VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ
DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

NÁZEV PRÁCE

THESIS TITLE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. JURAJ HOLUB**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. IVAN HOMOLIAK, Ph.D.**
SUPERVISOR

BRNO 2021

Abstrakt

Do tohoto odstavce bude zapsán výtah (abstrakt) práce v českém (slovenském) jazyce.

Abstract

Do tohoto odstavce bude zapsán výtah (abstrakt) práce v anglickém jazyce.

Kľúčové slová

Sem budou zapsána jednotlivá klíčová slova v českém (slovenském) jazyce, oddělená čárkami.

Keywords

Sem budou zapsána jednotlivá klíčová slova v anglickém jazyce, oddělená čárkami.

Citácia

HOLUB, Juraj. *Název práce*. Brno, 2021. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Ivan Homoliak, Ph.D.

Název práce

Prehlásenie

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana X... Další informace mi poskytli... Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
Juraj Holub
25. septembra 2021

Poďakovanie

V této sekci je možno uvést poděkování vedoucímu práce a těm, kteří poskytli odbornou pomoc (externí zadavatel, konzultant apod.).

Obsah

Kapitola 1

Úvod

TODO

Kapitola 2

Blockchain

Táto kapitola vysvetľuje základné koncepty a pojmy spojené z technológiou blockchain, ako aj samotnú dátovú štruktúru blockchain. Sekcia 2.1 vysvetľuje pojmi distribuovaná účtovná kniha a blockchain. Ďalej rozoberá vlastnosti a využitie blockchainu. Sekcia 2.2 vysvetľuje kryptografiu používanú v blockchaine (hashovanie, a asymetrická kryptografia). Sekcia 2.3 popisuje peer-to-peer siete a ich využitie v blockchaine. Nazáver sú v sekcii 2.4 spojené všetky vysvetlené koncepty dokopy a je popísaná samotná dátová štruktúra blockchain.

2.1 Distribuovaná účtovná kniha

Účtovná kniha (anglicky *ledger*) sa v histórii ľudstva dlhodobo používa na záznam rôznych položiek, najčastejšie peňazí a majetku. Príchod digitalizácie a globalizácie presunul tento známy koncept z papierovej podoby do elektronickej. Toto prináša nové výzvy z hľadiska bezpečnosti. *Distribuovaná účtovná kniha* (anglicky *distributed ledger*) je všeobecne technológia, ktorá poskytuje dôveryhodnú a bezpečnú databázu zdieľanú naprieč viacerými inštitúciami, krajinami a to typicky verejne. Najtypickejším odvetvím využitia distribuovanej účtovnej knihy je bankovníctvo. Banka poskytuje centralizovanú autoritu, ktorá zabezpečuje bezpečnú manipuláciu s peniazmi klientov. Tento koncept označujeme ako centralizovaná účtovná kniha. [16]

V roku 2008 bola publikovaná práca [12], ktorá navrhla *decentralizovanú* distribuovanú účtovnú knihu. Práca navrhla koncept elektronického platobného systému, ktorého bezpečnosť je založená na kryptografickom dôkaze namiesto dôvere v centralizovanú autoritu. Takáto distribuovaná účtovná kniha sa nazýva **blockchain**.

2.1.1 Vlastnosti blockchainu

Blockchain je dátová štruktúra, ktorá má nasledujúce vlastnosti:

- **Decentralizácia**: Blockchain funguje nad peer-to-peer sieťou, ktorá nepotrebuje centralizovanú dôveryhodnú autoritu.
- **Auditovateľnosť**: Blockchain v sebe nesie celú histórie zmien jeho obsahu a teda každú zmena stavu dát uložených v blockchaine je možné sledovať.
- **Nemennosť**: Pri správnom použití a dostatočne veľkej sieti nie je možné zmeniť histórie alebo dátový obsah blockchainu.

- **Anonymita**: Užívatelia pracujúci s blockchainom používajú na identifikáciu asymetrickú kryptografiu s digitálnym podpisom. Takýto kryptografický identifikátor neodhaľuje skutočnú identitu užívateľa a pritom umožňuje nepopierateľne určiť vlastníka elektronického zdroja.

Tieto vlastnosti blockchainu sú zabezpečené pomocou peer-to-peer siete na ktorej je blockchain postavený (viď sekcia 2.3) a taktiež pomocou samotnej dátovej štruktúry, ktorá využíva modernú kryptografiu (viď sekcia 2.4). [1]

2.1.2 Aplikačné využitie

Blockchain bol navrhnutý a po prvýkrát implementovaný za účelom poskytnúť elektronickú peňažnú menu nezávislú od centralizovaného bankovníctva. Tento prvý, a najznámejší, blockchain je Bitcoin [12]. Avšak vlastnosti blockchainovej technológie nachádzajú uplatnenie vo veľkom množstve odvetví. Nasledujúci zoznam vymenúva niekoľko aplikácií, ktoré blockchain môže riešiť [9]:

