Katedra informatiky
Přírodovědecká fakulta
Univerzita Palackého v Olomouci

BAKALÁŘSKÁ PRÁCE

Kryptoměna, blockchain a Proof of Work

2025

Jan Mědílek

Vedoucí práce:
doc. RNDr. Miroslav Kolařík, Ph.D.

Studijní program: Informační technologie, prezenční forma

Bibliografické údaje

Autor:	Jan Mědílek
Název práce:	Kryptoměna, blockchain a Proof of Work
Typ práce:	bakalářská práce
Pracoviště:	Katedra informatiky, Přírodovědecká fakulta, Univerzita Palackého v Olomouci
Rok obhajoby:	2025
Studijní program:	Informační technologie, prezenční forma
Vedoucí práce:	doc. RNDr. Miroslav Kolařík, Ph.D.
Počet stran:	34
Přílohy:	elektronická data v úložišti katedry informatiky
Jazyk práce:	český

Bibliographic info

Author:	Jan Mědílek
Title:	Cryptocurrency, blockchain and Proof of Work
Thesis type:	bachelor thesis
Department:	Department of Computer Science, Faculty of Science, Palacký University Olomouc
Year of defense:	2025
Study program:	Information Technologies, full-time form
Supervisor:	doc. RNDr. Miroslav Kolařík, Ph.D.
Page count:	34
Supplements:	electronic data in the storage of department of computer science
Thesis language:	Czech

Anotace

Práce se zabývá vysvětlením základních pojmů souvisejících s kryptoměnami, technologií blockchainu a konsenzem Proof of Work. V práci je představena webová aplikace s implementací jednoduchého blockchainu, která interaktivní formou přibližuje princip jeho fungování na základě tohoto konsenzu.

Synopsis

The thesis explains basic concepts related to cryptocurrencies, blockchain technology and Proof of Work consensus. The thesis presents a web application with the implementation of a simple blockchain, which interactively presents the principle of its operation based on this consensus.

Klíčová slova: kryptoměna; blockchain; Bitcoin; Proof of Work

Keywords: cryptocurrency; blockchain; Bitcoin; Proof of Work

Chtěl bych tímto poděkovat své rodině a blízkým přátelům za podporu během celého studia. Dále bych chtěl poděkovat doc. RNDr. Miroslavu Kolaříkovi, Ph.D. za odborné vedení práce, poskytnutí odborných rad a ochotu.

Odevzdáním tohoto textu jeho autor místopřísežně prohlašuje, že celou práci včetně příloh vypracoval samostatně a za použití pouze zdrojů citovaných v textu práce a uvedených v seznamu literatury.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V posledních letech se kryptoměna stala nedílnou součástí digitálního světa a představuje nový finanční nástroj, který zásadně mění podobu trhu. Spolu s jejím rozvojem rostl i význam technologie blockchainu, kde Bitcoin byl první kryptoměnou využívající tuto technologii. Díky mechanismu blockchain je možné spravovat transakce a další data bez potřeby centrální autority.

Práce poskytuje přehled o fungování kryptoměn a technologií s nimi spojených. Kromě samotného principu kryptoměny jsou v práci rozebrány i klíčové pojmy, které jsou nezbytné pro pochopení celého systému.

Úvodní část práce je věnována vysvětlení pojmu kryptoměna, jejímu využití a fungování, přičemž popisuje i pojmy spojené s uchováváním a správou digitálních aktiv. Následně jsou prezentovány důležité kryptografické termíny, které umožňují fungování a bezpečnost blockchainu. V následující kapitole se práce zaměřuje na samotnou strukturu blockchainu a je rozebrán konsenzus Proof of Work, kde jsou vysvětleny všechny pojmy a procesy úzce související s tímto principem. Přestože je v práci kladen důraz zejména na konsenzus Proof of Work, zmíněn je zde i alternativní konsenzus Proof of Stake, který v některých kryptoměnách tento mechanismus nahrazuje. Závěrečná část popisuje implementaci jednoduché webové aplikace, která má za cíl interaktivní formou přiblížit uživateli fungování blockchainu a princip konsenzu Proof of Work.

2 Kryptoměna

2.1 Co je to kryptoměna

Kryptoměna je forma digitální měny využívající kryptografii k provádění nebo přijímání plateb pomocí *blockchain* technologie. Zásadní výhodou kryptoměny oproti tradiční, fyzické měně je její decentralizace, tedy že není řízena žádnou centrální autoritou (banka, vláda, firma apod.). Tento fakt zajišťuje kryptoměně odolnost vůči cenzuře i manipulaci jednotlivci. Pro potřeby využívání kryptoměny existuje distribuovaná síť uživatelů (takzvaných uzlů), která společně jednotlivé transakce validuje. [1]

Mezi neznámější kryptoměny patří Ethereum (ETH), Tether (USDT) a Bitcoin (BTC), podle kterého je nyní velká část kryptoměn principiálně založená.

2.2 Praktické využití kryptoměn v současnosti

V současnosti jsou kryptoměny využívány zejména k zahraničním platbám a jejich velký potenciál je spojován s možností investice. Existuje ovšem celá řada dalších způsobů využití, platba za zboží, služby nebo nemovitosti, tak jako tomu je u tradiční měny. Transakce bývají ve srovnání s tradičními bankovními převody levnější a rychlejší, a to zejména díky technologii, na níž jsou kryptoměny založeny. Výhodou je i to, že příjemcem a odesílatelem kryptoměny může být prakticky kdokoliv, kdo má přístup k internetu.

Spolu s tím je ale třeba upozornit na negativní stránku tohoto nástroje. Právě anonymita, kterou kryptoměny uživatelům poskytují, bývá zneužívána pro nelegální účely. Nejznámějším příkladem zneužití kryptoměn v tomto kontextu byl internetový černý trh Silk Road, kde se anonymně obchodovalo s drogami, zbraněmi a dalším ilegálním zbožím. [2]

2.3 Token versus mince

Mince tvoří nedílnou součást blockchainu. Fungují samostatně a nezávisle a zároveň slouží jako prostředek směny a využívají se k zaplacení transakce. Mince má několik vlastností: jsou zastupitelné, dělitelné, přenosné a jejich počet je omezený. K vytvoření mince je vždy potřeba nového blockchainu, který vyžaduje výpočetní výkon, znalosti a čas. Zástupci známých a rozšířených mincí jsou Bitcoin a Ethereum, který mají vlastní blockchain a síť.

Token je oproti minci digitálním aktivem (cokoliv, co společnost nebo jedinec vlastní a v budoucnu může přinést ekonomický prospěch) fungujícím na existující blockchainové síti. To znamená, že token nemá vlastní síť ani blockchain a využívá infrastrukturu jiné platformy. Nejčastěji jsou dnes tokeny vytvářeny na síti Ethereum pomocí chytrých smluv[1]. Tokeny vytvořené na této blockchainové

[1] Inteligentní smlouva stanoví podmínky smlouvy. Inteligentní smlouvy prováděny jako kód běžící na blockchainu, jako je Ethereum.

síti jsou známé jako ERC-20. Na rozdíl od mince je proces vytvoření tokenu jednodušší, díky už existující síti, ale i přesto poskytuje širší škálu funkcí. [3]

2.4 Peněženky

Krypto peněženky úzce spolupracují s blockchainem, uchovávají *soukromé klíče* (hesla) a *veřejné klíče* (čísla účtů), za pomoci kterých je umožněn přístup k vlastní kryptoměně. Nabízejí možnost jak přijímat, tak posílat kryptoměny a slouží k uchování pořízené kryptoměny klientem. Peněženky rozdělujeme do dvou kategorií. [4]

- Horké (hot) peněženky mají připojení k internetu nebo k zařízení, které je v danou chvíli k internetové síti připojené. Do této kategorie spadají softwarové peněženky, kdy si uživatel instaluje specifický software a má klíče pod svou kontrolou, a webové peněženky, kde klíče přímo spravuje poskytovatel služby.
- Chladné (cold) peněženky představují typ úložiště, které nemá připojení k internetu, což výrazně zvyšuje bezpečnost uložených kryptoměn. Ty se skladují na jakékoliv fyzické medium například na pevný disk, Universal Serial Bus (USB) a nebo na papír. [5]

3 Kryptografie v kryptoměně

3.1 Šifrování

Šifra je druh algoritmu, který přijímá jako vstup otevřený text spolu s klíčem a na výstupu generuje šifrovanou podobu textu. Cílem šifrování je převést nezabezpečená data z čitelné podoby na nečitelnou formu, kde zašifrovanou zprávu může přečíst jen vlastník dešifrovacího klíče. Šifra zaručuje nečitelnost zprávy nebo dat a zamezí přístupu osob a zařízení, která nejsou autorizovaná zprávu a data číst.

