^2/_3$ účastníkov siete. Základné požiadavky týchto hlasovacích mechanizmov sú:

- Zverejnená identita všetkých overovateľov transakcií - tieto riešenia nebudú fungovať na permissionless blockchainoch, pretože tam nie je zverejnená identita všetkých overovateľov. A takisto to predstavuje problém, ak sa nedokáže väčšina používateľov zhodnúť na tejto skupine overovateľov.

- Malý počet používateľov, ktorý overujú transakcie - jednotlivý overovatelia si posielajú pomerne veľa správ a hlasujú v niekoľkých kolách preto je efektívnosť docielená iba na malom počte overovateľov (do 20).

Jedným z hlavných predstaviteľov PBFT je Hyperledger Fabric, aj keď musím podotknúť, že Fabric je modulárna platforma a nemusí mať vždy PBFT hlasovací mechanizmus. No v prípade, že sa vývojári rozhodnú PBFT použiť, systém funguje nasledovne. Účastníci rozdeľujú na dve skupiny:

- Neoverovatelia transakcií - Ktorý slúžia len ako spojovník medzi inými účastníkmi ktorý overujú transakcie.
- Overovatelia transakcií - Títo účastníci majú spustený hlasovací mechanizmus na svojich počítačoch a aktívne sa podieľajú na hlasovaní o správnosti transakcií.

Hlasovací mechanizmus obsahuje automat (state machine), ktorý prijíma tri typy transakcií ako vstup:

- Deploy - Zahŕňa akceptovanie transakcie so smart kontraktom (Chaincode), ktorý je neskôr spustený.
- Invoke - Tento krok akceptuje jednotlivé argumenty transakcie, ktoré prislúchajú aktivite ktorú vyvoláva smart kontrakt a následne spúšťa smart kontrakt.
- Query - Vracia stav automatu ktorý dostal na vstupe od iného účastníka.

Každý smart kontrakt musí byť deterministický, pretože sa spúšťa na viacerých automatoch naraz a porovnávajú sa výsledky navzájom a tým sa validuje transakcia.

3.2.7 Federated Byzantine Agreement (FBA)

Tento hlasovací mechanizmus funguje iba v permissioned sieťach. Jeho podstatou je, že bloky sú uznané za schválené v prípade, že boli podpísané určitým kvórom overovateľov. Podpisy kontroluje konkrétny implementovaný algoritmus, ktorý kontroluje či bola splnená podmienka M z N podpisov, kde M je počet potrebných podpisov a M je počet aktuálnych podpisov.[https://chain.com/docs/1.2/protocol/pape
consensus]

3.2.7.1 Stellar

Stellar Consensus Protocol bol predstavený ako open-source platforma, ktorá by umožnila širokej verejnosti budovať aplikácie na tejto blockchain platforme. Tento protokol vznikol ako fork[odkaz na fork] Ripple [24] blockchainu v roku 2014. V súčasnosti už nemajú žiaden spoločný kód a každý plní inú úlohu.

Ripple sa snaží preniesť platby medzi dvoma bankami na blockchain, Stellar sa pokúša celkovo obísť banky a umožniť globálne transakcie medzi dvomi účastníkmi bez žiadnych ďalších sprostredkovateľov.

SCP využíva koncept kvórumných rezov (quorum slices), kde kvórum je množina uzlov, ktoré pracujú spoločne na tom, aby dosiahli zhodu a rez kvórom je podmnožina tejto množiny. Tento rez kvórom pomáha jednotlivému uzlu spracovávať proces dohody. SCP je globálny hlasovací protokol, ktorý sa skladá z nominačného (nomination) a hlasovacieho (ballot) protokolu. Ako prvý sa spúšťa nominační protokol, počas ktorého sa navrhujú nové hodnoty na schválenie. Každý uzol, ktorý dostane tieto hodnoty bude hlasovať za jednu z nich. Po niekoľkých kolách sa eventuálne všetky uzly zhodnú na rovnakých hodnotách.

Po úspešnej exekúcií nominačného protokolu sa spúšťa hlasovací protokol, kde sa jedná o federatívne hlasovanie, ktoré má určiť či sa hodnoty ktoré boli nominované zaznamenajú alebo nie. V prípade že sa nevie jednotlivý rez dohodnúť presunie sa hlasovanie do vyššej úrovne a považuje sa za nové hlasovanie. Tým pádom sa zaručí, že sa rozhodne o nominovaných hodnotách. SCP tvrdí, že neobsahuje žiadne blokované stavy, nízku latenciu, decentralizovanú kontrolu a asymptotickú bezpečnosť. Nedokáže ale vždy garantovať bezpečnosť, v prípade, že si uzol zvolí neefektívny rez kvórom. Hlavný rozdiel medzi FBA (federated byzantine agreement) a klasickým BA je, že v prípade FBA jednotlivé uzly ktoré sa podieľajú na transakciách si takisto aj vyberajú rez kvórom [25].

3.2.7.2 Ripple

Tento projekt vznikol ako snaha zjednodušiť globálne transakcie medzi bankami. Jedná sa o plne permissoned systém, kde majú kontrolu banky. V tomto prípade sa jedná o protokol, ktorý využíva verifikované podsiete, ktoré pomáhajú celkovej sieti v rozhodovaní. Jednotlivý účastníci sa rozdeľujú na dve skupiny: server na ktorom beží rozhodovací protokol a klient ktorý prijíma a odosiela peniaze. Každý server má svoj vlastný UNL (unique node list), ktorý slúži pri rozhodovaní či server príjme transakciu alebo nie. V prípade, že server dostane transakciu spýta sa všetkých ostatných serverov vo svojom UNL a ak bude kladná odpoveď vo viac ako 80% tak je transakcia schválená. Tento systém funguje pokiaľ sa nepokazí viac ako 20% serverov ktoré majú hlasovať [10].

3.3 Výzvy a prekážky blockchainu

Blockchain tak ako každá novovznikajúca technológia svoje chyby a nedostatky. Preto je podstatné o nich hovoriť a snažiť sa ich vyriešiť. Ak si má blockchain zachovať pôvodnú podobu, bude potrebné vyriešiť škálovanie pre veľké počty používateľov a celkovú priepustnosť systému. Samozrejme, že sa

tieto problémy dajú zjednodušiť použitím permissioned blockchainu, no naozajstná výzva je umožniť to pre permissionless blockchainy. Medzi ďalšie výzvy patrí napríklad právna regulácia blockchainu, ako aj hrozby rôznych útokov pomocou budúcej technológie ako napríklad kvantové počítače.

Medzi hlavné technické výzvy blockchainu patrí zvýšenie priepustnosti systému, zníženie odozvy v celej sieti a jej škálovateľnosť. Je to skutočne závažný problém, pretože bráni technológií blockchainu slobodne sa rozrastať. Tento problém ma niekoľko úrovní a pre každý typ hlasovacieho mechanizmu trošku inú podobu. V prípade Bitcoinu je najväčší problém veľkosť bloku a počet spracovaní transakcií za sekundu. Momentálne teoretické maximum je 7 transakcií za sekundu. Vychádza to z toho, že každý blok ma nejakú veľkosť a ta veľkosť určuje maximálny počet transakcií, ktoré môže obsahovať. Bloky vznikajú v pseudo pravidelnom intervale približne každých 10 minút. VISA spracováva priemerne 2000 transakcií za sekundu a v špičke aj 10 000 transakcií za sekundu. O čosi lepšie sú na tom permissioned blockchainy, ktoré využívajú BFT hlasovacie mechanizmy. Kde napríklad Ripple dokáže spracovávať 1500 transakcií za sekundu [24]. Ak sa má blockchain stať niekedy globálny štandard, bude potrebné tento problém efektívne vyriešiť.

3.3.1 Regulácia

Ďalšou obrovskou výzvou pre blockchain je otázka regulácií. Konkrétne formy zdanenia a prístupu ku globálnym blockchainom. Predstava, že blockchain sa vyhne regulácií je naivná, a žijeme vo svete kde je všetko, čo sa dá zdaniť zdanené a nevyhne sa tomu ani blockchain. Veľmi ťažkou otázkou pre štáty je ako zdaniť blockchain a kde. Samozrejme v prípade súkromných blockchainov to je jednoduché, pretože za nich zodpovedá zriaďovateľ alebo prevádzkovateľ. V prípade verejných blockchainov je to už zložitejšie, štáty sa budú musieť dohodnúť kde budú takéto globálne systémy zdaňovať, keďže transakcia nie je viazaná na žiadnu geografickú polohu alebo hranice štátu a nachádza sa všade kde je internet. Rovnako budú musieť zodpovedať otázku koho zdania, overovateľa bloku pretože vytvoril hodnotu alebo zadávateľa či nebodaj prijímateľa transakcie. A ak áno ako budú takýchto ľudí identifikovať, pretože blockchain takúto identifikáciu nepotrebuje a nepodporuje. Toto sú len niektoré z mnohých otázok na ktoré budú musieť naši európsky zákonodarci odpovedať v blízkej budúcnosti [2]

3.4 Zhrnutie

Cieľom tejto kapitoly bolo vysvetliť čitateľovi základné charakteristické stavebné prvky blockchain architektúry. Bolo predstavených niekoľko rôznych implementácií blockchain technológie ako aj ich princíp fungovania. Niektoré z týchto implementácií sa ešte stále vyvíjajú a mnohé ešte len vznikajú, pretože rýchlosť vývoja blockchain technológií je obrovská. V nasledujúcej kapitole si

rozoberieme možné prípady použitia technológie blockchain a jej potenciálnych dopadov na reálny svet.

Kapitola 4

Blockchyain v reálnom svete

Prvá otázka ľudí, keď im poviem na čom pracujem pre moju bakalársku prácu, je *„a zmení to niečo, ten blockchain?“*. Moja odpoveď býva zväčša áno aj nie. Áno preto, pretože už veľa toho zmenil, napríklad najväčšie svetové inštitúcie pochopili, že už nie je možné stavať jeden legacy backend systém nad druhý a budovať neefektívne štruktúry a začali s tým niečo robiť a vyvíjať nové systémy, ktoré stoja práve na mnohých podobných technológiách ako blockchain. A *„nie“*, pretože blockchain nie je žiadna zázračná technológia, ktorá vyrieši všetky naše problémy ale je na vývojároch, niečo vďaka tejto technológii vytvoriť a dosiahnuť zmenu.

Mnohý prirovnávajú blockchain ku vzniku internetu. Keby som sa vás teraz spýtal čo vám priniesol internet, boli by odpovede štandardizácia komunikácie medzi počítačmi a vytvorenie najväčšej distribuovanej siete počítačov? Alebo by ste povedali, možnosť písať si s kýmkoľvek, pozerať filmy, ktoré doma nemáme a hrať hry s inými ľudmi v reálnom čase? Pretože, tieto fenomény nevznikli s internetom ale vďaka internetu. Tak isto ako mnoho ďalších revolučných nápadov vznikne alebo vznikajú, nie spolu s blockchainom ale na jeho platforme.

V tomto zmysle dokážeme kategorizovať postupný výboj blockchainu, na takzvaný Blockchain 1.0, Blockchain 2.0 a Blockchain 3.0. Kde každá ďalšia generácia prináša razantný skok oproti ten predošlej a vyžaduje si funkčnosť tých predošlých. Zjednodušene povedané Blockchain 1.0 by mal priniesť štandardy pre distribuované spracovanie transakcií a vedieť si tieto transakcie správne uchovávať a zaznamenávať. Mohli by sme to prirovnať ku TCP/IP štandardu. Satoshi Nakamoto svojím Bitcoinom takýto štandard naozaj vytvoril a značne posunul debatu ohľadom distribuovaného e-cash systému ku realite. Z pohľadu e-cash systému je bitcoin naozaj nadčasový, no žiaľ jeho nedostatočná programovateľnosť a obmedzujúce vlastnosti ako napríklad teoretický maximálny počet transakcií za sekundu je nepostačujúci pre potreby globálnej revolúcie, pretože z princípu inklúzie, nemôžeme blockchainu klásť žiadne geografické obmedzenia, tak ako napríklad pri cenzúre internetu niektorými štátmi, ktorá

aj tak nikdy nie je dokonalá.

Blockchain 2.0 by logicky mal byť krok ku aplikáciam, ktoré využívajú blockchain ako platformu na sprostredkovanie najrôznejších služieb. Rôzne dApps, ako sa v krypto svete nazývajú aplikácie bežiace na blockchain protokoloch, by mali kompletne zmeniť naše rozmýšľanie a hodnoty v internetovom svete. A postupne vybudovať dôveru v tento systém fungovania vecí.

Veľmi pomaličky ho potom bude nasledovať blockchain 3.0, respektíve zmeny v fungovaní spoločnosti. Je logické, že po tak razantných zmenách v internetovom svete sa budú ľudia čím ďalej dovolávať, za ich aplikáciu do fungovania štátu, e–demokracie alebo iných možno nových distribuovaných foriem vládnutia. Každopádne prechod medzi 2.0 a 3.0 je skôr vízia ako skutočnosť nasledujúcich rokov. Veľmi rád by som sa v tejto kapitole venoval porovnaniu stavu informačných systémov v momentálnom stave a možnými dopadmi blockchainu na nich [26].

4.1 Smart kontrakt

Zaujímavosťou blockchainu je, že popri transakciách dokáže reprezentovať ešte aj spúšťací kód. Blockchain, dokáže konečne implementovať smart kontrakty, ktoré Szabo v roku 1994 definoval ako *„automatizovaný transakční protokol, ktorý vykonáva podmienky kontraktu.“*[27] Smart kontrakt môže byť napríklad nezávislá zmluva na ktorej sa dohodnú dve strany, ktorá je automaticky vykonávaná na blockchaine. Konkrétne, ak si chcem kúpiť niečo cez internet, tak musím poslať najprv peniaze a dôverovať prijímateľovi, že splní svoju časť dohody a pošle mi to, čo som si zaplatil. Tento model nefunguje, pretože sme ľudia. Preto používame prostredníkov ako napríklad Amazon, E-bay či Aliexpress. Kde ten proces funguje rovnako lenže má prostredníka, peniaze posielam prostredníkovi, ktorý ich uvoľní až keď dostanem tovar. Tento proces je nákladný pre prostredníkov, pretože musia uchovávať všetky údaje a spravovať každú jednu kúpu tovaru. Sekundárny dôsledok toho je, že sa tovar postupne zdražuje, pretože s postupným rozšírením tejto služby sa zvyšujú náklady na prevádzku.