- **Elektronická peňaženka**: Elektronické peňaženky pre obchod s nejakou formou peňazí (typicky v podobe tokenov). Takéto tokeny sú typicky vlastnené pomocou privátneho kľúča, ktorý má uschovaný majiteľ. Majiteľ môže vlastníctvo tokenov presúvať na iné subjekty v danej sieti.
- **Zmenárne**: V dnešnej dobe existuje veľké množstvo elektoronických peňažných mien postavených nad blockchainom. Takéto meny všeobecne označujeme ako kryptomeny. Z dôvodu veľkého množstva kryptomien sa prirodzene zvyšuje dopyt po zmenárni medzi jednotlivými kryptomenami. Klasická zmenáreň je riešená tradične centralizovanou autoritou. Avšak blockchain je vhodnou technológie aj pre decentralizovanú zmenáreň.
- **Súborové systémy**: V dnešnej dobe už existujú decentralizované súborové systémy založené na peer-to-peer sieťach. Implementácia takéhoto decentralizovaného súborového systému ako blockchain by nám umožnila nepopierateľne a trasovateľne verzovať zmeny v obsahu.
- **Správa identít**: Správa identít je typicky centrálna autorita, ktorá prideľuje pre konkrétne entity určité zdroje na ktoré majú právo. Ide o schému podobnú banke. Blockchain by v tomto prípade opäť umožnil náhradu tejto centralizovanej autority za decentralizovanú sieť.
- **Voľby**: Elektronické voľby sú ďalším vhodným príkladom, kde sa dá efektívne využiť blockchain. Voliace entity predstavujú decentralizovanú sieť a vlastnosti blockchainu zase poskytujú transparentnosť a verejnú overiteľnosť.
- **Reputačné systémy**: Reputačné systémy slúžia na meranie úrovne dôvery v určité entity. Typickým príkladom je reputácia rôznych predajcov na základe hlasovania zákazníkov. Transparentnosť a nemennosť blockchainovej histórie by znížila možnosť manipulácie s reputáciu v prospech nejakej entity.
- **Aukcie**: Elektronická aukcia je služba veľmi podobná elektronickej peňaženke alebo zmenárni s podobnými bezpečnostnými požiadavkami. Tieto vlastnosti by opäť dokázala pokryť technológia blockchain.

2.2 Kryptografia v blockchaine

Pre pochopenie technológie blockchain je potrebná základná znalosť modernej kryptografie. V tejto sekcii je popísaný kryptografická hashovacia funkcia (pozri 2.2.1) a jej využitie na tvorbu dátových štruktúr zabezpečených proti modifikácii obsahu (viď sekcia 2.2.2). Ďalej je vysvetlený koncept asymetrickej kryptografie a digitálneho podpisu (viď sekcia 2.2.3). Tieto kryptografické primitíva sú základom na ktorom stojí nemennosť, auditovateľnosť a anonymita blockchainu.

2.2.1 Hashovacia funkcia

Hashovacia funkcia je taká funkcia h, ktorá má ako parameter x reťazec bitov ľubovolnej dĺžky a vracia reťazec y s konštantnou dĺžkou(viď rovnica 2.1). Reťazec y voláme hash. Hashovacia funkcia vracia pre konkrétny vstup vždy rovnaký hash.

$$h(x) = y \tag{2.1}$$

Kryptografická hashovacia funkcia, alebo tiež jednocestná funkcia (anglicky *one way function*), je taká hashovacia funkcia pre ktorú platia nasledujíce tri vlastnosti:

1. Pre daný hash x je výpočetne nezvládnuteľné nájsť správu takú, že $h(x) = y$. Anglicky voláme túto vlastnosť *first preimage resistant*.
2. Pre danú správu je výpočetne nezvládnuteľné nájsť inú správu s rovnakým hashom. Anglicky voláme túto vlastnosť *second preimage resistant*.
3. Pre ľubovoľnú správu je výpočetne nezvládnuteľné nájsť inú správu s rovnakým hashom. Anglicky voláme túto vlastnosť *collision resistant*.

Hashovacie funkcie majú v oblasti počítačovej bezpečnosti dôležité využitie:

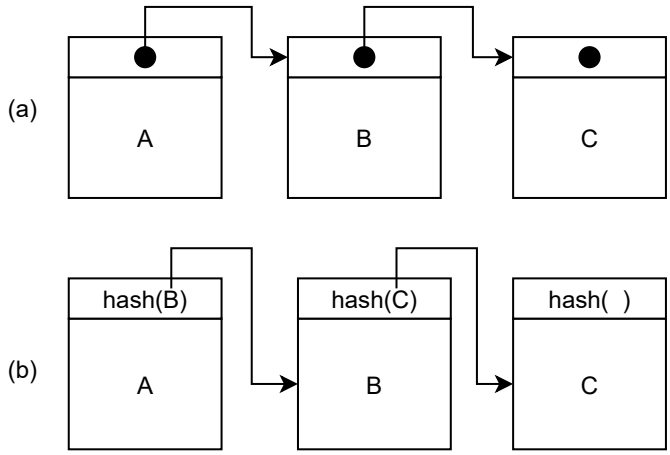
- Bezpečné ukladanie hesiel: Digitálna služba neukladá v databáze heslo, ale len jeho hash. Pri ukradnutí databázy nedochádza k odhalenie hesiel užívateľov.
- Integrita dát: Hashovacia funkcia môže byť použitá na ochranu integrity ľubovoľných dát. Ak spočítate hash veľkého súboru a bezpečne ho uložíte tak ste schopný detekovať, že niekto tento súbor zmenil.
- Digitálny podpis: Hashovacia funkcia je kryptografické primitívum potrebné pre vytvorenie digitálneho podpisu.

Existuje množstvo hashovacích funkcií. Medzi veľmi známe a používané patrí napríklad MD5 (128 bitový výstup), SHA256 (256 bitový výstup), SHA512 (512 bitový výstup). [11, 18]

2.2.2 Hash ukazovateľ

Hash ukazovateľ (anglicky *hash pointer*) je primitívom pre tvorbu dátových štruktúr s kryptografickým zabezpečením proti manipulácia s obsahom (anglicky *tamper-evident*). Hash ukazovateľ funguje ako klasický ukazovateľ v zozname či strome. Navyše však neumožňuje meniť už pridané prvky. Jediná povolená operácia je pridanie ďalšieho prvku do dátovej štruktúry.