Šifra je lidstvu známa už od dávné historie, kde od samého počátku bylo potřeba chránit tajné informace. Postupem času se metody šifrování zdokonalovaly a přizpůsobovaly požadavkům moderní doby. Dnes existuje celá řada šifrovacích metod, které se liší složitostí, účelem a mírou zabezpečení.

Za jednu z prvních a nejjednodušších šifer můžeme považovat *Caesarovu šifru*, pojmenovaná po římském vojevůdci Juliu Caesarovi. Princip spočívá v posunu každého znaku v textu o pevně daný počet míst v abecedě. Přestože se dnes může jevit Caesarova šifra jako primitivní, v době svého vzniku představovala efektivní způsob, jak ochránit citlivé informace před nepovolanými osobami. [6, 7, 8]

Symetrická šifra je taková šifra, ve které se pro zašifrování a dešifrování používá stejný klíč. Tento algoritmus je oproti asymetrickým šifrám rychlejší a jednodušší. Často se používá pro zašifrování velkého množství dat. Klíč by neměl být z šifry zřejmý ani snadno prolomitelný, aby případný útočník nemohl klíč odhalit. Mezi nejvýznamnější symetrické šifry používané po celém světe patří *Advanced Encryption Standard (AES)*. [8, 9]

Narozdíl od symetrické šifry asymetrická šifra používá jeden klíč pro šifrování a druhý pro dešifrování, přičemž ze znalosti jednoho klíče nelze odvodit klíč druhý. V asymetrické šifře uvádíme jeden klíč soukromý a druhý veřejný. Tento algoritmus dokáže zajistit větší bezpečnost, ale také autenticitu, kdy lze identifikovat autora zprávy pomocí veřejného klíče. Hlavní výhodou tohoto algoritmu je bezpečnost. Na druhou stranu je pomalejší než symetrické šifrování z důvodu používání delších klíčů a provádění složitějších výpočtů. [8, 9, 10]

V BTC je soukromý klíč 256bitové náhodné číslo. Vytváří se softwarově pomocí bezpečného generátoru pseudonáhodných čísel například pomocí algoritmu *ISAAC*. Každý soukromý klíč by měla vlastnit pouze jedna osoba. Ta může s BTC manipulovat, díky prokázání držení soukromého klíče. Zatímco v BTC veřejný klíč je obvykle odvozen z jednoho soukromého klíče pomocí kryptografie. [11]

3.2 Nonce

V kryptografii je *nonce* („number used once“) označován jako číslo, které lze použít v šifrované komunikaci jen jednou. Obvykle jde o náhodně nebo pseudonáhodně vygenerované číslo, které se používá v autentizačních protokolech

k zajištění jejich jedinečnosti. Díky tomu nelze znovu použít staré zprávy při pokusu o útok na komunikaci. Mohou navíc obsahovat časové razítko (*timestamp*), aby bylo možné určit přesný okamžik, kdy ke komunikaci došlo.

V kontextu BTC je nonce použit u blockchainů s *konsenzem Proof of Work* v procesu těžení, který si vysvětlíme v kapitole 4.3. Hodnota bitcoinového nonce je omezená na 32bitové číslo, což znamená, že může nabývat hodnot jen do něco málo přes 4,29 miliardy. [12]

3.3 Hashovací funkce

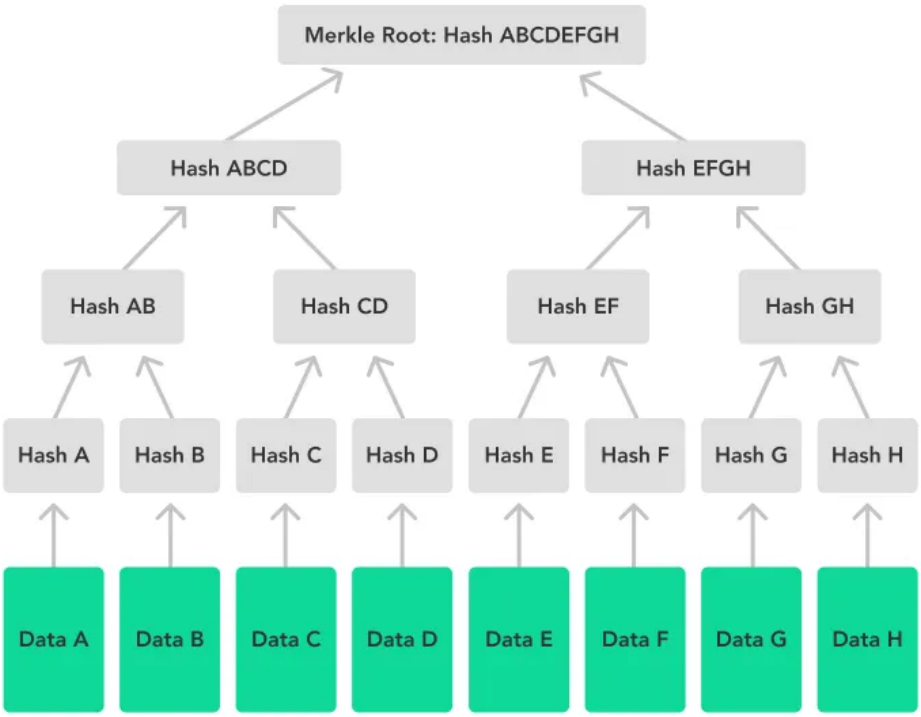
Hashovací funkce je matematická funkce, kde vstup tvoří data libovolné délky a výstupem je *hash* fixní délky. Při stejném vstupu generuje hashovací funkce vždy stejný výstup. Naopak i drobná změna vstupu způsobí výrazně odlišný výstup, což je klíčová a žádoucí vlastnost hashovacích funkcí. Z hashe nelze zpětně získat původní text zprávy, což ho odlišuje od klasického šifrování. V reálném použití je extrémně nepravděpodobné, že by dvě odlišné zprávy měly stejný hash. [8, 13]

BTC například používá hashovací funkci SHA-256, kde nezáleží na tom, jestli je vstupem jedno slovo, celá věta, stránka z knihy nebo celá kniha. Výstup bude vždy stejně dlouhý. V případě této funkce má hash přesně 256 bitů, tedy 32 bajtů. [14]

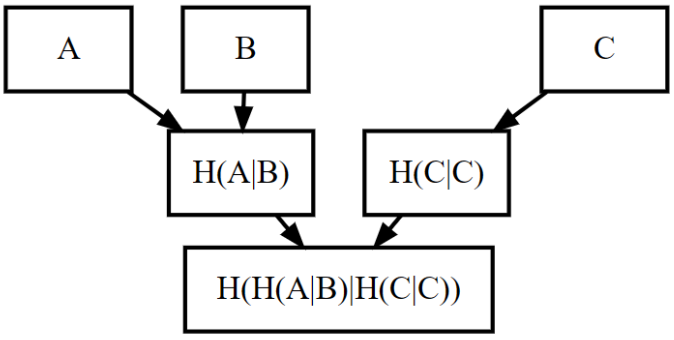
3.4 Merkleovy stromy

Hashový strom neboli Merkleův strom je datová struktura využívající hash. Jde o stromovou datovou strukturu, kde jsou data uložena v listech, zatímco v ostatních uzlech se nacházejí hashovací hodnoty vypočítané ze dvou hashů jejich přímých potomků. Kořen stromu, označovaný jako *Merkle root*, má speciální význam. Představuje výsledný hash, který vzniká postupným hashováním všech hodnot v podstromech, tedy finální hash celého stromu (viz Obrázek 1). Oproti jednodušším strukturám, jako jsou lineární seznamy hashů nebo hashové řetězce, umožňuje hashový strom ověřit integritu konkrétního listu efektivním způsobem.

Tento typ stromu využívá jak verzovací systém *Git*, tak Bitcoin, který využívá strom k ukládání transakcí. [8, 15, 16] Ideální Merkleův strom by měl mít sudý počet listů. Pokud existuje lichý počet transakcí (viz Obrázek 2), jedna transakce se zdvojí a její hash se spojí sám se sebou. [17]



Obrázek 1: Merkleův strom. Převzato z [15]



Obrázek 2: Merkleův strom s lichým počtem listů. Převzato z [17]

4 Blockchain

Blockchain je elektronická kniha záznamů, kterou sdílí a spravují počítače v decentralizované peer-to-peer síti[2]. Tato kniha se neustále rozšiřuje o bloky, které jsou její strukturou. Blockchain si lze představit jako řetěz bloků, kde každý blok odkazuje na předchozí a je identifikován hashem. Aby se nové bloky mohly přidat do blockchainu, musí se síť dohodnout, zda jsou platné. Tento proces se nazývá konsenzus a používají se mechanismy jako Proof of Work (PoW) nebo Proof of Stake (PoS). Blockchain může uchovávat různé druhy dat, přičemž nejčastěji jde o finanční transakce, jak je známe například u kryptoměn, ale také autorská práva, digitální identity a licence.