Smart kontrakt vie s pomocou blockchainu tieto náklady na prevádzku drasticky znížiť až vynulovať. Dve strany by spolu uzatvorili smart kontrakt, napríklad o výmene tovaru za peniaze a uverejnili by ho na blockchaine. Objednávateľ by poslal peniaze na smart kontrakt a odosielateľ by na smart kontrakt poslal elektronický podací lístok. Akonáhle sa tieto podmienky stretnú kontrakt sa splní a peniaze pôjdu na účet odosielateľa. A objednávateľovi príde balík. Určite ste si všimli, že v tejto modelovej situácii môže dôjsť ku mnoho zvratom. Ako napríklad, odosielateľ pošle falošný podací lístok alebo v skutočnosti nepošle to čo ma hodnotu ale napríklad tehlu. Toto sa snaží vyriešiť takzvaný multi-signature kontrakt. Znamená to, že nato aby sa kontrakt splnil ho musí podpísať viacej strán najmenej však 3. Tým pádom sú peniaze na

účte zablokované tak, že môže dôjsť iba trom výsledkom podpisu kontraktu a jeho následného ukončenia:

- objednávateľ a odosielateľ – jedná sa o úspešný kontrakt alebo odosielateľ sa rozhodne o odškodnenie objednávateľa bez zásahu agenta
- objednávateľ a agent – kontrakt zlyhal, agent sa postaví na stranu objednávateľa a vráti mu peniaze
- agent a odosielateľ – tovar bol doručený, agent sa postaví na stranu odosielateľa napriek nezhode

Tento spôsob zaručí, že minimalizujeme podvodné scenáre. Blockchain je prevažne o budovaní reputácie, pretože nespochybniteľná história transakcii hovorí veľa o ľuďoch. Napríklad ak vidím, že niekto má veľa nesplnených smart kontraktov tak od neho nebudem kupovať a opačne ak niekto neposiela peniaze tiež mu nebudem predávať. Bude potrebné uprednostniť niekoho s vynikajúcou reputáciou nad najnižšou cenou. A prečo by si niekto kazil reputáciu ak si ju tak dlho budoval.

Tento koncept sa dá jednoducho upraviť aj na iné záležitosti ako predaj tovaru. Smart kontrakt by mohol byť napríklad zmena vo firme, kde ju musí podpísať najmenej polovica zamestnancov. Multi-signature kontrakt si medze nekladie a všetko je o dohode zúčastnených. Tieto kontrakty by mohli drasticky znížiť cenu za uzatváranie kontraktov a ich vymožiteľnosť. Pretože, ak sa porušia podmienky kontrakt respektíve nezávislí agent ihneď reaguje a nečaká na súdny proces a iné administratívne úkony. Napríklad, že si kúpite auto na lízing. Po splatení poslednej splátky sa auto stane automaticky vašim. Alebo viete zakomponovať penále za zmeškanú platbu do týchto pravidiel, či prípadné zablokovanie auta iba pre banku v prípade opakovaných zmeškaných platieb.

Tieto smart kontrakty zmenia spôsob akým obchodujeme od základov.*„Ekonomické benefity týchto kontraktov zahŕňa zníženie straty v prípade podvodu, zníženie rozhodcovských a exekučných nákladov či zníženie nákladov na transakciu.“* [27]

4.2 Finančné služby

Bankovníctvo je druhé najstaršie remeslo na svete. Len za posledných sto rokov sa veľmi drasticky zmenilo upustením od zlatého štandardu, či uvoľnením menovej politiky. Jedno sa ale nezmenilo, schopnosť bankovníctva produkovať zisk. Dnešné finančné inštitúcie sú jedny z najväčších spoločností na svete a majú priamy vplyv na politiku a dianie v biznise. Či už sa budeme baviť o veľkej hre ako akciové a devízové trhy alebo o každodennej funkcií bánk ktoré umožňujú miliónom ľudom požičať si peniaze a usadiť sa, poprípade pohodlne

investovať. Všetky tieto spoločnosti prešli od konca druhej svetovej vojny nejakou formou digitalizácie a postupne sa prispôsobovali novým veciam. No finančné inštitúcie majú veľmi dlhú tradíciu veci komplikovať a nie ich zjednodušovať. Je to pochopiteľné, pretože čím sú veci komplikovanejšie tým viac si môžu od zákazníkov vypýtať peňazí. A tí im to samozrejme zaplatia, pretože nemajú inú možnosť. Dnes neexistuje alternatíva ku našemu finančnému systému, neexistuje spôsob ako legálne poslať peniaze z jedného štátu do druhého bez žiadneho prostredníka. Preto som vždy skeptický keď idem do banky niečo vybaviť.

Naša ekonomika aj tu v srdci Európy sa značne globalizovala a zrýchlila. A nielen to, dokonca sa zrýchlil aj náš život ako sa tomu ľudovo hovorí. Preto je neskutočne absurdné, že keď si niečo kúpim cez Internet, mám to doma skôr ako moja banka spracuje moju transakciu. Ktorej to trvá zväčša 2 až 3 dni. No ešte absurdnejší problém nastáva, keď chcete poslať peniaze do inej krajiny. Aj v krajinách eurozóny, kde máme jednotnú menu a jednotný systém spracovania platieb SWIFT, zaberie táto transakcia často aj niekoľko týždňov.

Samozrejme, že argumentovať, ale veď transakcia prebehla ihneď a peniaze odišli z môjho účtu. A budete mať čiastočne pravdu, lenže transakcia je prevod hodnoty z účtu platiteľa na účet príjemcu. To čo banka urobí vždy keď zadáte platbu je, validácia či máte dostatok prostriedkov a následne zablokuje tieto peniaze. A následne jej systémy v pozadí spracovávajú túto transakciu.

Niektoré tieto systémy pochádzajú ešte z obdobia sedemdesiatich rokov minulého storočia. Preto v tomto prípade, už nie je vhodné tieto systémy nazývať legacy ale skôr vykopávkami, niektoré časti sú napísané v už neexistujucích programovacích jazykoch, ktoré sú dávno neefektívne a zastaralé. To, že sa tieto systémy udržujú v chode ukazuje krehkosť nášho finančného systému. Pretože, ak sa boja vymeniť jeden systém za iný tak nenastáva žiaden posun, iba sa odkladá nevyhnutné. Keby ste ľudom povedali, aké počítače a programy spravujú ich financie, nikdy by svoje peniaze do banky nedali. Nádherne to povedal Vikram Pandit bývali CEO Citigroup: „*S príchodom technológií sa síce papierové procesy zautomatizovali a elektrifikovali, ale logika za nimi zostala z čias papieru.*“[2][Str. 55] Myslím si, že prišiel čas, aby sme aj toto podstatné odvetvie modernizovali a dokázali sa zbaviť starého, také jarné upratovanie vo finančných inštitúciach [2].

4.2.1 Banky investujú do vývoja blockchainu

Banky svoj prvotný nezáujem o blockchain, nahradili náhlym záujmom a veľkými investíciami do vývoja tejto technológie. Na jeseň v roku 2015 sa 9 najväčších bánk na svete rozhodlo spoločne založiť firmu, ktorá ma priniesť štandardy pre technológiu blockchain. Barclays, JPMorgan, Credit Suisse, Goldman Sachs, State Stree, BBVA alebo Royal Bank of Scotland sa rozhodli spolupracovať pri vývoji tejto novej technológie a pritiahli expertov z rôznych firiem aby im s tým pomohli. Nazvali to R3 konzorcium a ich prvotná idea

bola vytvoriť prvotné štandardy tejto technológie. No veľmi rýchlo sa dostali do konfliktu s odbornou verejnosťou, pretože sa nezhodli na tom, či by mal byť blockchain verejný alebo súkromný. Podrobne tento problém vysvetlím v nasledujúcej kapitole.

A tak v decembri 2015 vzniká ďalšia skupina. Linux Foundation v spolupráci s leadrami na trhu ako Cisco, Accenture, IBM, Intel, SWIFT alebo Digital Asset Holdings a mnoho ďalších vytvárajú Hyperledger projekt. Trošku paradoxom je, že sa ku nim pridal aj napríklad State Street či JPMorgan, ktorý podporili aj R3 projekt. Cieľom tohto projektu, nie je ani kompletne konkurovať R3 no vydali jasné stanovisko a signály, že blockchain musí byť open-source a prístupný verejnosti.

Pre Hyperledger je takisto ako pre R3 najväčšou prioritou vytvoriť spoločne štandardy na ktorých by mohli neskôr budovať. Vytvorili sa nám tu, dve skupiny s úplne rozličným prístupom a očakávaniami k tej to technológii a obe majú takmer neobmedzený rozpočet. Získajú veľké banky nadvládu tým, že si vyberú technológie z blockchain balíčku a uplatnia iba tie vhodné? R3 sa tým smerom vydalo, keď v novembri 2015 Goldman Sachs požiadalo o patent na *„metódy uzatvárania transakcií na finančných trhoch používaním distribuovanými peer-to-peer sieťami a kryptografických techník“*[2] nazvali to SETLcoin. Irónia toho, že sa banka pokúša patentovať open-source technológiu ukazuje jej úmysle s touto technológiou. No diskusia je stále otvorená a neustále sa vyvíja prinášam vám oblasti v ktorých sa najviac očakáva zmena práve technológiou blockchain.

4.2.2 Presun majetku

Základom dnešného finančného sveta je mobilita kapitálu, či už sa bavíme o tuzemských platbách alebo medzinárodných. Je to základ globalizácie a ekonomickej prosperity. Blockchain prináša radikálnu zmenu, a tou je rýchlosť. Nikdy sme si to až do teraz veľmi neuvedomili. Náš platobný systém je pomalý, neefektívny a zbytočne zložitý. Bolo to možno aj tým, že neexistovala iná alternatíva. No dnes už existuje a s drobnými chybami aj funguje. Myslím si, že blockchain ak by už nič iné nedosiahol, stane sa novým štandardom na presun majetku, akéhokoľvek. Práve v tejto sfére sú banky veľmi motivované, zníženie nákladov na prevádzkovanie systémov je pre nich dlhodobá priorita. A môže sa stať, že čoskoro uvidíme reklamy s formulkou *„Blockchain powered“* ako lákadlom pre ľudí. Aj, keď jediná vec, ktorú banky urobia bude vymenia staré systémy za nový výkonný pseudo-blockchain. Predstava, že platba zo Slovenska nebude ísť do Česka tri dni, ale povedzme niekoľko minút je veľmi uspokojujúca.

4.2.3 Uchovávanie majetku

Finančné inštitúcie sú dátovým skladmi pre ľudí, vlády a iné tretie strany. Preto je nesmierne dôležité aby tieto dáta uchovávali čo najbezpečnejšie. Dnešné robustné databázy sú dôležitou súčasťou ich každodenného fungovania, no tieto databázy potrebujú neustálu kontrolu a zálohy, pretože sa vždy eventuálne niečo pokazí. Problémom je, že tieto databázy boli vytvorené aby dáta uchovávali, nie aby ich pravidelne menili. Aj keď, niektoré transakčné databázy sú na tom výkonnosťou veľmi dobre, nedajú sa veľmi porovnávať s možnou výkonnosťou blockchainu a poprípade nejakej jeho odľahčenej verzie uzatvoreného transakčného systému.

4.2.4 Investovanie

Investovanie je čím ďalej tým populárnejšie, blockchain dokáže otvoriť brány ľudom, bez potreby mať nejakého prostredníka. Či, už sa bavíme o malom crowdfoundingu alebo IPO. Táto technológia umožní ľudom priamo investovať, či už je to v USA alebo v Paname. Globálna platforma pomôže hlavne rozvíjacím krajinám a otvorí dvere novým modelom investovania.

4.2.5 Účtovníctvo

Veľmi razantná zmena sa nevyhne ani vedeniu účtovníctva pre banky. V blízkej budúcnosti, keď banky prejdú na nový systém, kde všetky transakcie sú zaznamenávané aj do blockchainu. Preverenie všetkých transakcií bude otázkou minút nie mesiacov. Všetky transakcie budú dohľadateľné na jednom mieste a bude sa v nich dať efektívne vyhľadávať. Táto úžasná zmena pre banky znamená obrovský problém pre poradenské firmy, ktoré tieto audity vykonávali. Celý proces robenia auditu sa zmení od základov. Napríklad pre Deloitte, jednú z 4 najväčších poradenských firiem na svete, predstavujú audity takmer tretinu ich obratu. Je pre nich kľúčové, aby tuto zmenu postrehli a prispôsobili sa.

4.3 Digitálna identita

Prakticky od vzniku internetu sa rieši otázka ako identifikovať človeka online. V čase, keď sa vytváral základ internetu bola kombinácia login-u a hesla najjednoduchšia voľba. Lenže, ľudia sú len ľudia a s narastajúcim používaním internetových služieb začalo byť týchto hesiel veľa. Preto ľudia začali používať rovnaké slabé heslá a mnohokrát aj rovnaké prihlasovacie meno. Spolu s technologickým vývojom, kde zvýšenie výpočtovej sily umožnilo skúšať hádať hesla hrubou silou. Dospeli sme do stavu, kde sú tieto zabezpečovacie princípy nedostatočné.

Mnohé inštitúcie používajú veľmi zložité Know Your Customer (KYC) procesy. Cieľom týchto procesov je overiť totožnosť klientov a ich finančnú minulosť, prakticky sa jedná o klient due diligence. V mnohých štátoch sú tieto kontroly povinné zákonom a firmy nato míňajú nemalé peniaze.

Thomson Routers konštatuje, že „*... cena a zložitosť KYC procesov neustále rastie a ma negatívny vplyv na podnikanie. Finančné inštitúcie v priemere minú $60 miliónov ročne, no niektoré dokonca až $500 miliónov ročne.*“[28]

Nielenže sú tieto procesy drahé a pomalé, ale sú aj potencionálne nebezpečné, pretože jednotlivec sa spolieha na tretiu stranu. Servery tejto tretej strany zhromažďujú tieto citlivé dáta sa tým pádom stávajú terčom hackerov. Tieto procesy sa predražujú aj preto, že je potrebné ich dostatočne zabezpečiť proti útokom. Všetky tieto problémy by mohla vyriešiť digitálna identita. S blockchain technológiou by sme vedeli kompletne otočiť systém akým verifikujeme informácie pre tretie strany na taký, v ktorého strede stojí nespochybniteľná entita, ktorá verifikáciu poskytuje ak je o to požiadaná iba vo forme true/false odpovedi. Poskytnútím verejného kľúča, by si vedeli tretie strany ihneď skontrolovať, či sú moje informácie pravdivé. Príkladom takejto služby je napríklad Civic (civic.com), kde sa zaregistrujete, sprístupníte potrebné dokumenty.Oni ich overia a vytvoria digitálnu identitu, ktokoľvek bude chcieť spraviť kontrolu KYC, požiada používateľa o jeho verejný kľuč, vykonávateľ KYC následne pomocou tohto verejného kľúča a zadaných údajov overí pravosť údajov. Údaje nikdy nesťahuje a neukladá, preto sa nemôže ani stať terčom útoku.