Obrázok 2.1 demonštruje rozdiel medzi zoznamom vytvoreným pomocou klasických ukazovateľov a pomocou hash ukazovateľov. Bežný zoznam umožňuje pozmeniť ľubovoľný už



Obr. 2.1: (a) Zoznam pomocou ukazovateľov (b) Zoznam pomocou hash ukazovateľov

existujúci prvok nezávisle na zvyšku zoznamu. Naopak, hash pointer referencuje pomocou samotného dátového obsahu. Ak by sme zmenili dátový obsah prvku B, tak by sa narušila referencia v predchádzajúcom prvku. [1, 13]

2.2.3 Digitálny podpis

Digitálny podpis (anglicky *digital signature*) je kryptografický koncept používaný na autentifikáciu, autorizáciu a nepopierateľnosť. Digitálny podpis jednoznačne prepojí určitú entitu s informáciu. V technológii blockchain slúži digitálny podpis na určenie vlastníctva zdrojov, ktoré blockchain uchováva. [11, 12]

Moderná kryptografia používa pre zaistenie dôvernosti šifrovanie pomocou tajného kľúča. Pre zašifrovanie a dešifrovanie tajnej správy je potrebná znalosť tajného kľúča. Tento mechanizmus zaisťuje dôvernosť avšak nezaisťuje nepopierateľnosť pretože obe komunikujúce strany poznajú tajný kľúč a teda nie je možné právne dokázať kto správu napísal. Na zaistenie nepopierateľnosti sa používa asymetrické šifrovanie, ktoré používa dvojicu kľúčov:

- **Privátny kľúč** je tajný a pozná ho len odosielateľ správy. Odosielateľ používa tento kľúč na zašifrovanie správy.
- **Verejný kľúč** je dostupný komukoľvek. Ktokoľvek s týmto kľúčom dokáže dešifrovať správu.

Tieto dva kľúče tvoria dvojicu prepojenú matematickým spôsobom. Zo znalosti verejného kľúča je výpočetne nezvládnuteľné zistiť privátny kľúč. Zašifrovaná správa nie je dôverná pretože ktokoľvek môže použiť verejný kľúč na jej dešifrovanie. Avšak zašifrovaná správa je nepopierateľne napísaná vlastníkom privátneho kľúča.

Tento koncept je základom digitálneho podpisu. Ak chceme nepopierateľne dokázať, že nejaký dátový obsah (napríklad pdf dokument) sme vytvorili mi, tak vypočítame jeho hash (viď sekcia 2.2.1) a zašifrujeme ho naším privátnym kľúčom. Zašifrovaný hash priložíme k dokumentu. Príjemca dokumentu si následne pomocou verejného kľúča dešifruje hash priložený k správe a porovná si ho s tým ktorý vypočítal sám z danej správy. Ak sú hashe rovnaké tak nikto správu nezmenil a dokument je jednoznačne vytvorený vlastníkom tajného kľúča. Najznámejšie algoritmy na digitálny podpis sú RSA, DSA, ECDSA. [11]

2.3 Peer-to-peer sieť

Technológia blockchain je postavená na peer-to-peer sieťach. Peer-to-peer sieť sa podieľa na decentralizovanosti, nemennosti a auditovateľnosti blockchainu.

Peer-to-peer sieť je dynamický súbor nezávislých uzlov (anglicky *peers*), ktoré sú prepojené do grafu. Každý uzol obsahuje zdroje, ktoré zdieľa všetkým ostatným uzlom v sieti. [5, 17] Dôvod existencie peer-to-peer sietí je teda decentralizovaný spôsob zdieľania zdrojov ako sú súbory, fyzické zariadenia, výpočetný výkon alebo aj elektronické finančné zdroje. Dnes existuje množstvo peer-to-peer sietí. Veľmi známe sú napríklad Gnutella, Kazaa alebo BitTorrent. [2]

2.3.1 Referenčný model

Najbežnejšie technické riešenie peer-to-peer siete je navrstvenie siete (anglicky *overlay network*) na už existujúcu sieť, ktorou je typicky Internet. Takúto sieť potom môžeme definovať ako päticu (P, R, I, F_P, F_R), kde:

- P je množina uzlov
- R je množinu zdrojov
- I je priestor identifikátorov
- $F_P : P \to I$ je funkcia, ktorá mapuje uzoly na identifikátory
- $F_R : R \to I$ je funkcia, ktorá mapuje zdroje na identifikátory

Obrázok 2.2 ukazuje princíp fungovania takto definovanej siete. Tvorba siete s týmto modelom je potom závislá od šiestich návrhových aspektov:

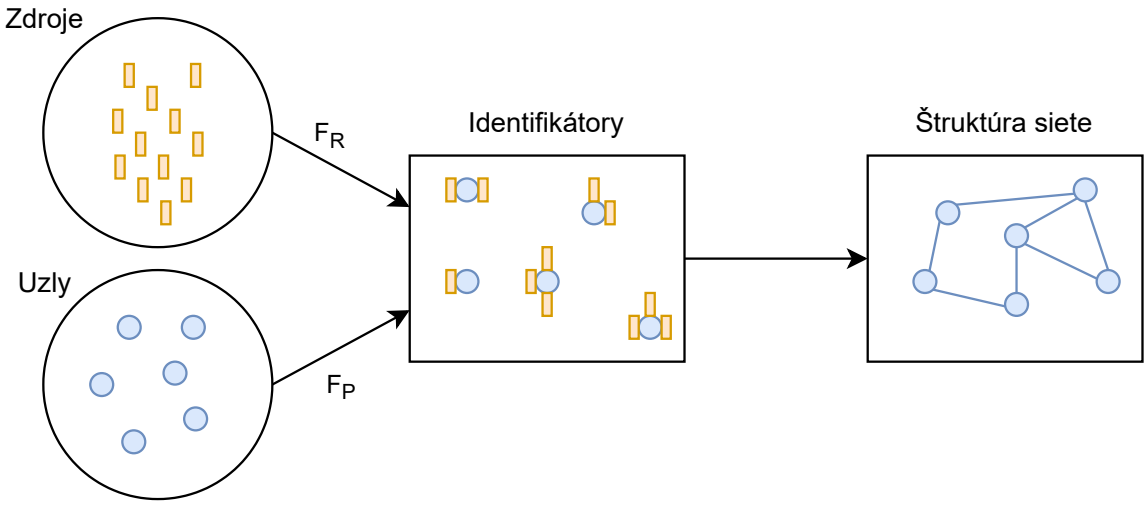
1. Voľba priestoru identifikátorov.
2. Mapovanie zdrojov a uzlov na identifikátory.
3. Správa priestoru identifikátorov v réžii uzlov siete.
4. Tvorba grafu (štruktúra siete).
5. Stratégia smerovania (anglicky *routing*).
6. Stratégia údržby.