Blockchain je často přirovnáván k databázi, přičemž typická databáze je centralizovaná. Na rozdíl od blockchainu lze data v databázi často jednoduše měnit. Imutabilita[3] je právě jednou z klíčových vlastností blockchainu. Většina databází právě tuto vlastnost nedokáže implementovat. [8]

Myšlenka blockchainu se poprvé objevila v roce 1991 jako systém, který měl znemožnit falšování časových razítek dokumentů. Až v roce 2009 byl poprvé nasazen při spuštění kryptoměny Bitcoin. [18]

4.1 Blok

Blok je kontejnerová datová struktura, skládající se z hlavičky obsahující metadata a těla, ve kterém je seznam transakcí za určité časové období. Jakmile jsou tyto transakce přidány do bloku, stává se blok neměnný. Každý blok musí obsahovat specifické údaje, které umožňují jeho rozpoznání sítí, ověření správnosti a následné připojení do blockchainu. [8, 19]

Jednotlivé bloky jsou vzájemně propojené do řetězce, čímž vzniká struktura známá jako blockchain (viz Obrázek 3). Každý blok navazuje na ten předchozí, což znamená, že jakákoli změna jednoho bloku ovlivní i obsah bloku následujícího, jelikož jeho obsah zahrnuje hash předchozího bloku. [20] Hash každého bloku je propojen s hashem bloku před ním, čímž je zajištěno správné pořadí bloků. [19] Díky tomuto mechanismu je zachována integrita a bezpečnost celého blockchainu. Každá existující kryptoměna má strukturu blockchainu naimplementovanou jiným způsobem, proto si vysvětlíme strukturu Bitcoinu, který sloužil jako základ pro vznik mnoha dalších kryptoměn.

Kdybychom postupně prošli celý blockchain až po počáteční blok, narazili bychom na blok známý jako *genesis block*. Zmíněný blok neobsahuje žádný odkaz na blok předchozí a je ve většině případů vytvořen přímo v kódu softwaru dané kryptoměny. [8]

Blok Bitcoinu obsahuje hlavičku o velikosti 80 bajtů (viz Tabulka 1), počet transakcí a jednotlivé transakce. Velikost validního blok je v Bitcoinu omezena na

[2]Peer-to-peer (P2P) neboli klient-klient je typ počítačové sítě, ve které jednotliví klienti komunikují přímo mezi sebou bez potřeby prostředníka.

[3]Imutabilita je schopnost uchovávat data v neměnné podobě.

jeden megabajt [20], ale díky implementaci *Segregated Witness* (SegWit) může být velikost bloků rozšířena až na 4 megabajty, přestože v praxi se velikost bloku pohybuje kolem 2 megabajtů. Velikost určuje, že počet transakcí v jednom bloku je omezený, což může v době vyššího zatížení sítě vést ke zpomalení zpracování. Postupné zvyšování velikosti bloku by mohlo vést k větší centralizaci, protože větší bloky by byli schopni zpracovat pouze účastníci sítě s dostatečným výpočetním výkonem. [21]

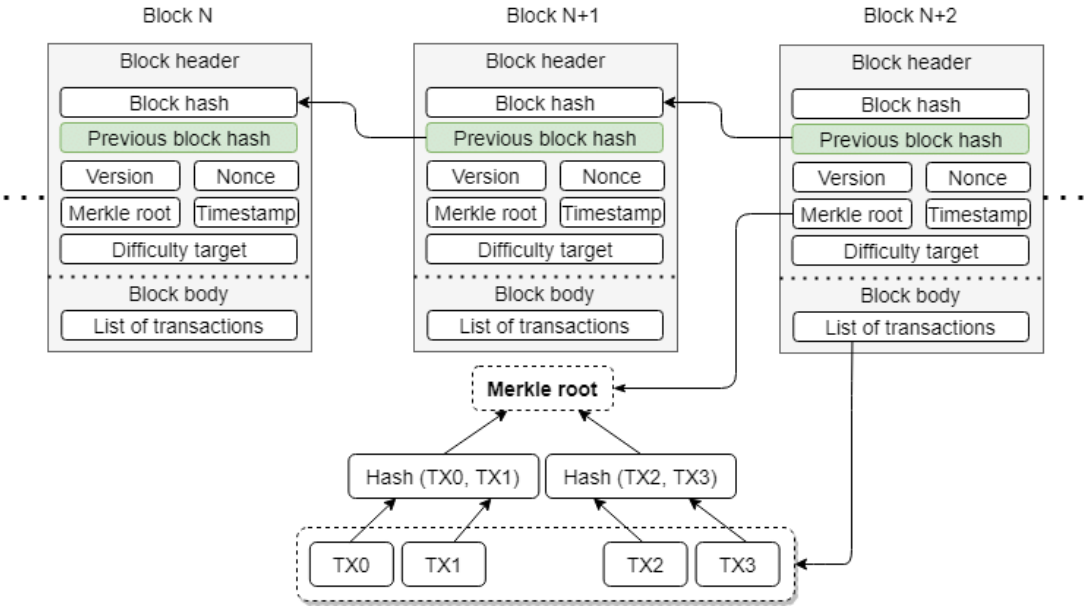
Velikost v bajtech	**Popis**	**Datový typ**
4	verze	int32_t
32	hash hlavičky předchozího bloku	char[32]
32	hash kořene stromu	char[32]
4	časové razítko	uint32_t
4	obtížnost	uint32_t
4	nonce	uint32_t

Tabulka 1: Struktura Bitcoin hlavičky bloku v blockchainu. Převzato z [17]

4.2 Transakce

Následující část textu byla převzata z [11]. Transakce převádí BTC vlastněné vstupy (*inputs*) transakce ve prospěch výstupů (*outputs*) transakce. Každý vstup transakce je tvořen dvojicí adresa a množství BTC převáděných ve prospěch této adresy. Výstup transakce, který nebyl použit jako vstup jiné transakce, se nazývá neutraceným výstupem transakce (*unspent transaction output*, Unspent Transaction Output (UTXO)). Transakce musí být podepsána majitelem soukromých klíčů všech adres, které jsou součástí transakčních vstupů. Majitelé tím vyjadřují souhlas s převodem jimi vlastněných BTC ve prospěch transakčních výstupů. Tento okamžik by u bankovní transakce odpovídal pokynu bance k vykonání transakce.

Součet BTC vlastněných vstupy této transakce zmenšený o součet BTC převáděných ve prospěch výstupů dané transakce se nazývá transakční poplatek. Výše poplatku není pevně stanovená, je nastavitelná majiteli soukromých klíčů od adres tvořících transakční vstupy. Poplatek nesmí být záporný, transakce nemůže utratit více BTC, než kolik jich bylo do transakce vloženo. Poplatek může být nulový, ale s rostoucí výší transakčního poplatku bude transakce BTC systémem zpracována dříve. Při nízké nebo nulové výši poplatku naopak hrozí možnost, že transakce nebude nikdy zpracována.



Obrázek 3: Struktura blockchainu. Převzato z [22]

4.3 Proof of Work

Jedním z nejstarších typů algoritmů pro tvorbu bloků je důkaz prací (PoW). Pro tvorbu bloku pomocí důkazu práce se používá pojem *těžba bloku* (*mining*), což je metafora odvozená od fyzické těžby zlata. Lze si pod ní představit statisíce počítačů po celém světě připojených k internetu, které mají spuštěný specializovaný software za účelem finančního zisku (kryptoměny). Ten zajišťuje ověřování transakcí a zároveň kontrolu mezi jednotlivými uzly, aby nedošlo k podvodu.

Princip PoW spočívá v hledání řešení náročného matematického problému, k jehož vyřešení je potřeba velkého množství výpočetních operací a výpočetní výkon k práci (work). Naopak ověření správnosti nalezeného řešení je relativně snadné a rychlé.