Takýto systém môže priniesť mnoho výhod, najväčšou je asi bezpečnosť a rýchlosť tohto procesu. Všetky dáta sú overiteľné kdekoľvek a kedykoľvek.

4.4 Zhrnutie

V tejto kapitole sa rozobrali možné prípady použitia technológie blockchain. Jednoznačne to nie su všetky možné prípady využitia ale skôr tie najpodstatnejšie. Dopady technológie blockchain sú naozaj obrovské a preto ich nebolo možné pokryť všetky v tejto práci. Smart kontrakty majú využitie v takmer každom biznise a v prípade, že sa ich podarí úspešne implementovať v globálnej mierke, uvidíme potenciál blockchain technológií naplno aj v bežnom živote. V nasledujúcej kapitole sa rozoberá praktická časť mojej bakalárskej práce a to konkrétne sprievodca, ktorý bude pomôže identifikovať potrebu používať technológiu blockchain.

Kapitola 5

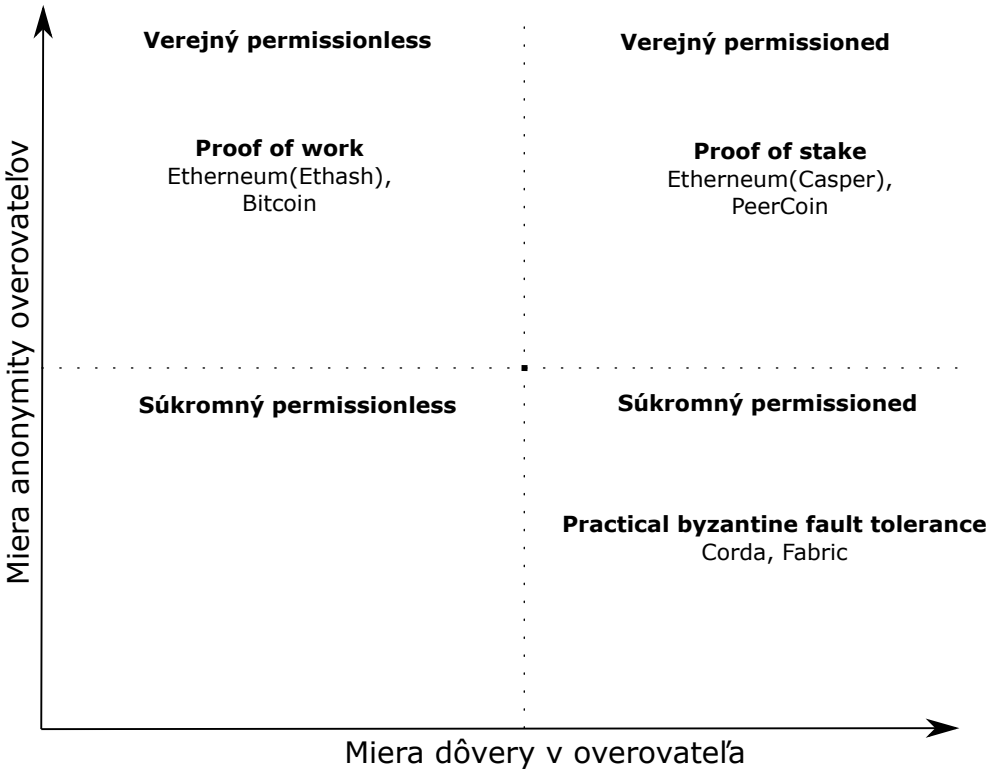
Praktická časť

Blockchain nie je jednoduchá technológia, človek musí zohľadniť mnoho faktorov a čaká ho beh na dlhú trať. Ako ste už čítali v predošlých kapitolách blockchain má veľa odlišných implementácií a nové stále ešte vznikajú. S možnosťou nastavovať neskutočne množstvo parametrov a hlasovacích mechanizmov je každá implementácia blockchainu takmer jedinečná a aj tí najväčší konkurenti sa líšia v mnohých malých ale podstatných detailoch. V tejto kapitole predstavím môjho sprievodcu svetom blockchainu, ktorý pomôže lepšie zhodnotiť, či vôbec blockchain technológiu potrebujete a ak áno akú a kde to zapadá v celkovom obraze vývoja technológie.

Tento sprievodca má tri na seba nadväzujúce časti, v tej prvej sa najprv venujem tomu či vôbec používateľ blockchain potrebuje. V druhej sa snažím identifikovať jednu technológiu ktorá by bola pre používateľa sprievodcu najlepšia a napokon v tretej časti to zaradím do kompletného obrazu všetkých technológií a usmerním používateľa načo by sa mal zamerať. Ako si určite všimnete vytvoriť takéhoto zložitého sprievodcu je veľmi ťažké, nielen preto, že sa jednotlivé implementácie môžu zmeniť zo dňa na deň ale aj preto, že sa mnohé technológie prekrývajú a či už viac alebo menej na seba podobajú, rozhodujú potom práve tie malé implementačné detaily.

5.1 Celkový obraz delenia technológie blockchain

Existuje veľa spôsobov ako rozdeliť svet blockchainu. Rozhodol som sa ho rozdeliť podľa dvoch najnákladnejších parametrov. A to mieru dôvery v overovateľa a anonymitu takého overovateľa. Toto základné rozdelenie som rozšíril o konkrétne implementácie a pomocou rozhodovacích stromov sa snažím zaradiť potreby používateľa sprievodcu do tejto mapy. Graf je rozdelený na štyri kvadranty, kde každý ma odlišné parametre a špecifiká ktoré nižšie rozoberiem po jednotlivých kvadrantoch. Je potrebné poznamenať, že týmto grafom sa snažím generálne rozdeliť typy blockchainu a preto nemusia ich typické charakteristiky platiť rovnako pre všetky implementácie prislúchajúce k danému



Obr. 5.1: Graf znázorňuje pozíciu rôznych typov blockchainu podľa miery dôvery v overovateľa a anonymity takého overovateľa. V každom kvadrante sú znázornené najznámejšie hlasovacie mechanizmy a ich implementácie.

kvadrantu. Niektoré implementácie totiž zapadajú do viacero kvadrantov, ako nižšie rozoberiem a predvediem na grafe 5.3 s konkrétnymi implementáciami.

1. Verejný permissionless - tento model je ten najslobodnejší s najväčšou kontrolou verejnosti. Ktokoľvek sa môže kedykoľvek pripojiť a začať overovať transakcie, preto je miera dôvery v jednotlivého overovateľa nízka a anonymita takého overovateľa najvyššia. V tomto kvadrante si sú všetci účastníci rovný a anonymný. Blockchainy v tomto kvadrante sa veľmi zle škálujú na veľa používateľov. Pokiaľ sa podarí udržať združenia tažiteľov na uzde nedôjde nikdy k centralizácii.

2. Verejný permissioned - tento kvadrant zahŕňa verejný blockchain kde môže ktokoľvek, kedykoľvek prísť a aj odísť. Hlavným rozdielom oproti prvému kvadrantu je postavenie jednotlivých overovateľov medzi sebou. V prípade PoS ma najväčší hlas ten, kto vsadil najviac majetku. Preto si už nie sú všetci rovní. Do tohto kvadrantu pripadá takisto DPoS, v ktorom sú overovatelia vybraný hlasovaním. Zvýšená dôvera v jednotlivého overovateľa dovoľuje znížiť počet týchto overovateľov a nepriamo

aj zrýchliť schvaľovanie jednotlivých blokov. Škálovateľnosť implementácií v tomto kvadrante je porovnateľne lepšia ako v prípade prvého kvadrantu, pretože schvaľovanie transakcií nie je priamo viazané na veľkosť siete. Predovšetkým DPoS ale aj PoS bude konvergovať ku centralizácií moci, pretože najväčší hráči budú mať najviac majetku a tým pádom aj najväčší hlas v rozhodovaní.

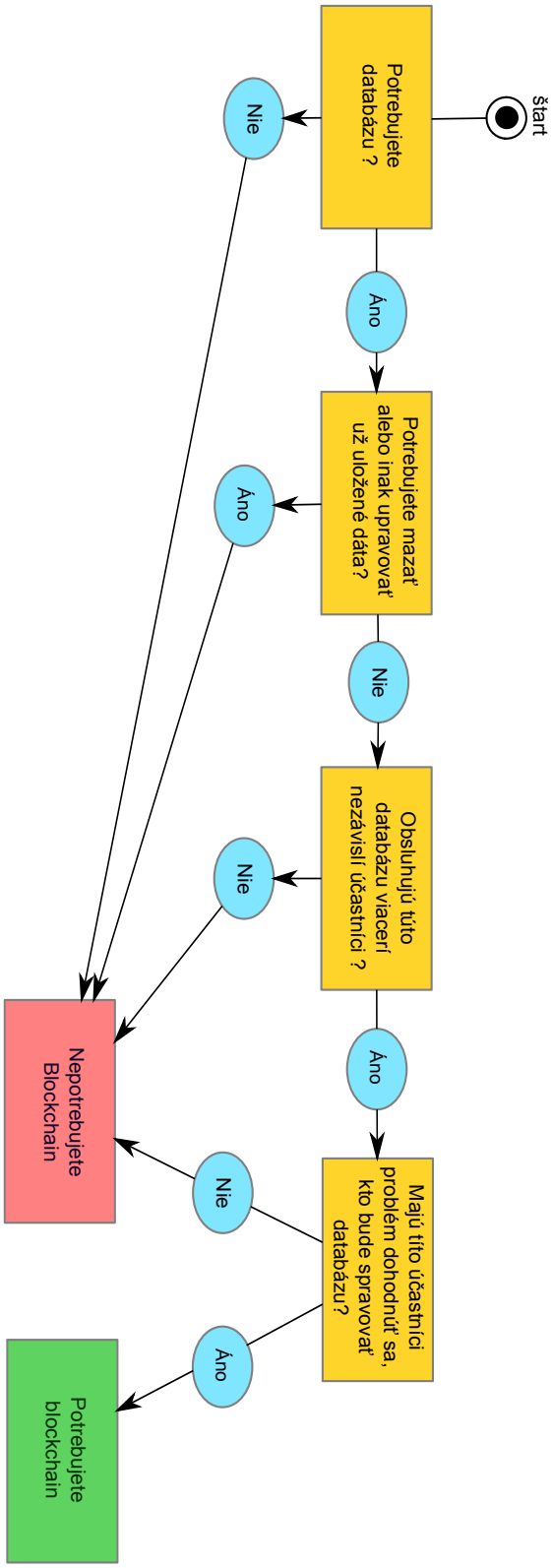
3. Súkromný permissionless - tento kvadrant je nemožné splniť, je to paradox, ak chcete vytvoriť systém, kde budete kontrolovať, kto môže systém používať a povoliť im slobodne sa rozhodovať máte problém. Pretože, oni vás môžu prehlasovať a vy zase odoprieť prístup nepohodlným overovateľom, ktorý majú iný pohľad na budúcnosť siete. Ak chcete súkromný blockchain tak potrebujete aby neboli transakcie verejné, ale všetky systémy pre permissionless hlasovanie potrebujú verejné transakcie, preto je tento kvadrant prázdny.

4. Súkromný permissioned - tento kvadrant je výlučne pre uzatvorené systémy, kde je dôvera v jednotlivého overovateľa maximálna, pretože sú určovaný licenciou alebo iným spôsobom. Všetci účastníci sú známy a overovatelia sú špeciálne volený. Tento systém má vynikajúce škálovanie ako aj rýchlosť spracovania transakcií. Chýba mu ale verejná kontrola a mnohé implementácie nemajú verejne prístupný zoznam transakcií. Vo svojom princípe sa jedná prípad, kde to síce spracovanie transakcií funguje ako u iných blockchain architektúrach, ale je celý pod kontrolu jednej alebo viac konkrétnych entít. Môžu zasahovať do histórie transakcií a robiť úpravy, meniť stav na účtoch alebo rušiť transakcie. Veci ktoré sú takmer nemožné v iných kvadrantoch.

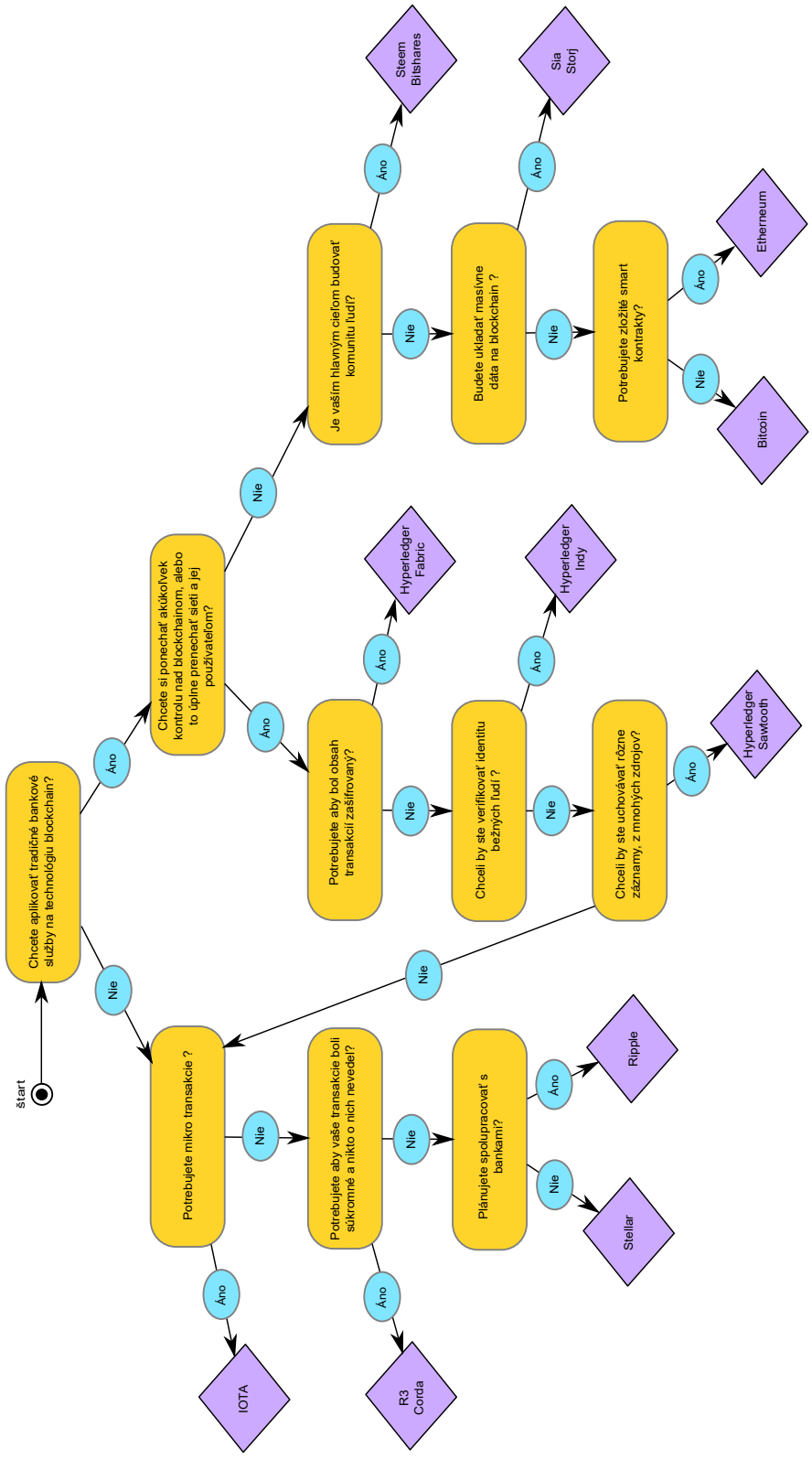
5.2 Rozhodovacie stromy použité v sprievodcovi

Pre znázornenie rozhodovacieho procesu som sa rozhodol použiť rozhodovací strom hlavne pre jeho prehľadnosť a jednoznačnú interpretáciu. Jedná sa o grafické znázornenie rozhodovania, pri ktorom sa postupne odpovedá na upresňujúce otázky a postupne sa dopracujeme k výsledku. Tieto jednotlivé výsledky sú do stromu rozdelené na základe svojich spoločných vlastností.