Konkrétne riešenie pre popisovaných šesť aspektov je zavislé od požiadaviek na efektivitu, škálovateľnosť, samoorganizovateľnosť, odolnosť voči chybám a kooperáciu. [2]

2.3.2 Využitie v blockchaine

Peer-to-peer sieť umožňuje blockchainu uchovávať jeho obsah decentralizovane a pritom bezpečne. Tento koncept si vysvetlíme na prípade blockchainu, ktorý sa využíva ako kryptomena.

Elektronické financie sú typicky reprezentované pomocou elektronických mincí. Takáto minca je reprezentovaná pomocou nejakej sekvencie bitov. Avšak narozdiel od fyzických



Obr. 2.2: Referenčný model peer-to-peer siete. [2]

mincí, elektronické mince umožňujú jednoduchú falzifikáciu. Útočník skopíruje bitový reťazec danej mince a zaplatí ním viacnásobne rôzne produkty. Tento útok sa volá zdvojnásobenia výdavkov (anglicky *double-spending attack*). Proti tomuto útoku existuje tradičné zabezpečenie pomocou centrálnej autority. Banka je centrálna autorita, ktorá schvaľuje všetky manipulácie s elektronickými mincami a teda neumožní použiť mincu takýmto podvodným spôsobom. Avšak toto riešenie nie je možné použiť v decentralizovanej sieti, kde centrálna autorita neexistuje. V prípade decentralizovanej siete je možné zabrániť tomuto útoku pomocou použitia dátovej štruktúry blockchain. [8]

Kryptomena Bitcoin ako prvá navrhla použitie peer-to-peer siete v spojení s blockchain technológiou pre zabránenie double-spending útoku. V takejto sietu je jediný zdroj na zdieľanie a to je dátová štruktúra blockchain v ktorej sú uložené všetky informácie o elektronických financiách. Zjednodušene môžeme povedať, že majorita uzlov siete zdieľa rovnaký zdroj (rovnakú kópiu blockchainu). Ak chce niektorý uzol vykonať finančnú transakciu tak zašle správu s navrhovanou zmenou blockchainu do siete. Uzly v tejto sieti nie je potrebné identifikovať pretože správy posielané v tejto sieti nie sú smerované na žiadne konkrétne miesto. Keď uzol prijme správu s nejakou modifikáciu tak si overí či ide o validnú požiadavku na finančnú transakciu. Štruktúra blockchainu používa modernú kryptografiu na overenie validnosti transakcie (pozri sekciu 2.2). Blockchain, ktorý vlastní väčšina siete je ten, ktorý sa považuje za pravdu. Útočník by musel teda vlastniť aspoň 51 % uzolov v sieti aby mohol vykonať double-spending útok. Ak je daná sieť dostatočne veľká tak by toho útočník nemal byť schopný dosiahnuť. [12]

2.4 Datová štruktúra blockchain

Blockchain je dátová štruktúra podobná zoznamu (anglicky *linked list*). Blockchain organizuje dáta do podmnožín, ktoré sa volajú bloky. Blok je podobný uzlu v zozname. Každý blok obsahuje referenciu na ďalší blok. Rozdiel medzi zoznamom a blockchainom je v tom, že referencia blockchainu je zabezpečená proti manipulácia (anglicky *tamper-evident*) pomocou modernej kryptografie. Bežný zoznam používa referenciu pomocou ukazovateľov (anglicky *pointers*), ktoré môže ktokoľvek a kedykoľvek pozmeniť bez toho aby pozmenil dátový obsah.

Naopak, blockchain vôbec neumožňuje meniť už pridané bloky. Jediná povolená operácia je pridanie ďalšieho bloku na koniec blockchainu. [1]

Každý blok obsahuje dáta, ktoré sú typicky vo forme transakcií. Kryptograficky bezpečný blockchain by mohol fungovať aj tak, že v každom bloku bude uložená práve jedna transakcia. Z dôvodu optimalizácie je ale v jednom bloku uložené množstvo transakcií. Vďaka tejto optimalizácii nemusí celá sieť vytvárať konsenzus po každej transakcii. Samotné transakcie v rámci jedného bloku sú ukladané v ďalšej dátovej štruktúre, ktorá taktiež používa kryptografické hashovanie (viď sekcia 2.4.3). [13]

2.4.1 Blok

Blok sa skladá z hlavičky a tela. Telo bloku obsahuje dáta a hlavička obsahuje metadáta. Dáta v tele bloku sú uložené vo forme transakcií. Transakcie sú popísané v sekcii 2.4.2. Počet transakcií v bloku je typicky obmedzený maximálnou veľkosťou bloku. Hlavička bloku obsahuje metadáta o bloku, kde najdôležitejšie a najbežnejšie sú nasledujúce:

- Hash všetkých transakcií.
- Časové razítko vytvorenia bloku.
- Hash ukazovateľ na predošlý blok v blockchaine.
- Náhodná výzva (anglicky *nonce*), ktorej využitie vysvetľuje sekcia 2.6.1

[20]

2.4.2 Transakcia

Transakcia je elementárna dátová jednotka na ukladanie dáta v blockchaine. Bitcoin, prvý blockchain, použil transakciu na manipuláciu s elektronickými financiami. Takáto transakcia sa skladá z troch častí:

- **Množina vstupov**: Každý vstup má uložený hash predošlej transakcie s ktorej vychádza. Ďalej definuje, ktoré výstupy s predošlej transakcie si nárokuje. Nakoniec obsahuje digitálny podpis, ktorý autorizuje tvorcu transakcie.
- **Množina výstupov**: Každý výstup má hodnotu, ktorá je uchovávaná v blockchaine (typicky minca nejakej kryptomeny). Suma hodnôt všetkých výstup transakcie musí byť menšia alebo rovná sume všetkých vstupov transakcie. Ak je menšia, tak tento rozdiel je použitý ako odmena pre toho, kto publikoval tento blok blockchainu.
- **Hlavička**: Obsahuje hash transakcie, ktorý je používaný ako unikátny identifikátor pomocou, ktorého sa na transakciu odkazujeme.