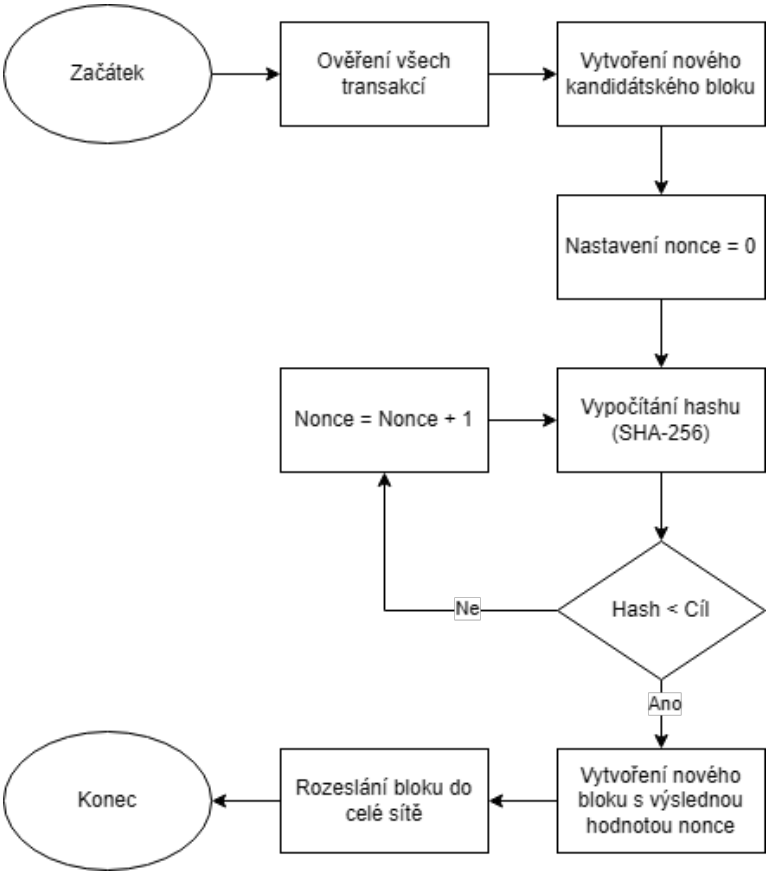
Cílem je nalézt vstup pro hashovací funkci, který splňuje určité předem dané omezení. Vzhledem k vlastnostem hashovacích funkcí neexistuje efektivnější způsob než opakované zkoušení náhodných vstupů, vypočítaní cílového hashe a kontrola, zda výstup splňuje podmínku. [8, 11, 23]

4.3.1 Těžba

Aby uzel v síti (počítač) získal odměnu, má za úkol vytvořit blok a vypočítat hash pro zmíněný blok podle zadaných podmínek. K nalezení takového hashe je třeba změnit hodnotu nonce, která se jako jediná v hlavičce může libovolně měnit. Uzel opakovaně hádá nonce a hash, dokud on sám nebo jiný uzel v síti

nenajde správné řešení. Ten je poté zaslán všem uzlům v síti a do blockchainu se připojí blok vítězného uzlu.

Tento proces probíhá v praxi následujícím způsobem. Z dostupných transakcí vytvoří uzel (počítač) kandidátský blok, jehož součástí je 80bajtová hlavička. Na tuto hlavičku je aplikována hashovací funkce SHA-256 (v Bitcoinu se tato funkce aplikuje dvakrát), čímž vznikne výsledný hash. Cílem je najít takovou hodnotu nonce, aby výsledný hash začínal určitým počtem nulových bitů, který odpovídá předem stanovené obtížnosti. Hash se porovnává s cílovou hodnotou a pokud je menší než cílová hodnota, lze blok považovat za vytěžený. V opačném případě počítač změní hodnotu nonce a celý postup opakuje, dokud nenajde správný výsledek (celý tento proces popisuje Obrázek 4). [8, 11]



Obrázek 4: Těžba nového bloku. Převzato z [24]

4.3.2 Coinbase transactions a odměna za těžbu

Každý blok v blockchainu obsahuje jednu speciální transakci nazývanou *coinbase transakce*, která na rozdíl od ostatních transakcí nemá žádné vstupy. Slouží jako odměna za úspěšné vytěžení bloku, kde výstup této transakce je adresa patřící úspěšnému tvůrci daného bloku. Tato odměna se skládá ze dvou částí: pevně dané částky za vytěžení bloku a součtu poplatků ze všech transakcí zahrnutých v bloku.

V případě Bitcoinu odměna původně činila 50 BTC. Přibližně každé čtyři roky, jakmile je vytěženo 210 000 nových bloků, dochází k události zvané *Bitcoin halving*, kdy se odměna za těžbu bloku sníží na polovinu. Aktuální odměna po posledním halvingu v dubnu 2024 činí 3,125 BTC.

Vytváření nových bitcoinů není nekonečné, jelikož celkový počet bitcoinů je omezen na 21 miliónů. Jakmile se dosáhne tohoto počtu, žádný nový Bitcoin vznikat nebude. Odměna za vytěžení bloku v podobě nových bitcoinů tedy zcela zanikne, přesto bude ale těžba nadále fungovat, jelikož těžaři budou mít motivaci pokračovat díky transakčním poplatkům.[8, 11, 25]

4.3.3 Bitcoinová síť

Bitcoinová síť je decentralizovaný systém, ve kterém je jeho stabilita, bezpečnost a funkčnost zajištěna jednotlivými uzly, které se na jejím chodu podílejí. Pomocí náhodně vybraných uzlů v síti jsou bloky přenášeny pomocí peer-to-peer sítě. Vysvětleme si několik základních pojmů v Bitcoinové síti.

Úplný uzel (*full node*) obsahuje plnou kopii blockchainu a aktualizuje se na základě informací o blocích a transakcích. Nové informace získává od svého souseda, aktualizuje svou plnou kopii blockchainu a pomocí algoritmu vlny, který zajišťuje rychlé šíření informací po síti je dále předává sousedům, kteří je dosud neobdrželi.

Úplná peněženka (*full wallet*) je typ úplného uzlu, který navíc poskytuje služby vytváření a skladování soukromých klíčů a z nich odvozených *bitcoinových adres*[4]. Umožňuje jak vytvářet, tak i podepisovat transakce.

Odlehčená peněženka (*lightweight wallet*) je alternativa úplné peněženky. Také vytváří soukromé klíče, adresy a transakce, ale nenabízí služby úplného uzlu. Uchovává si pouze hlavičku a potřebné informace o konkrétních transakcích získává od úplných uzlů. Výhodou odlehčených peněženek jsou výrazně nižší nároky na úložný prostor, které jsou v řádech desítek MB, místo více než 16 GB u peněženek úplných. Nevýhodou je závislost na sousedních uzlech, které můžou poskytovat nepravdivé informace, které si nemůže ověřit. V bitcoinové síti dnes existuje tisíckrát více odlehčených peněženek než úplných.

Samostatný těžař (*solo miner*) je typem úplného uzlu, který se narozdíl od úplného uzlu pokouší bloky vytěžit. Od ostatních uzlů přijímá transakce, kontroluje jejich správnost a skládá je do bloků, přičemž opakovaně mění hodnotu

[4]Blockchainová adresa je jedinečný identifikátor, který se používá k odesílání a přijímání kryptoměn. Adresa se odvozuje od veřejného klíče.

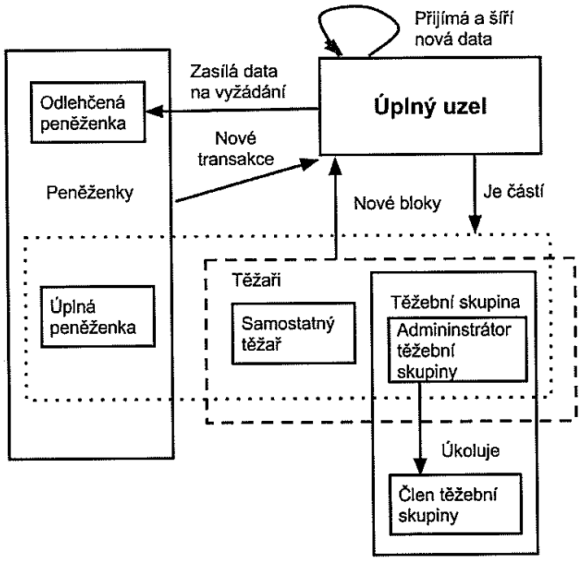
nonce ve snaze nalézt správné řešení. Při dosažení správného řešení získá odměnu prostřednictvím coinbase transakce. Vzhledem k tomu, že výpočetní výkon bitcoinové sítě neustále roste, je velmi nepravděpodobné pro samostatného těžaře vytěžit blok bez cizí pomoci.