Používam dva rôzne rozhodovacie stromy, najmä kvôli kompaktnosti a jednoduchšej orientácií používateľa. Prvá časť sa zameriava predovšetkým na správne identifikovanie potreby použitia technológie blockchain. Rozhodovací strom môže pripadať jednoduchý a zbytočný ale je to jedna z najpodstatnejších častí rozhodovania, či treba použiť blockchain technológiu. Druhý rozhodovací strom sa zameriava na identifikovanie bližších potrieb používateľa, na základe špecifickejších otázok ohľadom budúceho použitia. Na základe výsledkov ktoré vzniknú v tomto rozhodovacom strome ich budem interpretovať pri tretej časti a to celkovom pohľade na zaradenie technológií.



Obr. 5.2: Diagram pre rozhodovací strom potreby použitia technológie blockchain



Obr. 5.3: Diagram pre rozhodovací strom výberu správnej technológie blockchain

5.2.1 Potreba blockchain technológie

Blockchain je síce fascinujúca technológia, ale nie je vhodná na všetko. Mnoho ľudí si myslí, že použitie blockchainu im zaručí úspech ich projektu a vôbec sa nezamýšľajú nad tým, či je to vôbec správne riešenie. Voľba správnej technológie pre projekt často predurčuje úspech daného projektu. Preto sa budeme v prvej časti rozhodovacieho stromu venovať, či je vôbec potrebné používať technológiu blockchain.

Ako moste vidieť na obrázku 5.2, tento rozhodovací strom je jednoduchý a snaží sa vylúčiť čo najväčšie spektrum možností. Postupne si rozoberieme všetky otázky a rôzne možnosti.

1. ***Potrebujete databázu?*** Blockchain je zo svojej podstaty špeciálny typ databázy, dalo by sa to v zjednodušenej podobe nazvať aj účtovná kniha. Preto je táto elementárna otázka nesmierne dôležitá, používateľ by mal zvážiť či je databáza naozaj potrebná pre jeho potreby. V prípade, že nie je databáza potrebná mal by zvážiť iné možnosti uchovávania dát ako napríklad Excel tabuľky alebo vyhľadávacie zoznamy.

2. ***Potrebujete mazať alebo inak upravovať už uložené dáta?*** Táto otázka je zameraná na vylúčenie prípadov, kde sa veľmi aktívne zasahuje do databázy. Blockchain neumožňuje meniť už uložené dáta. Nedovoľuje to jeho vnútorná integrita, pretože by sa zmenil koreňový hash merklovho stromu a museli by sa všetky bloky na novo overovať. Preto sa prípade, že je nutné meniť už uložené dáta odporúča použiť inú tradičnú databázu.

3. ***Obsluhujú túto databázu viacerí nezávislí účastníci?*** Táto otázka ma dve roviny, ta prvá je, či existuje viacero účastníkov, ktorý budú používať databázu a ta druhá či sú nezávislí. V prípade, že nie je potrebné aby túto databázu používali viacerí účastníci naraz nemá zmysel budovať najkomplexnejšiu distribuovanú databázu akú poznáme. Stále totiž platí, že je najlepšie mať dáta čo najbližšie. Nezávislosťou sa myslí, či to nie sú len pobočky nejakej materskej inštancie, blockchain je zameraný na distribuovanosť siete a decentralizáciu, ak existuje prísna hierarchia účastníkov, ktorý budú databázu používať. Stráca toto riešenie efektívnosť a vlastne aj zmysel.

4. ***Majú títo účastníci problém dohodnúť sa, kto bude spravovať databázu?*** V bežnej prevádzke decentralizovanej databázy existujú situácie, kde sa dvaja alebo viacerí účastníci musia dohodnúť na tom čo je vlastne pravda. V týchto prípadoch sa väčšinou vyberie jeden účastník, ktorý bude kontrolovať správnosť všetkého. Jedná sa v mnohých prípadoch o nejaký hlavný uzol, ktorý ma právo všetko meniť. Mnohokrát to je samotná firma, ktorá spravuje databázu. Ak nie je možné vybrať takýto centrálny bod, či už preto lebo neexistuje alebo sa nedá zaručiť

jeho správne a poctivé správanie. Prichádzame do bodu kedy bude treba naozaj distribuovanú peer-to-peer databázu a tou je blockchain.

5.2.2 Upresnenie správnej blockchain technológie

Rozhodovanie o tom akú architektúru blockchain technológie využiť nie je o nič ľahšie ako rozhodovanie, či vôbec použiť blockchain technológiu. Je potrebné zohľadniť mnoho faktorov ako prístup či rýchlosť a implementačných detailov ako napríklad, spôsob akým bude sieť dorozumievať. V tejto fáze výberu blockchain architektúry je potrebné si naozaj rozmyslieť, čo od implementácie blockchain technológie požadujeme, mnoho rozhodnutí je už nenávratných a rôzne si vyžadujú úplne rozličný prístup od vytvorenia až po nasadenie. V nasledujúcej druhej časti rozhodovacieho stromu 5.3 sa zameriame na výber tej správnej architektúry a popíšeme si rozhodovací proces a prečo nie je taký priamočiary.

1. ***Chcete aplikovať tradičné bankové služby na technológiu blockchain?*** Tradičné bankové služby zahŕňajú napríklad lízing, hypotéku, pôžičky, predaj cenných papierov, dobropisov a iné. Problém s týmito službami je, že nám veľmi nezapadajú do kontextu blockchain sveta. Aj napriek tomu, že ich verejný blockchain dokáže napodobniť respektíve substituovať niečím iným, myslím si, že tieto dlho praktikované služby ostanú v takmer nezmenenej podobe ibaže budú fungovať na nových technológiách. Tento predpoklad vylučuje akúkoľvek verejnú kontrolu respektíve v blockchain terminológií anonymitu overovateľov. Banky fungujú stovky ak nie tisíce rokov na uzatvorenom systéme a obmedzenom prístupe a neexistuje dôvod prečo by sa to malo zrazu zmeniť. Uzatvorený a centralizovaný systém nijak nezapadá do kontextu o čo sa snaží technológia blockchain. Aj keď môžete argumentovať, že tieto systémy ktoré banky navrhujú a vyvíjajú majú distribuovanú sieť a ako tak decentralizované rozhodovanie, lenže všetky tieto decentralizované uzly sú pod niekoho kontrolou, nie sú to samostatne zmýšľajúce osoby, ktoré by konali vo vlastnom záujme. Preto sa tieto systémy v budúcnosti, podľa môjho názoru, nebudú ani volať blockchain pretože tento termín predstavuje iné ideály na ktorých vznikol.

2. ***Chcete si ponechať akúkoľvek kontrolu nad blockchainom, alebo to úplne prenechať sieti a jej používateľom?*** Toto je jedna z najťažších otázok, ktoré sa spájajú s výberom blockchain architektúry. Rozhodnutie medzi permissionless a permissioned typom architektúry rozhoduje nielen o tom, ktoré hlasovacie mechanizmy je možné použiť ale aj o tom ako veľmi chceme vložiť dôveru do rúk ľudí, ktorý budú tento systém používať. Každý človek si samozrejme chce prenechať nejakú kontrolu nad svojím výtvorom, no absolútne vzdanie sa akejkoľvek kontroly prináša mnoho výhod. Medzi tie hlavné patrí dôvera ľudí, že im s tým

nebude nikto manipulovať. História ukázala, že štáty a iné inštitúcie sú ochotné špehovať a manipulovať svojich občanov. Vzdanie sa akejkoľvek kontroly eliminuje pozíciu, kde by sa niekto mohol pokúšať tlačiť alebo inak ovplyvňovať sieť, zákonmi alebo inými prostriedkami.

Permissionless blockchain má samozrejme aj svoje nevýhody a preto môžeme pozorovať nárast záujmu o permissioned blockchain v korporátnom prostredí. Z pohľadu firmy je nemožné, aby použili svoje peniaze či reputáciu a nechali systém rásť bez akejkoľvek kontroly alebo usmerňovania. Z právneho hľadiska to nie je korektné, pretože permissionless blockchainy sú takpovediac mimo existujúce právne normy. A ak by ho vytvorila nejaká právne korektné vytvorená inštitúcia, musela by za neho právne zodpovedať, čo v prípade žiadnej kontroly nad jeho smerovaním firmu pomaly ale určite privedie ku krachu.

Ďalšou nevýhodou je, že v permissionless blockchaine musia byť všetky transakcie viditeľné pre všetkých, je pre mňa nepredstaviteľné ako by mohli bankové inštitúcie ukázať ich všetky transakcie verejnosti, to je žiaľ cena ktorou sa platí za úplnú decentralizáciu a distribuovanosť siete.

3. ***Je vaším hlavným cieľom budovať komunitu ľudí?*** Účelom tejto otázky je lepšie určiť potrebný hlasovací mechanizmus. Aj keď má permissionless blockchain mnoho variant hlasovacích mechanizmov, ktoré môže použiť DPoS vyniká v svojej schopnosti budovať silnú a jednotnú komunitu. Jeho systémom voľby jednotlivcov z pomedzi uchádzačov dokáže naozaj vybrať najlepších lídrov pre komunitu a ľudia ju dokážu aktívnejšie usmerňovať.

4. ***Budete ukladať masívne dáta na blockchain?*** Ako som už spomenul, blockchain je schopný uchovávať dáta permanentne. Je to ale veľmi drahý spôsob ako tieto dáta uchovávať. Ako sme si už vysvetlil dáta sa uchovávajú vo forme merkle stromov. Táto dátová štruktúra dokáže síce verifikovať integritu dát bez potreby mať tieto dáta priamo uložené v transakcií, ale my chceme vedieť efektívne k týmto dátam aj pristúpiť. Ukladať veľké datové súbory na blockchain si vyžaduje zásadné zmeny vo fungovaní hlasovacích mechanizmov, pretože absurdne veľká veľkosť bloku je limitujúci faktor. Ak ma byť niečo na blockchaine musí to byť všade, preto by posielanie týchto veľkých blokov v momentálnej prenosovej rýchlosti nebolo jednoducho možné. Tu vzniká priestor pre špecializáciu blockchainu na tento typ služby, ktorá je jednoznačne možná no potrebuje odlišný prístup.

5. ***Potrebujete zložité smart kontrakty?*** Pojem smart kontrakt sme si už vysvetlili v sekcií 4.1, revolučnosť tejto idei dokazuje to, že takmer všetky blockchain platformy priamo podporujú smart kontrakty. Táto otázka je ale zložitejšia než sa zdá pri pohľade na diagram 5.3 zistíme,

že sa rozhodujeme medzi dvoma veľmi podobnými technológiami, kde jediné čo tieto technológie rozlišuje je turingová úplnosť a možnosť vytvárať zložité smart kontrakty. Aj keď sa ľudia pokúšajú doplniť Bitcoin o turingovu úplnosť pridaním side chain, nikdy to nebude tak plne implementované v jadre systému ako v prípade Etherneum blockchainu.

To ale neznamená, že Bitcoin je odsúdený na zánik a plne ho nahradí Etherneum, Bitcoin má svoje výhody ako absolútnu anonymitu a nemožnosť ho nijak legálne obmedzovať, pretože neexistuje entita ktorá ho spravuje. Je tak prvým a zatiaľ ešte jediným naozajstným blockchainom. V blízkej budúcnosti sa najväčšou pravdepodobnosťou vytvoria riešenia ako napríklad Lightning Network [29], ktoré umožnia bitcoinu konkurovať rýchlosťou transakcií s tými najlepšími systémami na svete.

6. ***Potrebujete aby bol obsah transakcií zašifrovaný?*** Jedným z hlavných argumentov proti permissionless blockchainu je nutnosť mať všetky transakcie zverejnené. V prípade permissioned blockchainu to tak už nie je. Preto sa naskytuje otázka, či treba teda obsah transakcií šifrovať. Šifrovanie obsahu transakcii docieli, že ľudia síce budú vedieť zistiť či s niekým obchodujete, ale už nie za koľko a pod akým kontraktom. Táto informácia je viditeľná iba pre účastníkov transakcie. Táto malá zmena oproti permissionless blockchainu má obrovské dopady na dôveryhodnosť blockchainu a spojená s riadením privilegovaných používateľov, ktorý môžu usmerňovať sieť je toto obrovský prechod od samoregulujúcich sietí ku priamo riadeným. Táto skutočnosť ale otvára dvere pre enterprise použitia veľkých korporátov.