2.4.3 Binárny hashovací strom

Binárny hashovací strom alebo tiež Merkle strom (anglicky *Merkle tree*) je datová štruktúra podobná binárnemu stromu, ktorá slúži na efektívne a rýchle vypočítanie hashu veľkého množstva dát. Blockchain používa tento strom na časovo efektívny výpočet hashu všetkých transakcií. Takto vypočítaný hash je uložený v hlavičke bloku.

Merkle strom je vyvážený binarny strom, kde listové uzly obsahujú jednotlivé transakcie uložené v danom bloku blockchainu. Každý nelistový uzol stromu obsahuje hash vypočítaný

z jeho potomkov. Koreňový uzol teda obsahuje hash celého stromu a teda aj všetkých transakcií. Pridanie, odobranie, zmena obsahu, alebo zmena poradia transakcií bude teda viesť k zmene koreňového hashu. Konštrukcia stromu, inak povedané výpočet hashu všetkých transakcií, prebieha následovne:

1. Všetky transakcie sú uložené do listovej úrovne stromu. Ak je počet transakcií nepárny tak, je posledná vložená dvakrát.

2. Nad každým listovým uzlom je vypočítaný hash.

3. Každý nelistový uzol skonkatenuje hash ľavého a pravého syna, vypočíta nad nimi hash a uloží si ho.

Konštrukcia takéhoto stromu pre n transakcií má časovú zložitosť $O(log(n))$. Takýto spôsob výpočtu hashu je teda veľmi efektívny pre veľké množstvo transakcií (blok v blockchaine bežne obsahuje stovky transakcií). [4]

Merkle strom umožnuje efektívne šetriť pamäťové nároky blockchainu. Do blockchainu sú neustále pridávané nové bloky, ktoré obsahujú aj rovnaké staré transakcie. Ak už sú transakcie zaznamenané v dostatočne veľkom množstve blokov tak sú z hľadiska bezpečnosti nemenné. V nových blokoch ich už preto nie je potrebné ukladať. Nový blok si preto uloží len hashe starých vetiev stromu, ale ich obsah už nepotrebuje. Takto je zachovaná integrita hashu všetkých transakcií. [12]

2.5 Ťažba blokov

Ťažba (anglicky *mining*) bloku je proces pridania nové bloku na koniec blockchainu. Ťažba bloku zahŕňa validáciu transakcií a blokov. Preto je ťažba kritická pre správne a bezpečné fungovanie blockchainu. Každý uzol siete, ktorý ťaží nové bloky sa nazýva anglickým slovom *miner*. Tieto uzly umožňujú rozširovanie blockchainu. Aby takéto uzly existovali, musia byť motivované. Miner dostane za každý vyťažený blok ako odmenu zdroje uložené v blockchaine.

Ťažba všeobecne pozostáva z nasledujúcich krokov:

1. Miner prijíma požiadavky na transakcie z peer-to-peer siete. Každú transakciu si validuje pomocou kryptografie popísanej v sekcii 2.2.

2. Miner musí taktiež udržiavať aktuálny stav blockchainu. Je potrebné sledovať či nevznikli nové bloky a udržiavať si validný blockchain.

3. Ak miner vlastní validnú a aktuálnu kópiu blockchainu, môže začať vytvárať nový blok. Do nového bloku vloží transakcie, ktoré prijal a boli validné.

4. Novo vytvorený blok je potrebné distribuovať do siete. Ak väčšina siete blok získa a akceptuje, tak bol pridaný do blockchainu. Tento proces zahŕňa problém konsenzu v sieti, ktorý je podrobne vysvetlený v sekcii 2.6.

5. Ak sa podarilo úspešne blok pridať do blockchainu tak miner získava odmenu. Odmena za vyťažený blok je konštantná čiastka zdrojov poskytovaných daným blockchainom. Napríklad Bitcon poskytuje v roku 2021 ako odmenu 6,25 bitcoinov čo približne 300 dolárov [1]. Avšak táto odmena môže byť navýšená o poplatky, ktoré sú v transakciách.

[1] https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

Ak teda chcete aby sa vaša transakcia dostala do blockchainu čo najrýchlejšie, poskytnete vyššiu odmenu v podobe poplatku za transakciu. Miner bude potom viac motivovaný pridať práve túto transakciu do bloku.

[13]

2.6 Konsenzus

Konsenzus v blockchaine zabezpečuje, že skupina uzlov (peerov) sa zhodne na rovnakom stave blockchainu. Tradične je konsenzus zabezpečený centrálnou autoritou s ktorou musia byť všetky uzly spojené. Avšak blockchain je decentralizovaný a teda toto riešenie nie je možné. Konsenzus v decentralizovanej sieti blockchainu je zabezpečený pomocou protokolu, ktorý sa snaží nájsť kompromis medzi nasledujúcimi vlastnosťami [7, 19, 10]:

- Konzistentnosť: Vždy keď dôjde k potvrdeniu zmeny, celý reťazec sa aktualizuje a všetci čítajú rovnaké hodnoty.
- Dostupnosť: Pre každú požiadavku na dáta musí byť poskytnutá odpoveď.
- Odolnosť voči prerušeniu (anglicky *partial tolerance*): Sieť funguje aj v prípade, že v nej vznikajú chyby.