Alternativou samostatného těžaře jsou těžební skupiny (*mining pools*), které se skládají z administrativního uzlu a z těžařských uzlů. Administrativní uzel musí provozovat úplný uzel a sestavuje nové bloky, avšak samotný proces těžby přenechává těžařům ve skupinách, kteří hledají správnou hodnotu nonce. Administrativní uzel má za úkol také sledovat, kolik výpočetního výkonu (*hashrate*[5]) jednotlivý těžaři ve skupině poskytnou.[11]

Zapojením se do mining poolu těžaři přicházejí o část své nezávislosti a odměny za vytěžení se dělí mezi mining pool a samotné těžaře. Obvykle si mining pool nastavuje poplatky ve výši 1 % až 4 % za poskytování služby mining poolu.[26]

Největším mining poolem je v současnosti *Foundry USA*, která se podílí přibližně na 30 % celkového hashratu bitcoinové sítě, přičemž její výkon dosahuje přibližně 240 EH/s[6]. Druhým největším mining poolem je *AntPool* s podílem okolo 20 %, kde se výkon pohybuje kolem 145 EH/s.[27]

Přestože se mining pooly snaží podporovat decentralizaci, koncentrace velkého množství výpočetního výkonu v několika málo skupinách způsobuje určitou formu centralizace, což odporuje původnímu principu decentralizace Bitcoinu. Foundry USA a AntPool dohromady drží více než 50 % celkového hashratu trhu, což tuto obavu dále prohlubuje. [28]



Obrázek 5: Bitcoinová síť. Převzato z [11]

[5]Hashrate udává množství hashů, které zařízení dokáže uhádnout za jednu sekundu.

[6]Jednotka EH/s (exahash za sekundu) vyjadřuje výkon 10^{18} hashovacích operací za sekundu.

4.3.4 Block time

Block time označuje průměrnou dobu potřebnou k vytěžení jednoho bloku v blockchainu. V případě BTC je průměrný block time 10 minut, které jsou klíčové pro zachování integrity sítě a umožňují těžařům ověřit transakci. Block time je úzce spjat s obtížností matematického problému, který musí těžaři vyřešit. Pokud se bloky těží příliš rychle, síť automaticky zvýší obtížnost a pokud se naopak těžba zpomaluje, obtížnost se sníží. Díky tomuto mechanismu je block time stabilní. [21]

Jedním z hlavních důvodů pro volbu desetiminutového block timu je snížení rizika *forku* a útoků typu *double-spending* (dvojí utracení). Pokud by byl interval příliš krátký, výrazně by vzrostla pravděpodobnost forku, zatímco příliš dlouhý interval by celý proces zpomalil. [29]

4.3.5 Fork

Ve většině případů potřebují softwarové systémy průběžné aktualizace a blockchainy nejsou žádnou výjimkou. Aktualizace v blockchainu mohou zahrnovat například přidání nové funkce, zavedení bezpečnostních opatření nebo řešení rozdílných názorů v komunitě. [30] Při změně protokolu blockchainu musí uzly v síti na tuto aktualizaci reagovat. Ne vždy ale všechny uzly provedou aktualizaci ve stejnou chvíli a může se stát, že část sítě validuje podle starého protokolu a část podle protokolu nového. V takovém okamžiku dochází k rozdělení sítě (*fork*).

Fork má dopad jak na uživatele, tak i na síť. Forky rozdělujeme podle rozsahu změn v protokolu na *soft fork* a *hard fork*. Soft fork je zpětně kompatibilní změna v protokolu a znamená to, že uzly s novým protokolem jsou schopny komunikovat s uzly se starším protokolem. V podstatě je soft fork méně rušivá aktualizace, která zavádí nové funkce, aniž by anulovala předchozí verze blockchainu. Soft fork se v blockchainových sítích objevuje poměrně pravidelně a zpravidla představuje drobné úpravy protokolu, jako je například změna maximální velikosti bloku. [8, 31, 32]

Hard fork na druhou stranu narušuje zpětnou kompatibilitu s předchozí verzí protokolu a dochází tu k trvalému rozdělení blockchainu, které vede ke vzniku nové kryptoměny. Důvodem jsou nová pravidla, která nejsou slučitelná s původními. Uzly mající stará pravidla nedokážou ověřovat bloky vytvořené podle nových pravidel.

Na rozdíl od soft forků jsou hard forky rizikovější, protože mohou způsobit rozvětvení sítě. Pokud všechny uzly změny nepřijmou, síť se může rozdělit na dvě samostatné větve, z nichž každá bude fungovat podle vlastní verze protokolu. Někdy je však ale hard fork nezbytný. Vzhledem k riziku se ale komunita snaží hard forkům vyhýbat. [32]

V historii Bitcoinu došlo k několika významným hard forkům, přičemž jedním z nejvýznamnějším byl hard fork v roce 2017, který vedl ke vzniku Bitcoin Cash (BCH). Cílem forku bylo zvýšit limit velikosti bloku z 1 MB na 8 MB, aby bylo možno zpracovávat více transakcí v bloku. V roce 2018 z forku BCH

vznikl Bitcoin SV (BSV), kde se zastánci BSV domnívali, že Bitcoin by měl znovu zvýšit velikost bloku, a to na 28 MB, aby umožnil ještě vyšší propustnost transakcí. Výsledkem tohoto hard forku bylo vytvoření dvou oddělených řetězců: BCH a BSV. [32]

Dalším příkladem je decentralizovaná anonymní organizace Decentralized Autonomous Organization (DAO), která se v roce 2016 stala terčem útoku na blockchain, při němž bylo odcizeno 3,6 milionu ETH. Prostřednictvím hard forku bylo možné škody napravit a blockchain se rozdělil na dvě větve: jednu, kde krádež zůstala zachována, a druhou, ve které k útoku nikdy nedošlo. [8]

4.3.6 Zastaralý blok

Zastaralý blok (*stale block*) je blok, který byl úspěšně vytěžen, ale nebyl zahrnut do aktuálně *nejdelšího řetězce*[7]. Obvykle k tomu dojde, protože jiný blok na stejné *výšce bloku*[8] byl do řetězce přidán dříve. K zastaralým blokům může dojít kvůli latenci v síti, což může způsobit dočasné rozdělení sítě na dvě větve. Těžaři řeší tuto situaci tím, že pokračují v těžbě na jedné z větví, která se následně stane nejdelší a tím pádem platnou. Druhá větev se opustí a její bloky se považují za neplatné (zastaralé).

Zastaralý blok tedy patří do větve, která už se dále nerozvíjí. Odměna za jeho vytěžení je neplatná a nelze ji utratit. Transakce z tohoto bloku se vracejí do *mempoolu*[9] a mohou být znovu vytěženy v dalších blocích.

Například pokud jeden těžař v Severní Americe a druhý v Austrálii najdou ve stejný čas blok na stejné výšce, každý z nich ho rozšíří mezi své okolní uzly. Síť pak krátce existuje ve dvou větvích. Jakmile některá větev získá další navazující blok, stane se z ní nejdelší a zbytek sítě považuje tuto větev za validní. Bitcoin má například velmi nízký počet zastaralých bloků za rok. Například v roce 2019 byly vytěženy pouze dva takové bloky, což je dosaženo nízkou latencí mezi mining pooly. [33]

4.4 Proof of Stake

Jedním z alternativních přístupů k dosažení konsenzu na rozšíření kryptoměnového systému o další blok je důkaz podílem (PoS), kde právo vytvořit nový blok mají pouze vlastníci dané kryptoměny. Tento mechanismus od roku 2022 využívá také kryptoměna ETH, která přešla z dříve používaného a energeticky náročnějšího konsenzu PoW. PoS je často zmiňován jako efektivnější, méně energeticky náročný a bezpečnější systém. PoW je však ale oproti PoS považován za ověřenější a bezpečnější metodu konsenzu.

[7] Nejdelší řetězec (*Longest chain*) je řetězec bloků, jehož vytvoření stálo nejvíce úsilí a je považován v síti za platný.

[8] Výška bloku (*block height*) označuje, kolikátý blok v pořadí se nachází v řetězci od genesis bloku.

[9] Mempool je fronta validních transakcích, které zatím nebyly přidány do bloku.

U konsenzu PoW těžaři prokazují svou účast tím, že vykonávají práci. V konsenzu PoS místo toho validátoři uzamykají určité množství ETH do chytré smlouvy, kde množství ETH slouží jako záruka a může být částečně nebo zcela odebrán, pokud se validátor zachová nepoctivě. Stejně jako těžaři v PoW, i validátoři v PoS zajišťují ověřování transakcí a vytvářejí nové bloky v rámci sítě. [8, 11]

4.4.1 Validace bloků

V konsenzu PoS nahrazuje celý proces těžby PoW staking, kde účastnici sítě (*validátoři*) zamykají záruku (*stake*), aby mohli být vybráni k ověření nových transakcí a vytvoření nového bloku do blockchainu. Výběr validátora probíhá na základě výše vsazených prostředků a doby jejich držení. Tento mechanismus upřednostňuje aktivní a dlouhodobě zapojené účastníky.