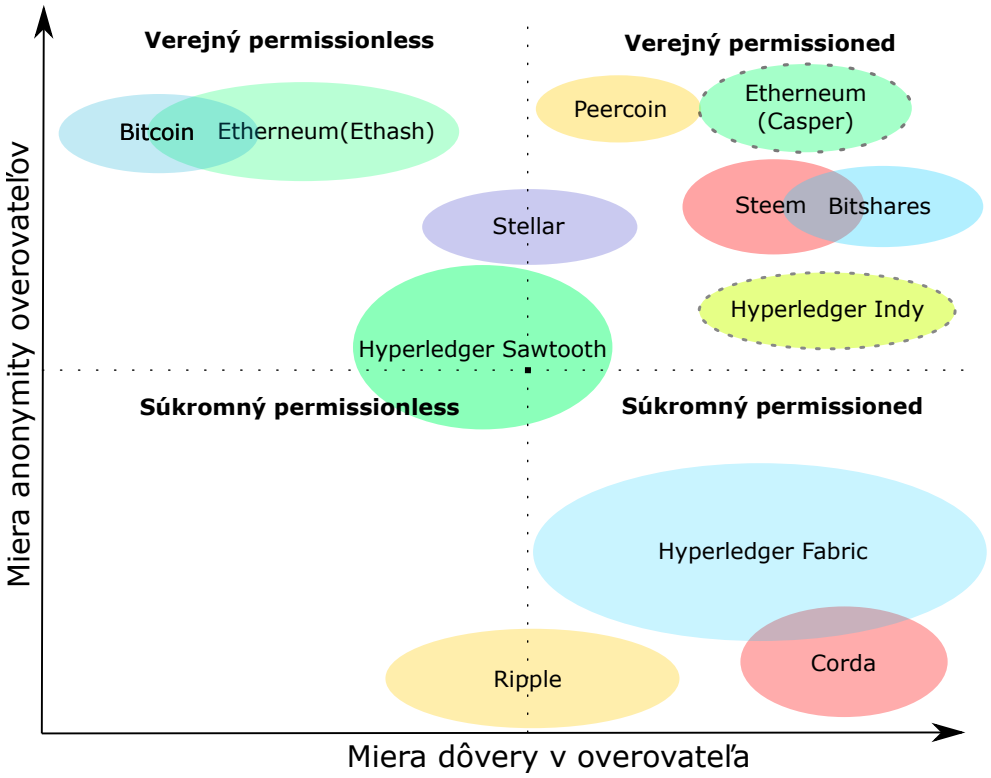
7. ***Chceli by ste verifikovať identitu bežných ľudí ?*** Ako som to už spomenul v sekcií možných prípadov použitia, overovanie identity (KYC) je jedna z najväčších nefinančných možností ako využiť blockchain. Verifikovanie identity pomocou blockchainu si vyžaduje ale veľmi úzku spoluprácu s nejakým partnerom, ktorý bude tieto identifikačné údaje na začiatku kontrolovať. Ak sa má tento spôsob rozšíriť medzi rôzne korporácie, musí byť tento partner nezávislí, respektíve najlepšie štátna agentúra. Táto podstatná zmena je nezlučiteľná s inými ďalšími použitiami blockchainu. Pretože banky a bankový sektor si veľmi ťažko nechá nejakú tretiu nezávislí stranu zasahovať do ich systémov.

8. ***Chceli by ste uchovávať rôzne záznamy, z mnohých zdrojov?*** Uchovávanie nemenných záznamov je jedna z veľkých výhod blockchainu. V prípade, že by ste chceli tieto základné dátové štruktúry obsiahnuté v merkle strome rozšíriť na niečo zložitejšie, ako napríklad celé objednávky alebo sledovanie tovaru, sú tieto dátové štruktúry nepostačujúce. Preto je potreba pozmeniť štruktúru jednotlivého bloku, a nato je vynikajúci Hyperledger Sawtooth, ktorý ponúka jednoznačne najlepšiu modularita v prípade obsahu jednotlivých transakcií.

9. ***Potrebujete mikro transakcie?*** V prípade, že potrebujete mikro platby alebo celý váš biznis plán pozostáva z mikro platieb nastáva pri použití blockchainu problém. Aj keď sme si v prvej kapitole vysvetľovali, ako dokáže blockchain znížiť cenu transakcií takmer na minimum ešte sa tak doteraz nestalo. Transakcie sú ešte stále pomerne drahé, a keďže sa platí za každú transakciu bez ohľadu nato koľko ste utratili nie sú mikro platby momentálne vôbec zmysluplné. Táto skutočnosť sa pravdepodobne časom ustáli a ceny za jednotlivé transakcie pôjdu budú klesať, je ale veľmi ťažké povedať, kedy sa bude môcť dať blockchain použiť na mikro transakcie. Je možné, že sa nikdy nepodarí znížiť cenu za jednu transakciu tak nízko aby sa mikro platby oplatili, preto je možno voľba Tangle technológie lepšie. IOTA ako jej najväčší zástupca vyzerá byť veľmi sľubne navrhnutý, má len jednu chybičku a to že je stále pod kontrolou vývojovej skupiny a tým pádom nie je kompletne bez regulácie.

10. ***Potrebujete aby vaše transakcie boli súkromné a nikto o nich nevedel?*** Mali sme tu už podobnú otázku, ktorá bola zameraná na šifrovanie obsahu transakcií, touto otázkou je ale myslená kompletne celá transakcia. Existujú prípady kedy by ste si neželali aby niekto vedel že s niekým vôbec obchodujete, poprípade sa nejedná o obchod ale o nejaký smart kontrakt, ktorý je potrebné utajiť. Takéto riešenie prináša Corda, kde jej unikátny overovací mechanizmus a uzavretá štruktúra umožňuje nevysielať všetky transakcie všetkým účastníkom ale iba tým zúčastnením. Ich hlavné zameranie je na archiváciu firemných dokumentov ako zmluvy a kontrakty, kde si to vyžaduje nielen plné šifrovanie ale aj diskrétnosť. Nechcete aby sa niekto dozvedel, že ste podpísali nejaké memorandum o budúcom obchode predtým ako to zverejníte, pretože by to mohli využiť špekulanti s akciami danej firmy.

11. ***Plánujete spolupracovať s bankami?*** Táto otázka obsahuje hlbšiu rovinu, v rozhodovacom strome sa rozhodujeme medzi dvoma veľmi podobnými technológiami, ktoré chcú vlastne dosiahnuť to isté ale iným spôsobom. Ripple a Stellar majú previazanú minulosť no ich cesty sa navždy rozišli a budú sa naďalej len vzďaľovať. Zjednodušiť globálne transakcie nie je jednoduché a určite existuje viacero možností ako to urobiť. Ripple sa o to snaží so spoluprácou bánk, kde sa Ripple snaží byť akýmsi prostredníkom, cez ktorý jednotlivé rôzne banky navzájom obchodujú. Jeho prísne strážená zatvorená štruktúra dodáva bankám istotu, že sa z ich peniazmi nič nestane. Stellar sa oproti tomu snaží banky z tohto procesu kompletne vylúčiť. Prenos financií z bodu A do bodu B bez akéhokoľvek prostredníka je ich hlavným cieľom. A majú preto odlišne nastavené parametre hlasovacieho mechanizmu.



Obr. 5.4: Graf znázorňuje konkrétny rozsah rôznych technológií blockchain podľa miery dôvery v overovateľa a anonymity takého overovateľa. Prelínajúce sa oblasti sú ťažko rozlíšiteľné alebo sú si jednotlivé implementácie veľmi blízke

5.3 Zaradenie do kontextu

V tejto časti vysvetlím všetky možné výsledky a pokúsim sa ich interpretovať používateľovi. Pri každom si určím jednoduché plusy a mínusy konkrétneho riešenia. Touto časťou chcem priblížiť používateľovi jednotlivé argumenty, ktoré je potrebné zvážiť pri finálnom rozhodnutí. Každopádne platí, že je potrebné zvážiť aj ďalšie implementácie v danom kvadrante, ktorý vyjde ako výsledok. Môže sa totiž jednať o veľmi špecifickú situáciu, ktorú som nezohľadnil pri vytváraní tejto práce.

- Steem/Bitshares

  Ako je možné vidieť na grafe 5.4 odporúčané riešenie leží v pravom hornom kvadrante. Tento kvadrant sa vynikajúce hodí na budovanie veľkých komunít, pretože tu patrí DPoS protokol, ktorý je nato perfektný. Jeho voľba lídrov, ktorý môžu ovplyvňovať sieť je presne na tento problém pripravená. Toto riešenie sa má menšiu mieru anonymity overovateľov oproti klasickému PoS, preto s v grafe nachádza nižšie ako Peercoin

alebo Casper. Je to spôsobené tým, že sa volia daný lídri, ktorý musia byť známy. V prípade, že by ste sa rozhodli zachovať rovnosť všetkých účastníkov, je možné použiť akýkoľvek verejnú permissionless blockchain architektúru.

+ Komunita si volí vlastných lídrov
+ Rýchlosť oproti bitcoinu
+ Flexibilita nastavenia siete
– Vedie k centralizácií moci
– Musí mať relatívne veľkú aktívnu základňu používateľov

- Sia/Stroj

  Tieto riešenia nenájdete v grafe 5.4, pretože nie sú samostatnými blockchain riešením. Jedná sa práve o unikátnu symbiózu, kde blockchain zaznamenáva transakcie o dátach, ako: kto, kde a na ako dlho ich chce uskladniť a tieto dáta sú potom pomocou rôznych mechanizmov uložené na dostupnom mieste čo najbližšie ku objednávateľovi. Blockchain teda neuchováva konkrétne dáta ale iba záväzok.

  + Decentralizované úložisko
  + Za úložné miesto platím rovno poskytovateľovi
  + Údaje sú šifrované a nikto ich nemôže spracovávať
  – Dáta nemusia byť vždy dostupné
  – Náročnejšia prevádzka

- Bitcoin / Etherneum(Ethash)

  Tieto dve technológie sú veľmi podobné a preto si ich podrobnejšie porovnáme s inými riešeniami. Ich riešenia sa nachádzajú v ľavom hornom kvadrante, kde sa jedná o tie najviac distribuované siete, ktoré sú ale veľmi energeticky náročné na prevádzku kvôli PoW. Ako si môžete všimnúť v momente, keď etherneum prejde na novú verziu, ktorá bude používať Casper, posunie sa viacej doprava ku väčšej dôvere v jednotlivého overovateľa. Táto zmena spôsobí zvýšenie rizika centralizácie ale sieť už nebude taká náročná na prevádzku. Je to cesta ktorou sa rozhodli vývojári ísť aby výrazné zlepšili škálovanie a flexibilitu. Tieto dve technológie sa hodia na systémy, ktoré dokážu fungovať verejne a bez potreby mať akúkoľvek kontrolu zvonku. Keďže sa jedná o verejný permissionless blockchain všetky transakcie musia byť verejne prístupné a to drasticky znižuje možné použitie v momentálnej dobe. Možno sa časom dostaneme do bodu kedy sa zmenia hodnoty v spoločnosti a nebude nám vadiť anonymná transparentnosť.

  + Anonymita
  + Odolnosť systému voči zásahom tretích strán
  + Transparentnosť
  – Veľká energetická náročnosť
  – Všetky transakcie sú verejne prístupné

- Hyperledger Sawtooth

  Táto technológia presahuje do každého kvadrantu, je to spôsobené jej modularitou. Táto konkrétna technológia sa dá nakonfigurovať na každú situáciu a využíva pritom ale stále PoET hlasovací mechanizmus. Táto implementácia blockchain technológie ponúka nielen veľkú flexibilitu ale vďaka PoET aj rýchlosť. Je to ideálny nástroj pre napríklad supply chain manažment alebo správu interných skladov.

  + Flexibilita
  + Nižšie prevádzkové náklady ako permissionless riešenia
  + Možnosť prispôsobiť firemným požiadavkám
  – Spolieha sa na nepreniknuteľnosť SGX od Intel–u, takže sa jedná o jediný bod zlyhania.
  – Komplexne neotestovaná technológia??

- Stellar

  Stellar vznikol ako hard fork od Ripple. Jeho cieľom je umožňovať globálne platby bez potreby mať prostredníka a za čo najkratší čas. V grafe sa nachádza medzi permissioned a permissionless, pretože má niečo z oboch. Je síce decentralizovaný ale funguje na základe dôvery v iných používateľov, ktorý musia vložiť dôveru vám. Jeho unikátna implementácia hlasovacieho mechanizmu SCP, umožňuje zachovávať decentralizáciu a vysokú rýchlosť spracovávania transakcií. Toto riešenie je veľmi vhodné na základné transakcie, aj keď podporuje multisig transakcie nevie spracovávať reálne smart kontrakty. Preto to je vhodné jedine ako platobná brána a nie ako komplexná platforma na budovanie distribuovaných aplikácii.

  + Porovnateľne lepšia škálovateľnosť ako čisto permissionless riešenia (1000 transakcií za sekundu)
  + Rýchla finalita transakcií
  – Malá developerská základňa
  – Žiadne smart kontrakty

- Ripple

  Ripple si vybral inú cestu ako Stellar. Snaží sa zjednodušiť globálne transakcie medzi bankami. V grafe sa nachádza v súkromných blockchainoch, pretože iba overený a schválený používatelia môžu overovať transakcie. Ripple bol zato veľmi kritizovaný a momentálne sa snaží viac decentralizovať svoju sieť.

  + Vysoká rýchlosť overenia transakcie
  + Škálovateľnosť (2500 transakcií za sekundu)[24]
  – Centrálne kontrolovaný
  – Riešenie hlavne pre banky a ich problémy

- Hyperledger fabric

  Hyperledger Fabric modulárna blockchainová platforma. Jej modularita umožňuje používateľovi prispôsobiť si blockchain jednoducho podľa svojich potrieb. Fabric sa nachádza v pravom dolnom kvadrante, kde sa jedná o jedno z najflexibilnejších riešení v skupine súkromných permissioned platforiem. Toto riešenie využíva skutočnosť, že je pripravené pre enterprise riešenia naplno. Jeho implementácia hlasovacieho algoritmu je veľmi rýchla a úsporná. Je to vďaka tomu, že všetci účastníci majú overenú totožnosť a transakcie overujú iba niektorý z nich.

  + Rýchlosť
  + Modularita
  + Open-source
  – Modularita pridala na komplexite
  – Nie je vhodný pre verejný blockchain

- Hyperledger Indy

  Jedná sa o modulárnu platformu pre overovanie totožnosti používateľov. Tento projekt má za cieľ drasticky znížiť náklady potrebné pre overenie totožnosti na internete. Jeho funkcionalita spočíva v tom, že sa údaje zaznamenajú na blockchain a je ich možné potom pomocou jednoduchej funkcie overiť. Táto konkrétna implementácia je ešte stále iba vo fáze návrhu preto je v grafe 5.4 zaznačená prerušovanou líniou. V prípade úspešného nasadenia má tento systém potenciál kompletne zmeniť spôsob ako firmy overujú svojich zákazníkov.

  + Drastické zníženie ceny
  + Jednoduchosť použitia
  + Zjednotenie procesov mnohých firiem

  - Musí byť globálne adaptovaný aby splnil očakávania
  - Systém je v štádiu návrhu a nie je jasná jeho konečná implementácia.

- IOTA

  V tomto prípade sa nejedná o blockchain technológiu ale jej veľmi príbuznú obdobu nazvanú Tangle, preto ju nenájdete v grafe 5.4. Táto technológia vyniká v množstve spracovaných transakcii a neexistujú tu poplatky za uskutočnenie transakcie. Je vhodná práve pre mikro transakcie, ktoré sú mnoho–krát nevýhodné pri tradičných blockchain technológiách pre ešte relatívne vysoké poplatky za transakcie. Využitie predovšetkým pre IoT (Internet of Things) platformy.