Existujú tri najbežnejšie techniky, ktoré sa používajú pre ustavenie konsenzu [9]:

- **Lotéria**: Takéto protokoly náhodne zvolia uzol, ktorý vyprodukuje nový blok. Výhodou tohoto prístupu je jeho jednoduchosť keďže takýto proces nevyžaduje žiadnu interaktivitu. Nevýhodou tohoto prístupu je, že pripúšťa možnosť voľby viacerých uzlov súčasne. V takom prípade sa reťazec rozvetví (anglicky *fork*) a je potrebné určiť ktorá vetva je správna. Typicky sa za správnu vetvu volí tá najdlhšia. Avšak takéto správanie oslabuje konzistentnosť blockchainu. Transakcie v posledných blokoch môžu byť potenciálne zahodené pretože nejde o správnu vetvu. Preto sa za konzistentné transakcie považujú až tie ktoré sú prekryté väčším množstvom nových blokov.
- **Hlasovanie**: Protokoly založené na hlasovaní dosahujú dohodu pomocou hlasovania všetkých zapojených uzlov. Môžeme použiť napríklad protokol Byzantskej chyby (anglicky *Byzant fault tolerance*), ktorý vyžaduje majoritu hlasov k uzavretiu konsenzu (typicky $\frac{2}{3}$). Výhodou je veľmi malá pravdepodobnosť vzniku vetiev reťazca. Na druhej strane, takéto protokoly majú nižšiu priepustnosť, ktorá klesá z narastajúcim počtom uzlov.
- **Kombinovaný prístup**: Tieto protokoly sa snažia kombinovať prístup lotérie a hlasovania s cieľom dosiahnuť výhody oboch prístupov. Napríklad je možné rozdeliť počet uzlov podieľajúcich sa na hlasovaní pomocou lotérie, čím sa zvýši priepustnosť.

[19, 9]

2.6.1 Proof-of-Work

Dôkaz prácou (anglicky *proof of work*) je najbežnejšia stratégia konsenzus protokolu. Ak chce uzol publikovať nový blok, musí investovať svoj výpočtový výkon do riešenia netriviálneho kryptografického problému. Uzol, ktorý ako prvý vyrieši tento problém má najväčšiu

pravdepodobnosť, že bude jeho blok pridaný do reťazca. Samozrejme, je tu možnosť, že problém vyrieši súčasne viacero uzlov. Konečná voľba je teda náhodná. Proof-of-work teda umožňuje, aj keď s oveľa menšou pravdepodobnosťou, že sa reťazec rozvetví. Bezpečnosť takéhoto konsenzu spočíva v tom, že majorita výpočtového výkonu siete (51 %) je vlastnená poctivými uzlami. [10]

Samotný kryptografický problém, ktorý sa rieši spočíva v počítaní hashu (viď 2.2.1) z hlavičky nového bloku (viď 2.4.1). Hlavička obsahuje atribút nonce, ktorý môže miner ľubovolne nastaviť. Zmenou tohoto atribútu môže miner získať iný hash hlavičky bloku. Konsenzus vyžaduje aby výsledná hash hodnota bola menšia rovná určitej zvolenej hodnote. Miner môže túto podmienku dosiahnuť len tak, že bude inkrementovať hodnotu atribútu nonce až dokedy túto podmienku nesplní. Táto úloha sa teda dá riešiť len pomocou metódy útok hrubou silou (anglicky *brute force*). Miner môže svoju šancu na úspech zvýšiť len tým, že poskytne väčší výpočtový výkon do jej riešenia. Na druhej strane, ostatné uzly môžu overiť, že jeho riešenia je správne veľmi rýchlo a efektívne. [20]

Proof-of-work konsenzus využíva dva typy uzlov. Prvý typ uzla je miner, ktorý vytvára nové bloky tak ako je popísané v sekcii 2.5. Druhý typ uzla je bežný vlastník zdrojov v danom blockchaine, ktorý môže vytvárať transakcie a distribuovať ich do siete. Druhý typ uzla teda nehrá žiadnu rolu v ustanovovaní konsenzu. [10]

Proof-of-work je overený konsenzus protokol, ktorý funguje a používa sa v blockchainoch ako je Bitcoin [12] alebo Ethereum [2]. Tento protokol má však jeden dlhodobý problém a to je spotreba energie. Uzly ktoré riešia kryptografický problém pre nové bloky spotrebujú veľké množstvo energie čo má nepriaznivý dopad na životné prostredie. Niektoré zdroje [3] napríklad hovoria, že v roku 2021 pokrýva ťažba Bitcoinu 0,5 % celkovej spotreby elektrickej energie na svete. Pre porovnanie, ide o sedemkrát väčšiu spotrebu energie ako má celá spoločnosť Google. [10]

2.6.2 Proof-of-Stake

Dôkaz podielom na vlastníctve (anglicky *proof of stake*) je založený na technike lotérie, kde pravdepodobnosť výhry rastie s množstvom už vlastnených zdrojov. Základnou myšlienkou, je že vlastník veľkého množstva zdrojov v danom blockchaine je veľmi nepravdepodobným útočníkom pretože svoje zdroje nechce ohroziť. Uzly sa teda musia preukázať vlastníctvom zdrojov v danom blockchaine ak chcú publikovať nový blok. Pravdepodobnosť výberu uzlu rastie s množstvom zdrojov, ktoré v sieti vlastní. [9, 14]

Veľkou výhodou proof-of-stake oproti proof-of-work je, že nevyžduje také veľké množstvo energie. Uzly už nemusia súťažiť v riešení výpočtovo náročných úloh. [10]

[2] https://ethereum.org/en/whitepaper/
[3] https://www.businessinsider.com/bitcoin-mining-electricity-usage-more-than-google-2021-9