Vybraný validátor připraví návrh bloku, v němž ověří, že všechny zahrnuté transakce jsou platné (kontroluje se správnost digitálních podpisů). Následně tento blok prochází *atestačním procesem*, kterého se účastní minimálně 128 validátorů a udělují danému blok hlas (*atest*) ve prospěch jeho přijetí do blockchainu. Za úspěšné ověření a přidání bloku získává validátor odměnu (*staking*) za jeho záruku, která se skládá z poplatků validních transakcích zahrnutých v bloku.

Zapojení do stakingu vyžaduje vysoký minimální vklad (například u Ethereum 2.0 (ETH2) je to 32 ETH). Validátoři ale mohou ztratit část svého vkladu procesem zvaným *slashing*, pokud se jejich uzel dostane do offline režimu nebo pokud validují špatný blok transakcí. Tato rizika i technické nároky vedou mnoho uživatelů k využití *stakingových poolů*. [8, 34, 35]

4.5 Bezpečnost konsenzu Proof of Work a Proof of Stake

Bezpečnost konsenzuálních algoritmů, jako jsou PoW a PoS, jsou klíčová pro návrh a provoz blockchainových sítí. Oba se snaží zajistit neměnnost dat, manipulaci s transakcemi a odolat různým typům útoků. Přestože je blockchain považován za bezpečný, čelí celé řadě rizik a hrozeb, které mohou ohrozit důvěryhodnost a stabilitu sítě.

4.5.1 51% útok

Sítě založené na principu PoW a PoS jsou náchylné k takzvanému 51% útoku, ke kterému dochází, pokud útočník získá kontrolu nad 50 % hashovací síly v PoW nebo když zakoupí více něž 50 % mincí sítě PoS. Tím může ovlivňovat průběh transakcí, zamezit jejich potvrzení, pozdržet platby nebo dokonce zpětně zvrátit již provedené transakce, což by umožnilo takzvané *dvojí utrácení*[10].

Tento typ útoku na BTC je prakticky nereálný, protože by k jeho provedení bylo potřeba velké množství výpočetního výkonu. Aby jedna osoba nebo skupina

[10]Dvojí utracení (double spending) je situace, kdy je možno utratit digitální měnu vícekrát.

mohla provést útok, musela by vlastnit zařízení s výpočetním výkonem přesahujícím 304 EH/s. Takový výkon by si vyžádal extrémní investice. Nejvýkonnější těžař dnes dosahuje zhruba 406 TH/s, kde se cena tohoto výpočetního výkonu pohybuje kolem 10 000 dolarů. K dosažení potřebných 304 EH/s by bylo nutné nasadit přibližně 84 000 těchto zařízení, což činí útok velmi nepravděpodobný. [8, 36]

Pro sítě s malým hashratem toto tvrzení neplatí, kde k ovládnutí většiny výpočetního výkonu stačí menší počet prostředků. Útoku se neubránil například v roce 2018 Bitcoin Gold (BTG), který útočníkovi umožnil dvojí utracení BTG v hodnotě přibližně 18 milionů dolarů. Jedním z dalších 51% útoků byl v roce 2020 na Ethereum Classic (ETC), při kterém se útočníkovi podařilo zdvojnásobit utrácení ETC v hodnotě 5,6 milionu dolarů. [37]

4.5.2 Sybil útok

Sybil útok nastává ve chvíli, kdy uzel v peer-to-peer síti vytvoří více entit s cílem vydávat se za legitimní uživatele. Každý falešný uzel vystupuje jako běžný uživatel sítě a ostatní účastníci sítě nedokážou rozpoznat, že všechny tyto uzly patří jednomu útočníkovi. Pokud se útočníkovi podaří do sítě nasadit dostatečný počet škodlivých uzlů, může získaný vliv využít k manipulaci sítě ve svůj prospěch a rozhodovat například o přijetí nových uzlů do sítě, což může v blockchainové síti vést až k 51% útoku. Realizaci Sybil útoku je dnes velmi těžké provést z důvodu vysokého počtu nezávislých uzlů s velkou výpočetní silou. [8, 38]

5 Implementace vlastního blockchainu

V práci jsme si popsali princip kryptoměny, blockchainu a konsenzu Proof of Work. Nyní si pojďme vysvětlit jednoduchou implementaci blockchainu, která nám simuluje princip konsenzu Proof of Work a blockchainu.

Implementace je realizována jako webová aplikace v jazyce Python za použití frameworku Flask, která má za cíl interaktivně demonstrovat základní principy blockchainu a PoW. Aplikace poskytuje uživateli nástroje pro práci s blockchainem a těžbou bloků, díky kterým umožňuje lépe pochopit zmíněné technologie.

5.1 Návrh blockchainu

Základním stavebním prvkem každého blockchainu je blok, který v implementaci představuje třída `Block`. Každý blok má atributy index (pořadí v blockchainu), časové razítko (neboli timestamp), hash předchozího bloku, hodnotu nonce, seznam transakcí a výsledný hash bloku. Jednotlivé transakce představuje třída `Transaction` skládající se z odesílatele, příjemce a částkou poslanou odesílatelem.

Všechny informace v bloku se poté převedou do jednoho řetězce, na který je aplikována hashovací funkce `sha256()` z knihovny `hashlib`. Díky tomu, že každý blok obsahuje hash předchozího bloku, je zajištěna integrita a neměnnost dat uložených v blockchainu. Výsledný hash každého bloku je tedy přímo závislý na obsahu bloku předchozího.

Pro připojení bloku do blockchainu je potřeba nalézt správnou hodnotu nonce, která zajistí, že výsledný hash bude splňovat předem stanovenou obtížnost.
V rámci této implementace je obtížnost přednastavena na hodnotu tři, což znamená, že uzel, který se pokouší blok vytěžit, musí nalézt hash začínající třemi nulami.

Po nalezení správného hashe je blok přidán do blockchainu, který je v implementaci reprezentován třídou `Blockchain`. Tato třída uchovává seznam všech doposud vytěžených bloků. Zároveň při inicializaci softwarově vytváří genesis blok, kde jeho index a hodnota předchozího hashe jsou nastaveny na nulu a seznam transakcí je nastaven na prázdný seznam. V implementaci je také použita struktura mempool, která slouží jako fronta neprovedených transakcí. Před vytěžením nového bloku je z mempoolu vybráno deset transakcí, čímž je simulována omezená kapacita bloku, jak ji známe z reálných kryptoměn. Jakmile je blok plný, je potřeba ho vytěžit, aby bylo možno odeslat nové transakce.

5.2 API rozhraní

Jak již bylo zmíněno aplikace komunikuje mezi frontendovou a backendovou částí prostřednictvím REST API. Uživateli umožňuje například zpracování transakcí, těžbu bloků, správu účtů a ovládání těžebních režimů. Jednotlivé endpointy jsou navrženy jako jednoduché HTTP požadavky typu `GET` a `POST` a jsou volaný v JavaScriptu pomocí `fetch`. Každý endpoint buď vrací data nebo chybovou hlášku

(HTTP kód a popis chyby). Pomocí nástroje `curl` můžeme v příkazovém řádku operačního systému kontaktovat jednotlivé endpointy. Dosáhnout stejného výsledku lze i vložením do jakéhokoli webového prohlížeče Uniform Resource Locator (URL) s `GET` požadavkem. Oba dotazy vždy zobrazí data ve formátu JSON.

5.3 Webová aplikace

Webová aplikace poskytuje rozhraní pro interakci s blockchainem prostřednictvím HTTP požadavků na REST API. Backend aplikace je napsána v jazyce Python za využití frameworku Flask, který zajišťuje veškerou logiku spojenou s provozem blockchainu a jednotlivými funkcemi.

Frontendová část aplikace je vytvořena pomocí jazyka HTML, JavaScriptu a frameworku Bootstrap. JavaScript využívá `fetch` API k odesílání HTTP požadavků (například `POST` nebo `GET`) na jednotlivé koncové body REST API.