  + Žiadne poplatky za transakcie
  + Výborná rýchlosť a priepustnosť sieťou
  - Príliš čerstvá technológia, ktorá nebola dôkladne otestovaná
  - Používa systém dôvery v určité časti sieti, ktoré môžu byť kompromitované
  - Zatiaľ málo rozšírená

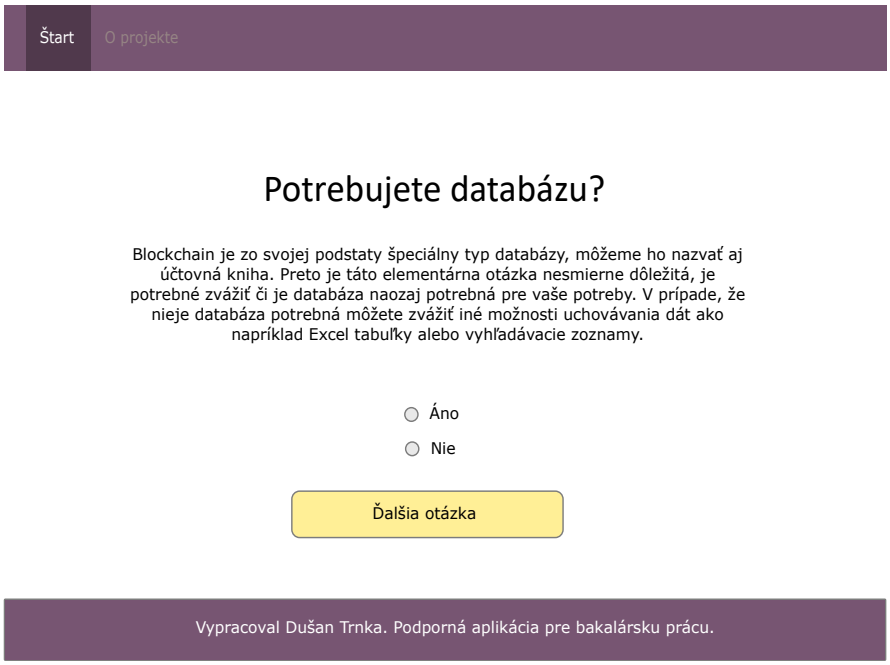
- Corda

  Corda je zástupca plne súkromného systému, kde si absolútnu kontrolu prenecháva prevádzkovateľ. Tento štýl systému je vhodný na vnútorné enterprise systémy, kde ho používajú aj tak iba ľudia z firmy. Nie je verejne prístupný a tak celá jeho pravosť a integrita leží na prevádzkovateľovi. V prípade blockchainu Corda je možné aby boli transakcie skryté a nikto o nich okrem odosielateľa a prijímateľa nevedel. Plné šifrovanie je samozrejmosťou. Tento systém ma jediné vyžitie v enterprise systémoch aj neprináša veľa výhod oproti iným enterprise riešeniam.

  + Súkromie
  + Rýchlosť
  - Kontrola prevádzkovateľa nad blockchainom
  - vysoké náklady na údržbu
  - Žiadna verejná kontrola

5.4 Podporná aplikácia

Pre jednoduché používanie som pripravil podpornú aplikáciu, ktorá aplikuje rozhodovací proces vytvorený v tejto práci. Jedná sa o webovú aplikáciu, kde



Obr. 5.5: Ukážka podpornej aplikácie pri kladení otázok. Užívateľ musí zaškrtnúť jednotlivú odpoveď a kliknúť na tlačítko „Ďalšia otázka“.

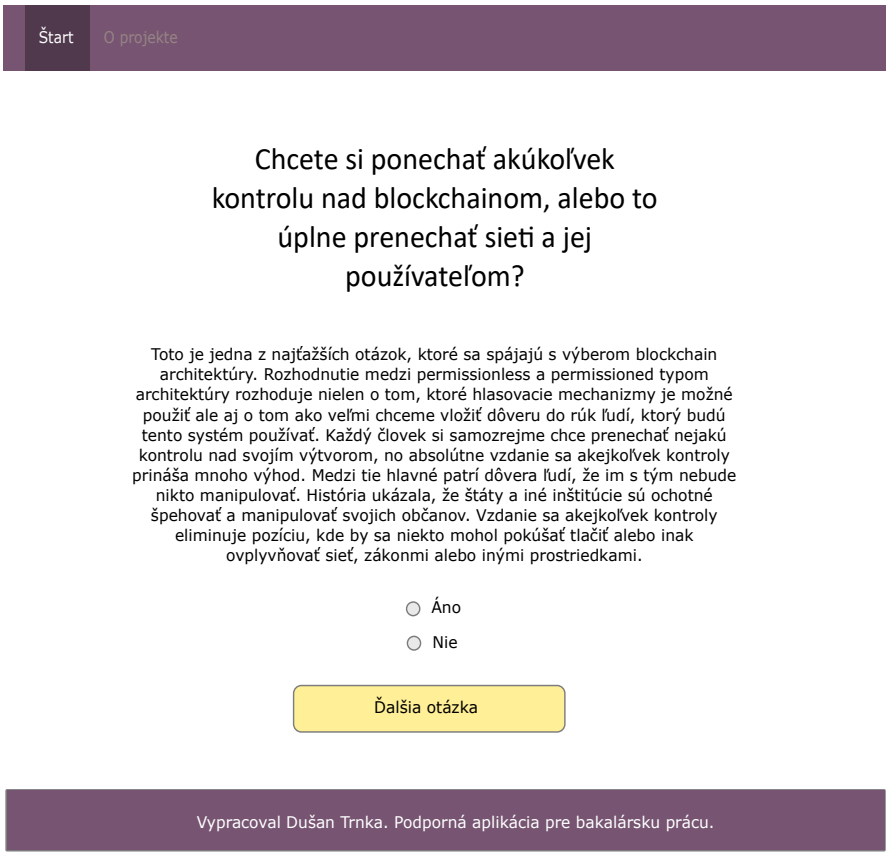
používateľ odpovedá na otázky a aplikácia to postupne vyhodnocuje. Pri rozhodovaní sa aplikácia riadi vnútorným rozhodovacím stromom, ktorý je presná implementácia 5.2 a 5.3. Ako môžete vidieť na obrázkoch 5.5, 5.6 a 5.7 táto aplikácia ma veľmi jednoduchý dizajn a je zameraná predovšetkým na funkčnosť navrhnutého sprievodcu. Užívateľ odpovedá na otázky aké môžete vidieť 5.6 a akonáhle dôjde ku výsledku zobrazí sa mu aj s malým vysvetlením a grafom, môžete vidieť na 5.7.

5.4.1 Použité technológie

Pre podpornú aplikáciu som použil Flask[30], webový framework napísaný v Python-e. Pre spracovanie jednotlivých odpovedí používam WTForms rozšírenie. Využitie týchto technológií mi umožnilo zrýchliť vývoj pri tejto jednoduchej aplikácií. Použitie napríklad Javy by bolo zbytočne prehnané. Táto aplikácia môže byť veľmi jednoducho rozšírená o nové poznatky pri rozhodovaní. Zdrojové kódy sú na priloženom médiu.

5.5 Modelové prípady

V tejto časti by som rád demonštroval ako môj sprievodca funguje na príkladoch. Modelové prípady som vybral po dohode s vedúcim aby mali čo najväčší



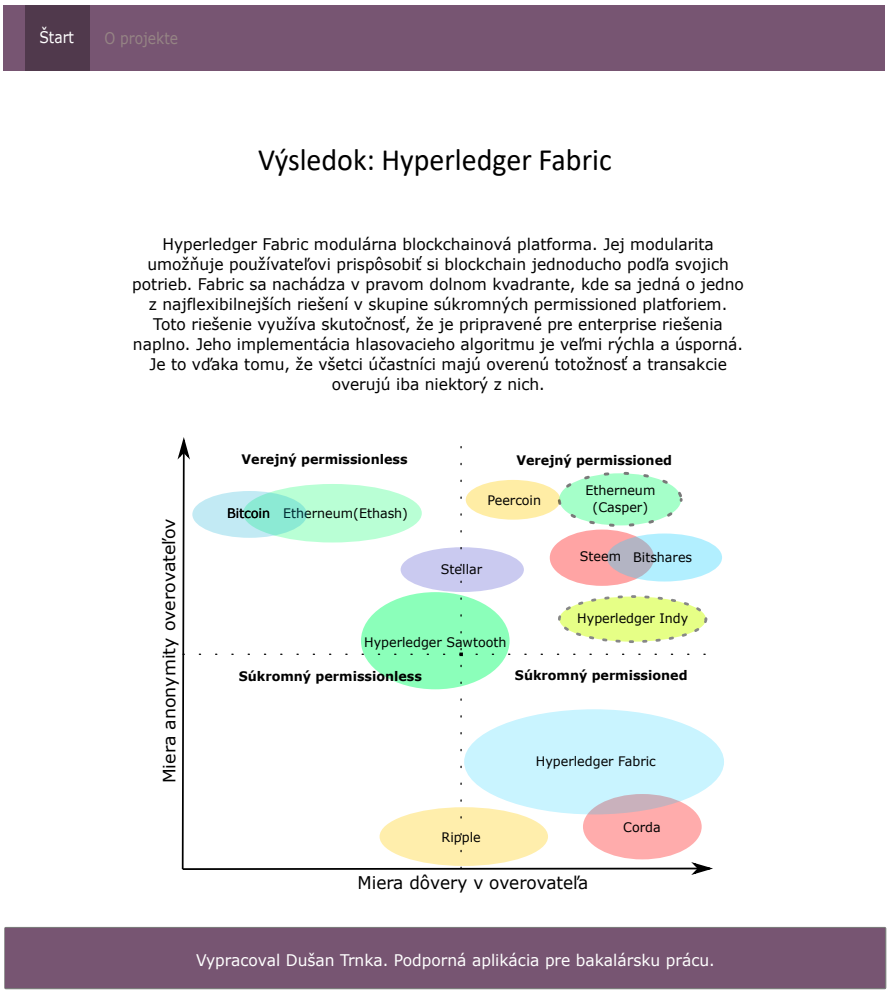
Obr. 5.6: Ukážka podpornej aplikácie pri kladení dlhšej otázky.

rozptyl. Pre každý prípad je v grafickej prílohe znázornený prechod rozhodovacím stromom. Kde ukazujem presne ako som pre konkrétny príklad odpovedal. Netriviálne otázky postupne rozoberiem s úvahou, ktorou by sa rozhodoval používateľ v danom prípade jednotlivé riešenia adekvátne okomentujem vlastnými postrehmi.

5.5.1 Zdravotný systém

5.5.1.1 Definícia

Ako ďalší modelový príklad o ktorom sa na Slovensku veľmi dlho hovorí no zatiaľ sa vôbec nerieši. Systém pre elektronické zdravotné karty je jeden z veľmi zaujímavých prípadov, kde sa jedná (v prípade Slovenska) o prepojenie štátnych inštitúcií a súkromných (zdravotných poisťovni). Jedná sa o koncept, kde by každá zdravotná karta bola digitalizovaná a údaje do nej by pridával ktorýkoľvek lekár alebo zdravotník, ktorý by pracoval s daným pacientom. Údaje by sa zjednotili, nemuseli by to ručne prepisovať všetci obvodný lekári a



Obr. 5.7: Ukážka podpornej aplikácie pri ukazovaní výsledku. Užívateľovi je ukázaná mapa kde sa nachádza daná technológia a stručný popis ponúkaného riešenia.

informácie by boli rýchlo prístupné všetkým kto ich potrebuje. Tento systém by musel byť neustále prístupný a aktuálny. Následne by tieto informácie mohli využiť napríklad zdravotné poisťovne alebo aj štát pri kontrole toho či zdravotné poisťovne správne účtujú jednotlivé zákonom predpísané zákroky. V tomto prípade za transakciu bude považovať akákoľvek lekárska správa, zákrok alebo iné výsledky.

5.5.1.2 Výsledok

Jednalo by sa o distribuovanú databázu do ktorej pristupuje naraz veľa používateľov a mala by uchovávať informácie v prístupnej podobe. Ako môžete vidieť priebeh na grafickej prílohe A.1 a A.2. Jednoznačne je možné použiť blockchain na toto riešenie pretože sme splnili všetky formálne podmienky na potrebu technológie. Pristúpili sme na možnosť kde si zachováme určitú kontrolu nad blockchainom. Chceme aby transakcie mohli vytvárať iba ľudia nato kvalifikovaný a preto nemôže ísť o permissionless systém. Odpovedali sme negatívne na možnosť šifrovať obsah transakcii, pretože chceme aby si mohol ktokoľvek s prístupom do systému pozrieť danú históriu pacienta. Samozrejme by tento prístup bol zaznamenávaný a pacient by si to vedel dohliadať. Takisto nechceme overovať identitu ľudí, pretože stačí integrovať už existujúci elektronický občiansky preukaz a už máme jednoznačnú identifikáciu. Odpovedali sme kladne na možnosť uchovávať rôzne záznamy, pretože to je to čo chceme.

Vyšla nám technológie Hyperledger Sawtooth, ktorá je schopná tieto dáta efektívne uchovávať a nepotrebuje verejnú kontrolu, pretože sa hýbeme v permissioned súkromnom systéme. Modularita tohto riešenia nám umožní to nastaviť tak aby transakcie nevidel nikto to nemá prístup do siete a to aby si každý kompetentný vedel pozrieť históriu daného pacienta. Tento systém by mohol byť podporovaný výpočtovými možnosťami štátneho cloudu a súkromných poisťovni. Ak by bol legislatívne zavedený ako povinný, je potrebné aby transakcie overovali minimálne zainteresované skupiny a nebolo to čisto v réžií súkromných poisťovní, pretože by mohli ovládnuť a podvádzať. Preto je vhodný systém integrácie štátu, súkromných poisťovni a napríklad lekárskej únie alebo iných kontrolných orgánov. Kde každá skupina má síce iné vlastné záujmy no jediný spoločný záujem je aby systém fungoval správne a pravdivo. Hlavná výhoda oproti iným zdieľaným databázam by bola kontrola viacerých nezávislých entít a prístupnosť.