Kapitola 3

Viacvrstvová abstrakcia

Existuje veľké množstvo blockchain protokolov, ktoré majú rôzne využitie a implementáciu. Avšak všetky tieto implementácie sú založene na spoločnom koncepte distribuovanej účtovnej knihy. Pre ich jednotnú klasifikáciu použijeme nasledujúci model abstrakcie so štyrmi vrstvami: [9]

1. **Sieťová vrstva** predstavuje najnižšiu vrstvu abstrakcie a zaoberá sa peer-to-peer sieťou. Sieť rieši pripájanie nových peerov a komunikácia medzi uzlami v sieti (šírenie transakcií a blokov). Táto vrstva má kritický dosah na výkonnosť blockchainu. Napríklad, verejný blockchain ako je Bitcoin tvorí veľmi rozsiahlu sieť s tisíckami aktívnych uzlov. V takejto sieti sa už vlastnosti ako stratovosť paketov alebo priepustnosť nezanedbateľne prejaví na rýchlosti a stabilite celého blockchainu. [6]

2. **Konsenzus vrstva** definuje protokol pomocou, ktorého sa ustavuje dohoda na stave blockchainu. Táto vrstva kľúčovo ovplyvňuje priepustnosť transakcií (*TPS - transaction per second*). Táto metrika je kľúčová napríklad v oblasti kryptomien. Pre porovnanie, centralizovaný platobný systém VISA [1] má TPS približne 1 500 zatiaľ čo Bitcoin približne 5.

3. **Dátová vrstva** (alebo tiež úložisko) definuje model transakcií (binárny hashovací strom, hashovacie a kryptografické algoritmy).

4. **Aplikačná vrstva** definuje využitie v konkrétnej službe (napríklad kryptomena).

[1] https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44

Kapitola 4

Útoky na konsenzus

4.1 Ovládnutie konsenzu útočníkmi

Tieto útoky narušia decentralizované siete tým, že útočníci dokážu utvoriť konsenzus. V takom prípade sa stáva sieť centralizovaná, kde centrálnou autoritou sú práve útočníci. Príkladom takéhoto útoku pre proof-of-work a proof-of-stake konsenzus je ovládnutie 51 % siete. V prípade protokolov Byzantskej chyby dokáže $\frac{1}{3}$ uzlov spôsobiť, že bude protokol narušený alebo dokonca zastavený. [9]

4.2 Porušenie synchronného doručovania

Ak útočník dokáže narušiť synchrónne doručovanie správ v protokole, ktorý synchronizáciu predpokladá tak takýto protokol prestane fungovať. Tento útok už nie je možné urobiť na protokole, ktorý umožňuje asynchronnú komunikáciu. [9]

4.3 title

Kapitola 5

Porovanie simulačných nástrojov

Použiť túto prácu na porovannie [15]

Caw, keď sa mrkneš na porovnanie simulátorov ktoré mám v práci, tak si môžeš všimnúť, že niektoré z iných simulátorov sú tvorené iba pre PoW ale taktiež u väčšiny nemáš dostupný zdroják alebo je o nich dokonca len napísaná práca a ani si ich nevieš vyskúšať. Bitcoin Simulator mal už naimplementovaný prenos správ a taktiež ukladanie blokov do ledgeru, čo mi celkom vyhovovalo a len som to rozšíril o tie protokoly, no napr. chalan predo mnou sa to snažil v NS3 urobiť komplet celé aj s výmenou transakcií, ktorá v mojom simulátore chýba a simulujem tam len časovým oneskorením pri dobe prenosu veľkosť jednotlivých blokov. Dávaj bacha ale akým spôsobom robíš niektoré operácie, lebo môj simulátor bol v konečnom dôsledku dosť pomalý a na simulácie som používal 64 CPU a 150GB RAM v metacentre, kde sa mi tesne pred odovzdaním podarilo ale vyčerpať fairshare skore, čiže na doknčenie práce som musel ešte použiť kamarátov účet NS3 je ale podľa mňa celkom dosť vhodný spôsob nakoľko ti umožňuje simulovať rozsiahle siete a rôzne správanie v nich.. taktiež ak by sa ti podarilo spraviť dobrý simulátor, tak by bolo fajn ho hodiť ako public tool v NS3, čo určite ocení oponent ale aj komisia. Inak je to celkom jednoduchá téma a len to znie zložito, no určite na ňu nekašli lebo kódiť to len v posledných mesiacoch neni dobrý nápad Btw, výhoda tej témy je to, že ak máš dobre vybraté protokoly, tak niektorí profáci nevedia ako majú správne fungovať a chalan predomnou dostal A za simulátor, čo nerobil ani zďaleka to čo mal.. z 3 protokolov mal naimplementované 2 a aj tie úplne mimo (pri Algorande mu chýbalo VRF a podobne), testy bezpečnosti ani neskúsil a testy výkonu boli len také na pár riadkov, čiže reálne nesplnené zadanie ale tým, že tomu oponent nerozumel, tak si myslel, že je to spravené perfektne

5.1 BlockSim

Simulátor v pythone.

https://www.frontiersin.org/articles/10.3389/fbloc.2020.00028/full#note1

Aktuálna implementácia zameraná na PoW (naimplementovaný Bitcoin, Ethereum). Autor tvrdí, že implementácia umožnuje prirodzené rozšírenie aj o simuláciu PoS. PoS simulácia by však neumožnila analýzu špecifickej sekvencie správ PBFT konsenzu.

5.2 VIBES

Simulátor v TS a Scale.

https://github.com/i13-msrg/vibes/blob/master/docs/Master_Thesis_VIBES.pdf

Podľa autora je možná inplementácia PoS. Ide len o diplomovu pracu a teda nástroj nebude asi moc rozsiahly a kvalitný.

5.3 Shadow

Simulator siete TOR, ale niekto urobil plugin na bitcoin.

https://shadow.github.io/

5.4 Bitcoin Simulator

https://arthurgervais.github.io/Bitcoin-Simulator/index.html

Simulator primo určen na PoW Bitcoin, ale minuly rok prave toto použili na PoS simulator.