Aplikace je vytvořená jako interaktivní prostředí pro uživatele, proto si uživatel může zvolit mezi manuálním nebo automatickým režimem. V manuálním režimu je nejprve nutné v oblasti „Vytvořit nový účet“ založit účty, které budou odesílat nebo přijímat platby. Každému účtu je přiřazen počáteční zůstatek měny, která je v rámci simulace označena jako UPOLCOIN. Po zadání jména a zůstatku stačí stisknout tlačítko `Vytvořit`. Všechny vytvořené účty jsou zobrazeny v oblasti „Seznam účtů“, kde je uvedeno jméno vlastníka a aktuální zůstatek měny. Následně uživatel v oblasti „Přidat transakci“ ručně zadává transakci, ve které vyplní jméno odesílatele, příjemce a částku převodu. Pro zařazení transakce do mempoolu stačí stisknout tlačítko `Odeslat transakci`. Transakcí může uživatel odeslat libovolné množství. Aby mohly být transakce zpracovány, musí být zahrnuty do nového bloku. Systém proto vybere prvních deset transakcí z mempoolu a přiřadí je bloku k vytěžení. Pod touto oblastí se nachází tlačítko `Zobrazit hlavičku bloku`, které umožňuje zobrazit strukturu připraveného bloku ještě před samotnou těžbou. Tento výstup je formátu JSON. Uživatel si tak může prohlédnout jeho index, časové razítko, prvních deset transakcí v mempoolu, hash předchozího bloku a aktuální hodnotu nonce, která má hodnotu `None`, jelikož k těžbě ještě nedošlo. Níže se nachází vstupní pole, ve kterém si uživatel nastaví počet uzlů v síti. Tyto uzly jsou v rámci implementace realizovány jako samostatná vlákna, přičemž každý z nich představuje těžaře v blockchainové síti. Hodnota počtu uzlů je přednastavena na čtyři a lze změnit zadáním čísla a stisknutí tlačítka `Nastavit`. Pod formulářem pro nastavení počtu uzlů se nachází možnost změnit obtížnost těžby. Uživatel si zde může zvolit obtížnost v rozmezí od dvou do pěti, přičemž výchozí hodnota je nastavena na tři. Je důležité mít na paměti, že vyšší hodnota obtížnosti znamená delší čas potřebný k vytěžení bloku. Optimální obtížnost pro aplikaci se považují hodnoty 3 a 4. Hodnotu je doporučeno měnit jen před začátkem nebo po skončení těžby. Proces těžby lze spustit tlačítkem `Spustit manuální těžbu`, díky kterému síť uzlů začne paralelně hledat správnou hodnotu nonce, která při aplikaci hashovací funkce SHA-256 vytvoří hash začínající třemi nulami, což odpo-

vídá předem nastavené obtížnosti. Těžba je založena na náhodě a může trvat různě dlouho, někdy je správný hash nalezen během jediné sekundy, jindy až po desítkách sekund (záleží na nastavené obtížnosti). Jakmile první z uzlů nalezne validní hash, zastaví těžbu, stává se výhercem a čeká na dokončení práce zbylých uzlů. V tuto chvíli jsou vybrané transakce zpracovány a účty uživatelů se aktualizují. Vítězný uzel zároveň získává coinbase transakci ve výši 10 UPOLCOIN jako odměnu za vytěžený blok. Následně se zobrazí informace o jednotlivých uzlech: jejich hashrate, délka těžby a nalezený hash. Uživatel si stisknutím tlačítka `Zobrazit/Skrýt pokusy` může prohlédnout posledních třicet provedených pokusů o nalezení správného hashe, kde každý pokus je reprezentován dvojicí nonce a odpovídajícího hashe. Z důvodu optimalizace není zobrazován kompletní seznam všech pokusů, protože v některých případech by šlo o tisíce řádků, což by vedlo k výraznému zpomalení aplikace. V závěru si uživatel může zobrazit strukturu celého blockchainu včetně genesis bloku a právě vytěženého bloku.

Při zvolení automatického režimu je uživateli ulehčena práce, jelikož za něho většinu operací provádí samotná aplikace. Pro interakci s automatickým režimem uživatel nejprve stiskne tlačítko `Vygenerovat účty`, které vygeneruje náhodné uživatelské účty ze seznamu předdefinovaných jmen a přiřadí k nim náhodný počáteční zůstatek v rozmezí 50 až 200 UPOLCOIN. Aplikace je navržena tak, aby v jakékoli chvíli neměl žádný účet záporný zůstatek. Po vygenerování uživatelských účtů je dalším krokem vytvoření transakcí a těžba bloku. Uživatel tuto funkci spustí stisknutím tlačítka `Spustit automatickou těžbu`, díky kterému v pozadí aplikace náhodně generuje nové transakce a vkládá je do mempoolu. Jakmile je mempool naplněn, aplikace je vloží do připraveného bloku a následně zahájí těžbu. Po vytěžení bloku se zobrazí podrobné informace o všech uzlech stejně jako v manuálním režimu, aktualizuje se stav blockchainu a zůstatky uživatelských účtů. Celý tento proces je automaticky opakován, čímž je simulováno nepřetržité těžení v blockchainu, jak je to v reálném blockchainu. Těžbu lze zastavit tlačítkem `Zastavit automatickou těžbu`. Je ale možné, že uživatel zastaví těžbu právě ve chvíli, kdy už začala těžba dalšího bloku. V takovém případě se těžba zastaví až po jeho dokončení a pro zobrazení uzlů s informacemi je nutné stisknout tlačítko `Zobrazit výsledek těžby`. Toto tlačítko je tedy nutné stisknout, když uživatel zastaví simulaci, došlo k obnovení zůstatku a blockchainu, ale neaktualizovaly se těžební uzly. Počet uzlů a obtížnost těžby lze upravovat i v automatickém režimu a to buď před jeho spuštěním nebo kdykoliv po jeho zastavení. Je důležité vzít v potaz, že při delším běhu automatického režimu může dojít ke zpomalení aplikace. Je to působeno narůstající velikostí dat, které aplikace vypisuje. Je možné, že aplikace bude natolik zahlcená, že přestane odpovídat na dotazy uživatele, proto je doporučeno v takovém případě stránku ručně obnovit. Po obnovení může uživatel s daty pokračovat v práci, protože stav blockchainu a účtů zůstává zachován.

Aplikace nabízí také tlačítko `Resetovat blockchain`, které stisknutím vymaže celý blockchain a všechna data spojená s blockchainem. Nabízí také tlačítko `Vymazat všechny účty`, které po stisknutí vymaže všechny účty včetně jejich zůstatků. Uživatel si tak může vytvořit nové účty a těžit bloky znovu od začátku.

Závěr

Kryptoměna je velmi rozsáhlé téma, se kterým se budeme i v následujících letech pravděpodobně setkávat. Nabízí nejen široké možnosti využití a investic, ale zároveň mění přístup k digitálním platbám, decentralizaci a zajištění bezpečnosti dat. Díky absenci centrální autority umožňuje uživatelům svobodně spravovat svá aktiva a spoléhat se na systém s předem definovanými a neměnnými pravidly.

Práce byla zaměřena na vysvětlení klíčových principů kryptoměn, fungování blockchainu a na konsenzus Proof of Work. V teoretické části byla nejprve představena kryptoměna spolu s potřebnými kryptografickými znalostmi pro pochopení celého systému. Následně byl popsán samotný blockchain a zmíněný konsenzus, včetně principu jeho fungování a provozních mechanismů těžby v rámci sítě. Byl stručně popsán i mechanismus Proof of Stake, který je energeticky úspornější. Zmíněny byly také vybrané bezpečnostní problémy, které mohou ohrozit stabilitu a důvěryhodnost blockchainových sítí a dokazují, že i přes velikost blokchainového systému, je systém v nějakých aspektech zranitelný.

V praktické části se aplikace zaměřuje na vizualizaci blockchainového systému v interaktivní formě, kde si uživatel může vyzkoušet celou řadu funkcí. Aplikace slouží jako názorná ukázka principů uvedených v teoretické části a napomáhá porozumění jednotlivým pojmům v praxi. Do budoucna lze aplikaci rozšířit o další konsenzuální mechanismy, jako je Proof of Stake, nebo o možnost propojení uzlů do samostatně komunikující sítě. Uvedená vylepšení by ještě více přiblížila reálné fungování blockchainových systémů.

Conclusions

Cryptocurrency is a very broad topic that will accompany us in the coming years. It brings many types of use, as well as investments. It brings not only new opportunities in the field of investments, but also changes the way we approach digital payments, decentralization and data security. Thanks to the absence of central authority, it allows users to freely manage their assets and rely on a system with predefined and immutable rules.

The bachelor's thesis was focused on explaining the key principles of cryptocurrencies, the functioning of the blockchain and the Proof of Work consensus. In the theoretical part, the cryptocurrency was first introduced along with the necessary cryptographic knowledge to understand the entire system. After that, the blockchain and the previously discussed consensus mechanism were explained, including how it works and how mining operates within the network. Although Proof of Work is historically the first consensus algorithm, the Proof of Stake mechanism, which is more energy efficient, was also briefly described. Selected security issues that can threaten the stability and credibility of blockchain networks were also mentioned and prove that despite the size of the blockchain system, the system is vulnerable in some aspects.

In the practical part, the application was focused on visualizing the blockchain system in an interactive form, where the user can try out a variety of functions. The application serves as an illustrative example of the principles presented in the theoretical part and helps to understand individual concepts in practice. In the future, the application can be expanded to support other consensus algorithms, such as Proof of Stake, or to include the possibility of connecting nodes into a separately communicating network. These improvements would bring the real functioning of blockchain systems even closer.