5.5.2 eCommerce

5.5.2.1 Definícia

Jeden z ďalších veľmi častých príkladov je internetový obchod alebo inak povedané logistika nákupu. V tomto príklade sa nebudem zaoberať prípadom, kedy sa obchodník rozhodne umožniť platby kryptomenami, pretože to nie

je blockchainové riešenie ale iba využitie infraštruktúry ktorá tu už existuje. Bližšie sa pozrieme na prípad veľkého e–shopu ako Amazon či E–bay. Nemá zmysel uvažovať nad malými e-shopmi, pretože buď majú iba jeden sklad a ich databáza nepotrebuje byť distribuovaná alebo majú jasnú hierarchickú štruktúru. V prípade veľkých globálnych hráčov sa budeme zameriavať hlavne na evidenciu tovaru a ich logistiku. Náš globály obchod funguje v 30 krajinách a má veľké množstvo skladov a chce previesť svoju evidenciu zásielok na systém blockchain.

5.5.2.2 Výsledok

Naplniť požiadavky evidenčného systému, ktorý je odolný voči výpadkom, ma dostatočnú rýchlosť a je spoľahlivo presný je problematické. Hlavne v tradičných databázových riešeniach je odolnosť voči výpadkom náročná či už finančne alebo si vyžaduje budovanie veľkej infraštruktúry. Ako môžete vidieť v grafickej prílohe A.3 a A.4, prešli sme formálnymi požiadavkami na blockchain. Keďže sa nejedná o tradičné bankový systém je potrebné si zachovať určitú kontrolu nad systémom, budeme ho používať hlavne na interné účely. Pretože, obchodujeme s mnohými dodávateľmi a zákazníkmi nechceme aby iný dodávatelia videli za aké ceny nakupujeme s ich konkurentmi. Potrebujeme skrytý obsah transakcií, ale je nutné aby iný účastníci vedel, že transakcia prebehla. Príklad kúpim kontajner grafických kariet z Číny, chcem aby dopravca vedel že som si ich kúpil, ale už nie za akú cenu poprípade iných podmienok. Hyperledger Fabric umožňuje práve to, že dokáže navzájom prepájať niekoľko nezávislých užívateľov bez toho aby sme prezradili všetky tajomstvá biznisu. Ak by sme použili verejný permissionless blockchain museli by sme všetko zverejniť a to už nie je prospešné pre biznis.

Tento prípad použitia je možné generalizovať na takmer akýkoľvek logistický systém alebo napríklad vo verejnej permissionless podobe by to mohol byť aj systém pre štátnu poštu. Kde by si mohol každý skontrolovať, stav zásielky a kto ju práve má stačilo by mu k tomu číslo zásielky, respektíve jej verejný kľúč.

5.5.3 KOS

5.5.3.1 Definícia

KOS alebo študijný informačný systém, je komplexný systém, ktorý združuje elektronické indexy a tvorbu rozvrhu celého ČVUT. Je to veľmi dôležitý systém, ktorý musí fungovať rovnako pre každú fakultu aj keď má iné nároky. Samozrejme obsahuje databázu všetkých študentov a predmetov ktoré kedy absolvovali, vykonáva aj iné dôležité funkcie ako plánovanie rozvrhov či kontrola dodržiavania študijného plánu. Pre zjednodušenie problému sa budeme zameriavať najmä na použitie blockchainu ako databázy pre všetky informácie a všetky zmeny v nej budeme považovať za transakcie.

5.5.3.2 Výsledok

V grafickej prílohe A.5 môžete vidieť prechod rozhodovacím stromom, v tomto prípade nám vyšlo, že nepotrebujeme blockchain technológiu. Na otázku: *„Majú títo účastníci problém dohodnúť sa, kto bude spravovať databázu?“* sme odpovedali negatívne. Hlavným dôvodom prečo nepotrebujeme blockchain je nezávislosť jednotlivých fakúlt pri spracovaní svojich študentov. Ak je niekto študentom jednej fakulty asi veľmi ťažko bude jeho štúdium spravovať iná fakulta. Ak absolvujem predmet na FIT nebude mi ho kontrolovať a zapisovať FEL. Každý študent je študentom jednej fakulty existuje tam minimálny spôsob ako využiť potenciál blockchainu. Všetko čo bolo do databázy vložené je už overené a ručené fakultou, ktorej daný študent prislúcha. Keď by sa použil blockchain bolo by to zbytočne náročné a nepredstavovalo by to žiadnu zmenu oproti terajšiemu riešeniu. A to sme si tento problém zjednodušili iba základnú databázovú funkcionalitu systému.

5.6 Zhrnutie

Ukázal som spôsob akým sa dá viesť rozhodovací proces pri výbere blockchain technológie. Na praktických ukážkach som predviedol ako tento proces funguje a čo všetko je potrebné pri výbere blockchain architektúry zvážiť.

Záver

Hlavným cieľom bakalárskej práce bolo sprehľadniť blockchain architektúru a vytvoriť sprievodcu, ktorý umožní používateľovi dôjsť z záveru, či potrebuje technológiu blockchain a ak áno akú architektúru. Blockchain je síce zaujímavé riešenie pre distribuovanú databázu, no nie je to odpoveď na všetko. Ako sme si ukázali blockchain je skôr nákladný a komplexný spôsob ako takúto databázu implementovať a jednoznačne nie je všeobecným riešením na všetky typy problémov.

Rovnako sme prebrali najrôznejšie prípady použitia technológie blockchain, kde sa to naopak oplatí používať blockchain a môžeme vidieť výrazný pokrok v týchto oblastiach. Skutočnosť, že sa do blockchainu rozhodlo investovať toľko nezávislých spoločnosti predurčuje, že tu táto technológia zostane a bude sa ďalej vyvíjať. Napriek tomu, že máme niekoľko veľmi úspešných implementácií blockchain technológie, stále ešte existuje dostatok problémov ktoré je potreba vyriešiť, predtým než sa blockchain usadí ako globálna platforma. Diverzifikácia implementácií ukazuje možný budúci smer vývoja, kde budú nezávisle špecializované blockchain platformy prispôsobené iba na jednu oblasť spolu navzájom prepojené a spolupracovať.

V praktickej časti sme ukázali ako môže vyzerať rozhodovací proces pri výbere blockchainu a jeho hlavné implementačné otázky, kde si používateľ musí zvážiť čo naozaj potrebuje, pretože môže síce používať blockchain technológiu no v súkromnom permissioned systéme sa to nemôže porovnávať s verejným permissionless systémom. Dočasná nejednoznačnosť definície blockchainu umožňuje nazvať čokoľvek čo používa reťaz blokov ako blockchain, aj keď to nedáva zmysel. Budúce regulácie a ďalší nezastaviteľný vývoj ukáže aké miesto si táto technológia v spoločnosti nájde.

Všetky ciele tejto práce považujem za splnené. Rýchly vývoj blockchain technológie predstavuje príležitosť túto prácu rozšíriť aj pre ďalšie nové implementácie ako aj možnosť zamerať sa výlučne na jeden typ, napríklad permissionless verejný blockchain. Táto práca bude mať prínos hlavne pre ľudí, ktorý niečo už o blockchain technológií počuli a chceli by sa dozvedieť viac v

ucelenej forme. Na priloženom fyzickom médiu prikladám všetky zdroje, ktoré som pri vypracovávaní tejto práce použil. Podporná aplikácie taktiež priložená na fyzickom médiu má najväčší potenciál práve pre ľudí, ktorý by napríklad chceli rýchlo zistiť, či má pre nich zmysel použiť blockchain technológiu. Pre mňa mala táto práca obrovské prínosy, pretože som sa skutočne zorientoval vo svete blockchain technológií a plánujem využiť moje nadobudnuté znalosti v ďalšom akademickom a kariérnom raste.

Literatúra

[1] Satoshi Nakamoto: Bitcoin: a peer-to-peer electronic cash system. [online], November 2008, [Prevzaté 12.4.2018]. Available at WWW: <https://bitcoin.org/bitcoin.pdf>

[2] Don Tapscott, A. T.: *Blockchain revolution*. Penguin, Máj 2016, ISBN 978-0399564062.

[3] Stiglitz, J. E.: Lessons from the global financial crisis of 2008. 2010.

[4] Ernst & Young LLP: The Big Data Backlash. [online], December 2013. Available at WWW: <http://tinyurl.com/ptfm4ax>

[5] Panemon Institute LLP: 2015 Cost of Data Breach Study: Global Analysis. [online], December 2015, sponzorované spoločnosťou IBM. Available at WWW: <www-03.ibm.com/security/data-breach>

[6] Panemon Institute LLP: 2014 Fifth Annual Study on Medical Identity Theft. [online], Február 2015, sponzorované spoločnosťou Medical Identity Fraud Alliance. Available at WWW: <https://tinyurl.com/q9plv4t>

[7] Spies, T.: Public Key Infrastructure. In *Computer and Information Security Handbook (Third Edition)*, Elsevier, 2017, pp. 691–711.

[8] Jess Denham: Taylor Swift reveals why she quit Spotify: I will not dedicate my life's work to an experiment. November 2014, [prevzaté 17.4.2018]. Available at WWW: <https://tinyurl.com/y9xzut2b>

[9] World Bank: Massive Drop in Number of Unbanked, says New Report. Apríl 2015, [prevzaté 18.4.2018]. Available at WWW: <https://tinyurl.com/nwcpudz>

[10] Zheng, Z.; Xie, S.; Dai, H.; etc.: An overview of blockchain technology: Architecture, consensus, and future trends. In *Big Data (BigData Congress), 2017 IEEE International Congress on*, IEEE, 2017, pp. 557–564.

[11] Fleder, M.; Kester, M. S.; Pillai, S.: Bitcoin transaction graph analysis. 2015. Available at WWW: <https://arxiv.org/abs/1502.01657>

[12] Sankar, L. S.; Sindhu, M.; Sethumadhavan, M.: Survey of consensus protocols on blockchain applications. In *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on*, IEEE, August 2017. Available at WWW: <https://ieeexplore.ieee.org/abstract/document/8014672/>

[13] Buterin, V.: On Public and Private Blockchains. [online], August 2015, prevzaté 20.4.2018. Available at WWW: <https://tinyurl.com/olkdtwu>

[14] Hearn, M.: Corda: A distributed ledger. 2016. Available at WWW: <https://tinyurl.com/y989w2lz>

[15] Foundation, T. L.: Hypeledger Fabric. [online]. Available at WWW: <https://www.hyperledger.org/>

[16] O'Dwyer, K. J.; Malone, D.: Bitcoin mining and its energy footprint. 2014.

[17] Sigrid Seibold, G. S.: Consensus Immutable agreement for the Internet of Value. 2016. Available at WWW: <https://assets. kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf>

[18] Edge, J.: ELC: SpaceX lessons learned. [online], prevzaté 1.5.2018]. Available at WWW: <https://lwn.net/Articles/540368/>

[19] Jakobsson, M.; Juels, A.: Proofs of work and bread pudding protocols. In *Secure Information Networks*, Springer, 1999, pp. 258–272.

[20] Back, A.; etc.: Hashcash a denial of service counter-measure. 2002. Available at WWW: <https://tinyurl.com/y94mco5n>

[21] Buterin, V.: Dagger Hashimoto. [online], 2014, prevzaté 14.4.2018. Available at WWW: <https://github.com/ethereum/wiki/wiki/Dagger-Hashimoto>

[22] Schuh, F.; Larimer, D.: BitShares 2.0: Financial Smart Contract Platform. 2015.

[23] Larimer, D.: Steem. 2017. Available at WWW: <https://steem.io/steem-whitepaper.pdf>

[24] David Schwartz, A. B., Noah Youngs: The Ripple Protocol Consensus Algorithm. 2014. Available at WWW: <https://tinyurl.com/mrdyc9z>

[25] Mazieres, D.: The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, 2015.

[26] Swan, M.: *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc., 2015, ISBN 978-1491920497.

[27] Szabo, N.: The idea of smart contracts. *Nick Szabo Papers and Concise Tutorials*, 1997.

[28] Reuters, T.: Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity. [online], Máj 2016, prevzaté 15.4.2018. Available at WWW: <https://tinyurl.com/y9e4rqe5>

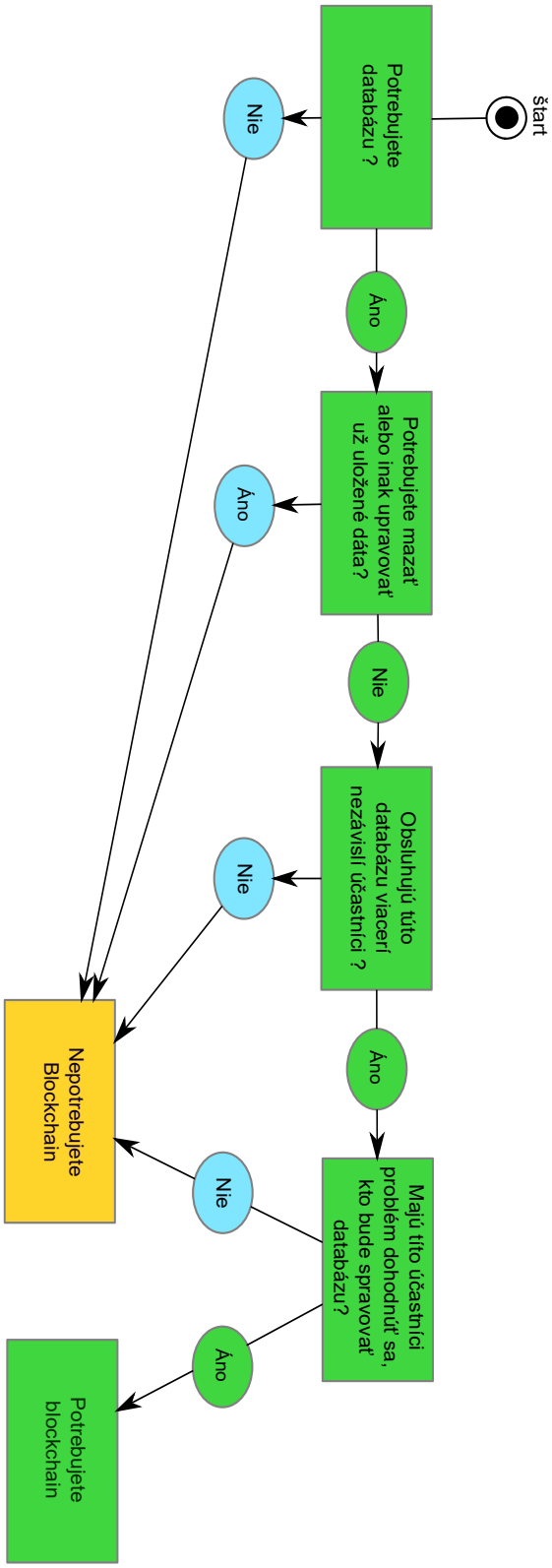
[29] Poon, J.; Dryja, T.: The bitcoin lightning network: Scalable off-chain instant payments. 2016. Available at WWW: <https://tinyurl.com/ybrpa56f>

[30] Grinberg, M.: *Flask web development: developing web applications with python*. Ö'Reilly Media, Inc.", 2018, ISBN 978-1449372620.