5.5 FoBSim

Simulacia blockchainu v pythone, tvrdia že sa da simulovat aj PoS. Zrejme bude problem s pravami.

https://github.com/sed-szeged/FobSim

5.6 SimBlock

SimBlock je simulátor založený na diskrétnej simulácii. Simulátor je implementovaný v programovacom jazyku Java a jeho zdrojový kód je voľne dostupný (anglicky *open source*) [1]. Simulátor podporuje proof-of-work protokoly Bitcoin, Leitecoin a Dogecoin.

Autori tohoto projektu v rámci vyhodnocovania presnosti simulátora vykonali experiment ktorý porovnal ich prácu s podobným už existujúcim simulátorom. Obe simulácie spustili s rovnakými parametrami a to pre protokoly Bitcoin, Leitecoin a Dogecoin. Výsledky oboch simulátorov boli veľmi podobné. Na základe tohoto experimentu autori zhodnotili, že ich simulátor má dobrú presnosť.

Autori ďalej navrhli úpravu algoritmu na voľbu susedných uzlov (anglicky *neighbor node selection algorithm*) v protokole Bitcoin. Navrhnutú úpravu odsimulovali a vyhodnotili, že ich vylepšenie algoritmu zvyšuje priepustnosť transakcií. Touto simuláciou bol demonštrovaný význam tohoto simulačného nástroja a to je zlepšovanie blockchainových protokolov z hľadiska výkonnosti a bezpečnosti. [3]

Open source simulator blockchainu v Jave. Klasicky zameraný na PoW (Bitcoin a Etherum je naimplementovae). Autir tvrdí, že je možná aj simulácia PoS. Dokonca by tam mala byť aj ukážka PoS implementacie [2]

https://dsg-titech.github.io/simblock/

[1] Apache License, Version 2.0

[2] https://github.com/dsg-titech/simblock/releases

Literatúra

[1] *Horizen Academy - Blockchain as a data structure* [https://academy.horizen.io/technology/expert/blockchain-as-a-data-structure/]. Accessed: 2021-06-03.

[2] Aberer, K., Alima, L., Ghodsi, A., Girdzijauskas, S., Haridi, S. et al. The Essence of P2P: A Reference Architecture for Overlay Networks. In:. Január 2005, s. 11– 20. DOI: 10.1109/P2P.2005.38. ISBN 0-7695-2376-5.

[3] Aoki, Y., Otsuki, K., Kaneko, T., Banno, R. a Shudo, K. SimBlock: A Blockchain Network Simulator. In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2019, s. 325–329. DOI: 10.1109/INFCOMW.2019.8845253.

[4] Bosamia, M. a Patel, D. Current Trends and Future Implementation Possibilities of the Merkel Tree. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING*. August 2018, zv. 6, s. 294–301. DOI: 10.26438/ijcse/v6i8.294301.

[5] Buford, J., Yu, H. a Lua, E. P2P Networking and Applications. *P2P Networking and Applications*. Január 2009. DOI: 10.1016/B978-0-12-374214-8.X0001-3.

[6] Fan, C., Ghaemi, S., Khazaei, H. a Musilek, P. Performance Evaluation of Blockchain Systems: A Systematic Survey. *IEEE Access*. 2020, zv. 8, s. 126927–126950. DOI: 10.1109/ACCESS.2020.3006078.

[7] Gilbert, S. a Lynch, N. Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-Tolerant Web Services. *SIGACT News*. New York, NY, USA: Association for Computing Machinery. jún 2002, zv. 33, č. 2, s. 51–59. DOI: 10.1145/564585.564601. ISSN 0163-5700. Dostupné z: https://doi.org/10.1145/564585.564601.

[8] Hoepman, J.-H. Distributed Double Spending Prevention. Marec 2008.

[9] Homoliak, I., Venugopalan, S., Hum, Q., Reijsbergen, D., Schumi, R. et al. The Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. Október 2019.

[10] Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A. et al. A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. *Mathematics*. 2020, zv. 8, č. 10. DOI: 10.3390/math8101782. ISSN 2227-7390. Dostupné z: https://www.mdpi.com/2227-7390/8/10/1782.

[11] Menezes, A. J. *Handbook of Applied Cryptography.* Taylor & Francis Inc, 1996. ISBN 0849385237ID.

[12] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Cryptography Mailing list at https://metzdowd.com.* Marec 2009.

[13] Narayanan, A., Bonneau, J., Felten, E., Miller, A. a Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press, 2016. ISBN 9780691171692.

[14] Nguyen, C., Dinh Thai, H., Nguyen, D., Niyato, D., Nguyen, H. et al. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access.* Jún 2019, PP, s. 1–1. DOI: 10.1109/ACCESS.2019.2925010.

[15] Paulavicius, R., Grigaitis, S. a Filatovas, E. A Systematic Review and Empirical Analysis of Blockchain Simulators. *IEEE Access.* 2021, zv. 9, s. 38010–38028.

[16] Robleh Ali, R. B. et al. *Distributed Ledger Technology: beyond block chain.* London, 1 Victoria Street, 2016.

[17] Schollmeier, R. A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications. In:. September 2001, s. 101 – 102. DOI: 10.1109/P2P.2001.990434. ISBN 0-7695-1503-7.

[18] Smart, N. *Cryptography: An Introduction.* McGraw-Hill, 2003.

[19] Zhang, S. a Lee, J.-H. Analysis of the main consensus protocols of blockchain. *ICT Express.* 2020, zv. 6, č. 2, s. 93–97. DOI: https://doi.org/10.1016/j.icte.2019.08.001. ISSN 2405-9595. Dostupné z: https://www.sciencedirect.com/science/article/pii/S240595951930164X.

[20] Zheng, Z., Xie, S., Dai, H.-N., Chen, X. a Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In:. Jún 2017. DOI: 10.1109/BigDataCongress.2017.85.