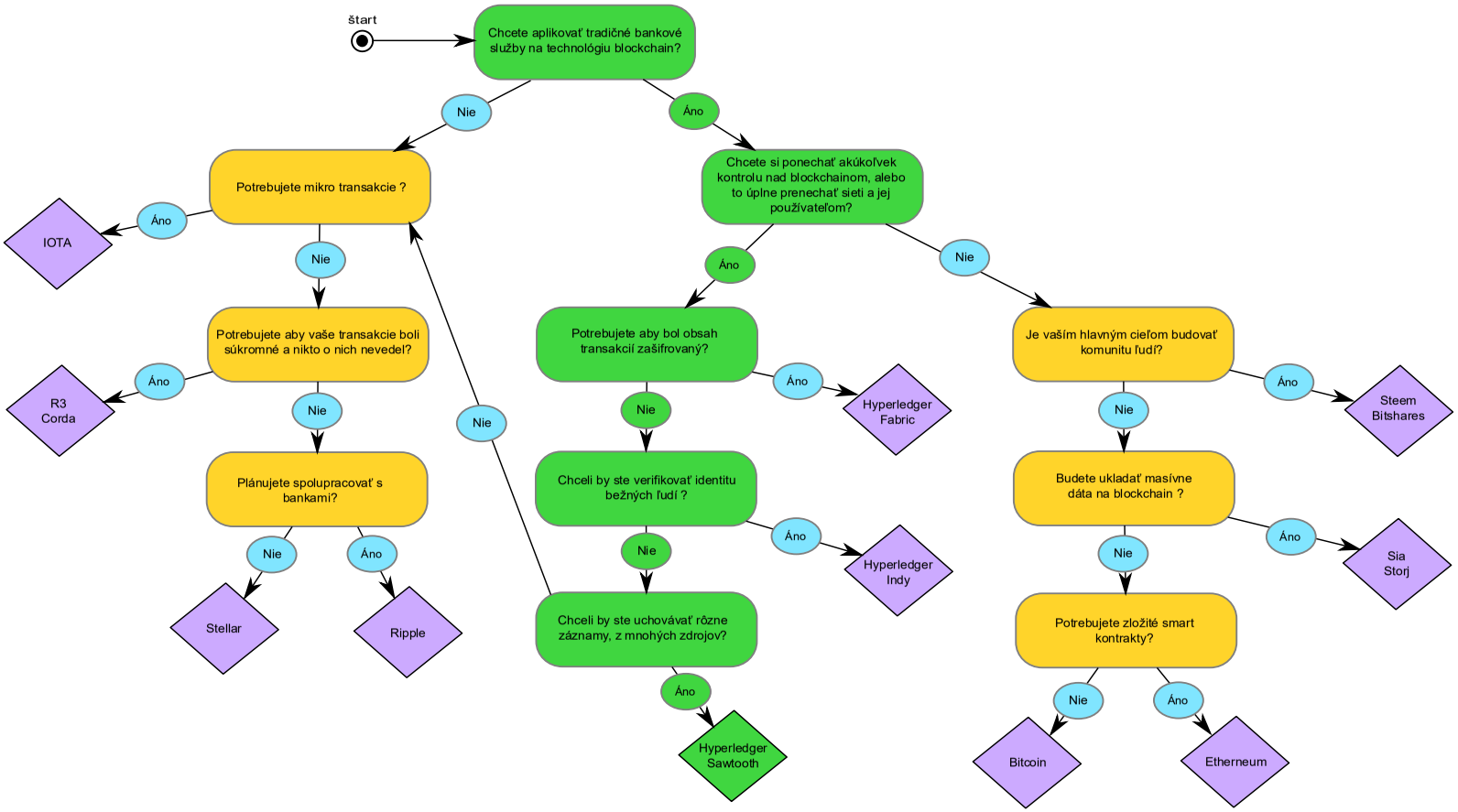
Dodatok A

Grafická príloha

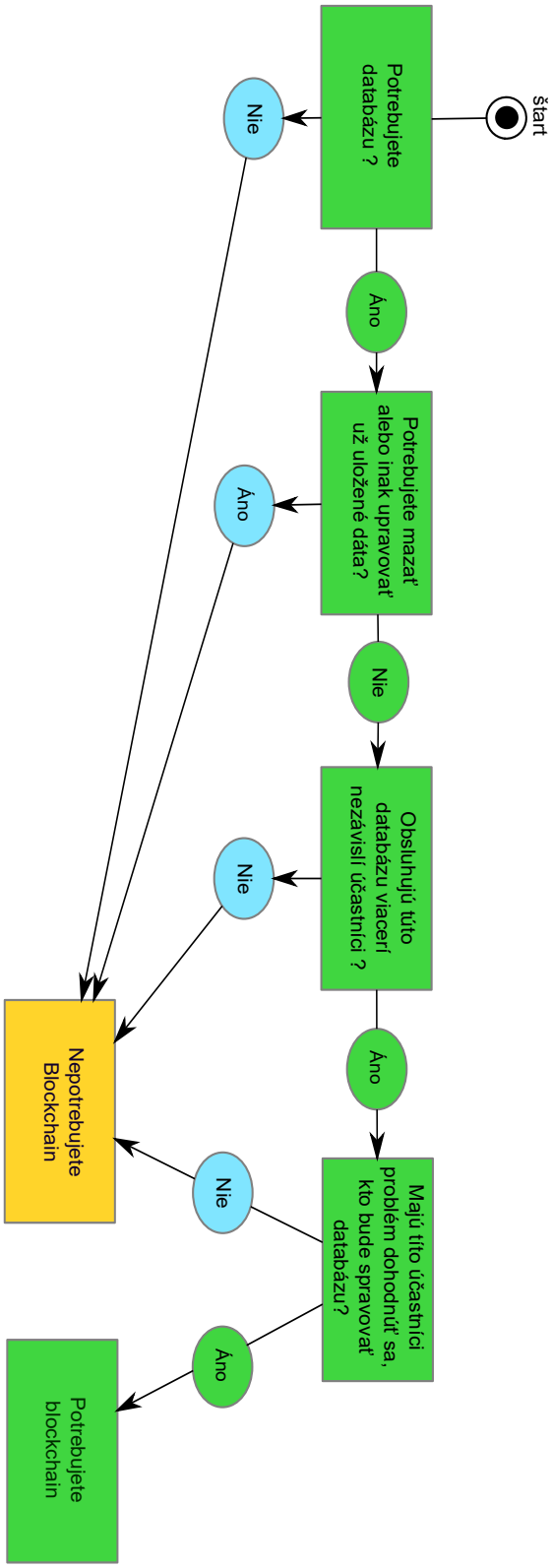
V tejto časti sa nachádzajú grafické prílohy pre prechody rozhodovacím diagramom pre jednotlivé modelové prípady.



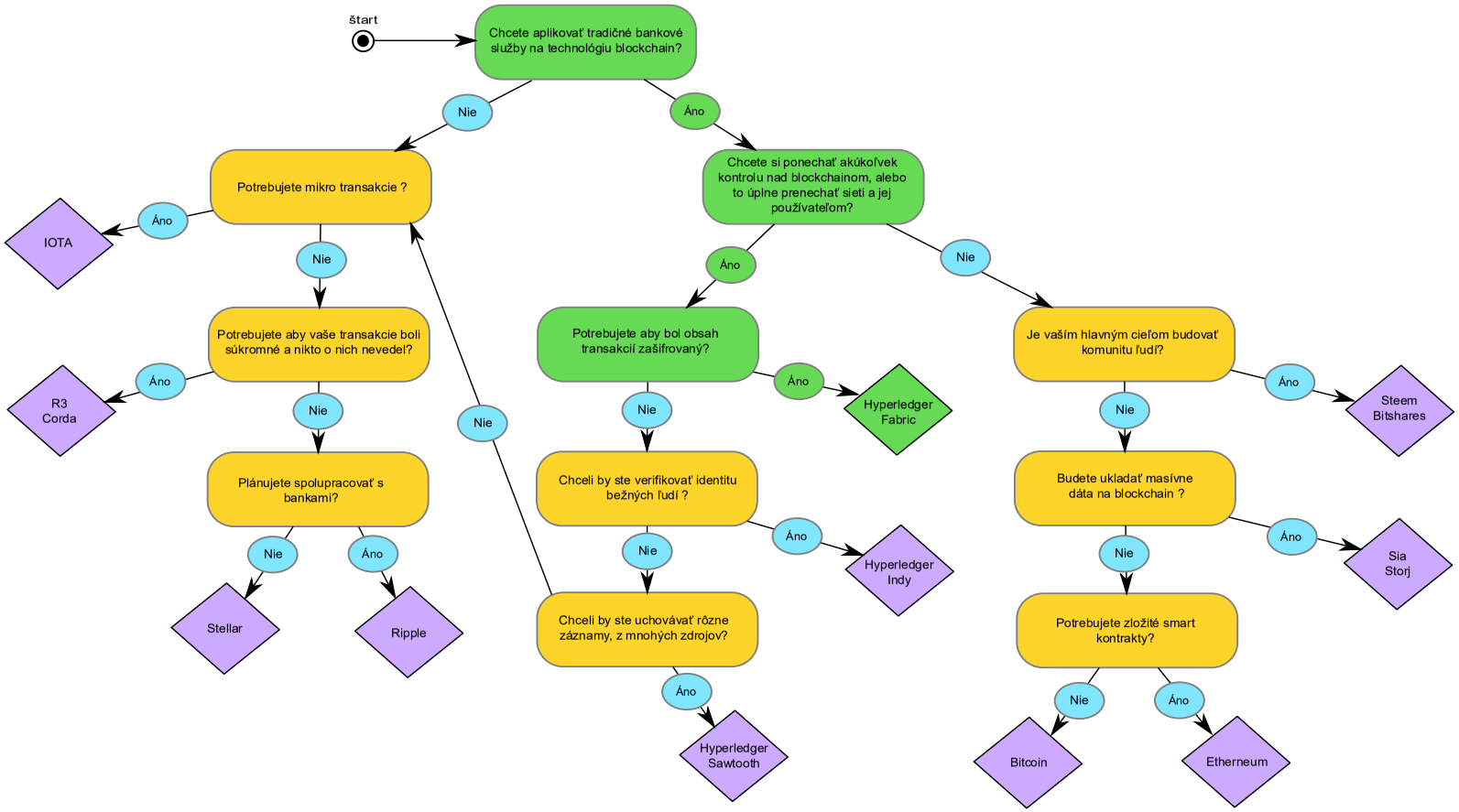
Obr. A.1: Znázornený prechod diagramom pre prvý modelový príklad. Prvá časť.



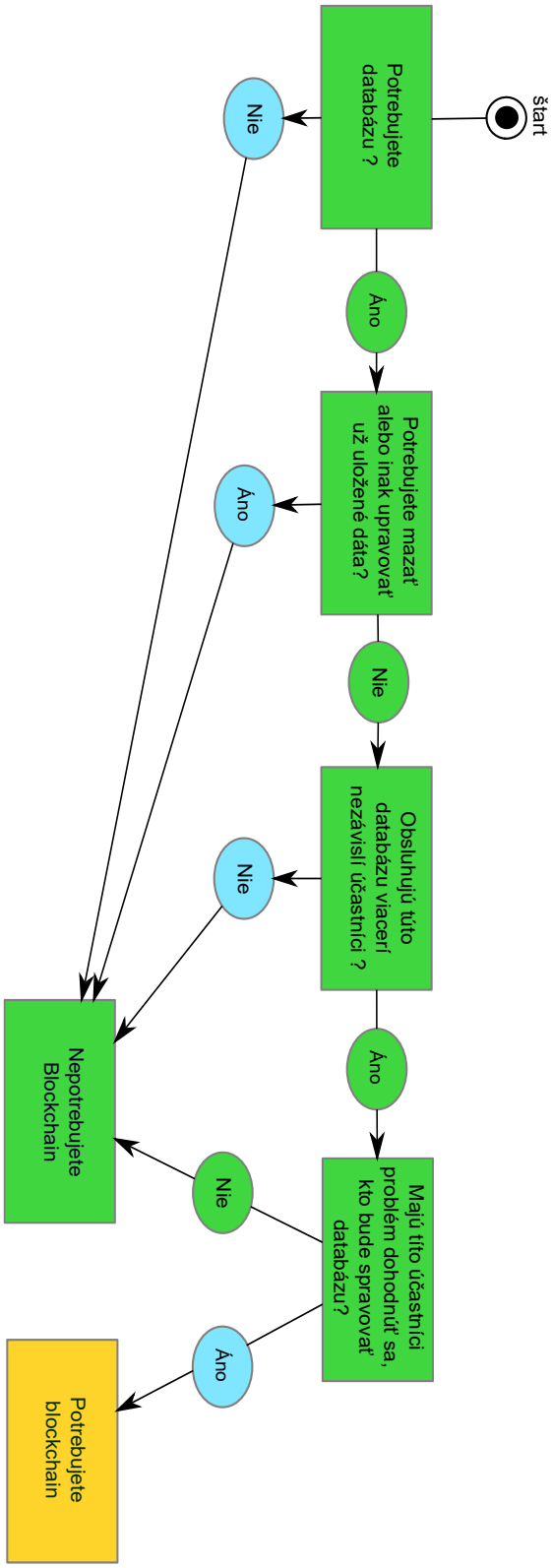
Obr. A.2: Znázornený prechod diagramom pre prvý modelový príklad. Druhá časť.



Obr. A.3: Znázornený prechod diagramom pre druhý modelový príklad. Prvá časť.



Obr. A.4: Znázornený prechod diagramom pre druhý modelový príklad. Druhá časť.



Obr. A.5: Znázornený prechod diagramom pre tretí modelový príklad. Prvá časť.

Dodatok **B**

Zoznam použitých skratiek

BA Byzantine Agreement

BFT Miera odolnosti voči byzantskej chybe (Byzantine Fault Tolerance)

BTC Token bitcoin blockchainu

DPoS Delegated Proof of Stake

FBA Federated Byzantine Agreement

IoT Internet of Things

IPO Initial Public Offering

PBFT Practical Byzantine Fault Tolerance

PKI Infraštruktúra verejného kľúča (Public Key Infrastructure)

PoS Proof of Stake

PoW Proof of Work

SCP Stellar Consesnsus Protocol

UNL Unique Node List

Dodatok C

Obsah priloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `impl` ..... zdrojové kódy implementácie
    - `static` ..... Obrázky použité v implementácií
    - `templates` ..... HTML šablony pre implementáciu
  - `thesis` ..... zdrojová forma práce vo formáte LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce vo formáte PDF
  - `thesis.ps` ..... text práce vo formáte PS