A Obsah elektronických dat

Na samotném konci textu práce je uveden stručný popis obsahu elektronických dat odevzdaných v systému katedry informatiky spolu s textem. Tato data jsou nedílnou součástí práce a tvoří (datovou) přílohu textu práce.

`text/`
: Adresář s textem práce ve formátu PDF, vytvořený s použitím závazného stylu KI PřF UP v Olomouci pro závěrečné práce, včetně všech (textových) příloh, a všechny soubory potřebné pro bezproblémové vytvoření PDF dokumentu textu (případně v ZIP archivu), tj. zdrojový text textu a příloh, vložené obrázky, apod.

`README.txt`
: Textový soubor s postupem pro instalaci, spuštění a ovládání aplikace.

`aplikace.zip/`
: Zip soubor obsahující všechny soubory a složky potřebné ke spuštění aplikace.

U veškerých cizích obsažených materiálů jejich zahrnutí dovolují podmínky pro jejich veřejné šíření nebo přiložený souhlas držitele práv k užití. Pro všechny použité (a citované) materiály, u kterých toto není splněno a nejsou tak obsaženy, je uveden jejich zdroj, např. webová adresa, v bibliografii nebo textu práce nebo souboru `README.*`.

Seznam zkratek

AES Advanced Encryption Standard

BCH Bitcoin Cash

BSV Bitcoin SV

BTC Bitcoin

BTG Bitcoin Gold

DAO Decentralized Autonomous Organization

ETC Ethereum Classic

ETH Ethereum

ETH2 Ethereum 2.0

PoS Proof of Stake

PoW Proof of Work

URL Uniform Resource Locator

USB Universal Serial Bus

USDT Tether

UTXO Unspent Transaction Output

Literatura

[1] Staff, Coursera (comp.). *How Does Cryptocurrency Work? A Beginner's Guide* [online]. 2025 [cit. 2025-4-4]. Dostupný z: ⟨https://www.coursera.org/articles/how-does-cryptocurrency-work⟩.

[2] Encyclopaedia Britannica, The Editors of (ed.). *Silk Road* [online]. 2025 [cit. 2025-4-7]. Dostupný z: ⟨https://www.britannica.com/technology/dark-web⟩.

[3] Coinbase. *What is the difference between a coin and a token?* [online]. [cit. 2025-4-9]. Dostupný z: ⟨https://www.coinbase.com/learn/crypto-basics/what-is-the-difference-between-a-coin-and-a-token⟩.

[4] Amure, Tobi Opeyemi. *Hot Wallet vs. Cold Wallet: What's the Difference?* [online]. 2024 [cit. 2025-4-14]. Dostupný z: ⟨https://www.investopedia.com/hot-wallet-vs-cold-wallet-7098461⟩.

[5] *What is a wallet and how do I get one?* [online]. [cit. 2025-4-14]. Dostupný z: ⟨https://www.bitpanda.com/academy/en/lessons/what-is-a-wallet-and-how-do-i-get-one/⟩.

[6] Dráb, Martin (ed.). *Lekce 1 - Úvod do šifrování a blokové šifry* [online]. [cit. 2025-4-16]. Dostupný z: ⟨https://www.itnetwork.cz/algoritmy/kryptografie/uvod-do-sifrovani-a-blokove-sifry⟩.

[7] Janko, David (ed.). *Lekce 2 - Symetrická a asymetrická kryptografie* [online]. [cit. 2025-4-16]. Dostupný z: ⟨https://www.itnetwork.cz/bezpecnost/symetricka-a-asymetricka-kryptografie⟩.

[8] ČEVELA, Jan. *Kryptoměny [online]*. 2024. SUPERVISOR: RNDr. Eduard Bartl, Ph.D. Dostupný také z: ⟨https://theses.cz/id/49y9nd/⟩.

[9] Academy, Binance. *Symmetric vs. Asymmetric Encryption* [online]. 2022 [cit. 2025-4-16]. Dostupný z: ⟨https://academy.binance.com/en/articles/symmetric-vs-asymmetric-encryption⟩.

[10] Paganová, Alžběta (ed.). *Co je kryptografie s veřejným klíčem?* [online]. 2019 [cit. 2025-4-16]. Dostupný z: ⟨https://www.ssl.com/cs/Nej%C4%8Dast%C4%9Bj%C5%A1%C3%AD-dotazy/co-je-kryptografie-s-ve%C5%99ejn%C3%BDm-kl%C3%AD%C4%8Dem/⟩.

[11] Lánský, Jan. *Kryptoměny*. First. Praha: C.H. Beck, 2018. xvi, 144 s. S. ISBN 978-80-7400-722-4.

[12] Team, The Investopedia (comp.). *Nonce: What It Means and How It's Used in Blockchain* [online]. 2024 [cit. 2025-4-17]. Dostupný z: ⟨https://www.investopedia.com/terms/n/nonce.asp⟩.

[13] SSL, Tým podpory (ed.). *Co je kryptografická funkce hash?* [online]. 2024 [cit. 2025-4-17]. Dostupný z: ⟨https://www.ssl.com/cs/%C4%8Dl%C3%A1nek/co-je-kryptografick%C3%A1-hashovac%C3%AD-funkce/⟩.

[14] Rhodes, Delton (ed.). *SHA-256 Cryptographic Hash Algorithm* [online]. 2025 [cit. 2025-4-17]. Dostupný z: ⟨https://komodoplatform.com/en/academy/sha-256-algorithm/⟩.

[15] Kumar, Rajeev (ed.). *Understanding Merkle Trees: The Backbone of Data Verification* [online]. 2023 [cit. 2025-4-18]. Dostupný z: ⟨https://medium.com/@rajeevprasanna/understanding-merkle-trees-the-backbone-of-data-verification-13b39af26fff⟩.

[16] Academy, Binance (ed.). *Merkle Tree* [online]. [cit. 2025-4-18]. Dostupný z: ⟨https://academy.binance.com/en/glossary/merkle-tree⟩.

[17] Developer, Bitcoin (ed.). *Block Chain* [online]. [cit. 2025-4-18]. Dostupný z: ⟨https://developer.bitcoin.org/reference/block_chain.html⟩.

[18] Hayes, Adam (comp.). *Blockchain Facts: What Is It, How It Works, and How It Can Be Used* [online]. 2025 [cit. 2025-4-14]. Dostupný z: ⟨https://www.investopedia.com/terms/b/blockchain.asp⟩.

[19] Gratton, Peter (comp.). *What Is a Block in the Crypto Blockchain, and How Does It Work?* [online]. [cit. 2025-4-15]. Dostupný z: ⟨https://www.investopedia.com/terms/b/block-bitcoin-block.asp⟩.

[20] *Block Chain*. [online]. [cit. 2025-4-15]. Dostupný z: ⟨https://developer.bitcoin.org/devguide/block_chain.html⟩.

[21] Coinbase. *Bitcoin block reward, block size, block time: what's the difference?* [online]. [cit. 2025-4-15]. Dostupný z: ⟨https://www.coinbase.com/learn/crypto-basics/bitcoin-block-reward-block-size-block-time-whats-the-difference⟩.

[22] Iqbal, Mubashar; Matulevičius, Raimundas. Exploring Sybil and Double-Spending Risks in Blockchain Systems. *IEEE Access*. 2021, roč. PP, s. 2. Dostupný také z: ⟨https://www.researchgate.net/publication/351730117_Exploring_Sybil_and_Double-Spending_Risks_in_Blockchain_Systems⟩.

[23] Nevil, Scott (comp.). *What Is Proof of Work (PoW) in Blockchain?* [online]. 2024 [cit. 2025-4-18]. Dostupný z: ⟨https://www.investopedia.com/terms/p/proof-work.asp⟩.

[24] Clouder, Alibaba (ed.). *Comprehensive Review of Proof-of-Work Consensus in Blockchain* [online]. 2020 [cit. 2025-4-22]. Dostupný z: ⟨https://www.alibabacloud.com/blog/comprehensive-review-of-proof-of-work-consensus-in-blockchain_597042⟩.

[25] Niklaus, Paul (ed.). *Bitcoin Halving Explained: What Investors Need to Know [2025]* [online]. 2025 [cit. 2025-4-22]. Dostupný z: ⟨https://www.blockpit.io/en-us/blog/bitcoin-halving⟩.

[26] Khaliq, Wijdan (ed.). *6 Best Bitcoin Mining Pools of 2025: A Comprehensive Guide* [online]. 2024 [cit. 2025-4-28]. Dostupný z: ⟨https://coinbureau.com/analysis/best-bitcoin-mining-pools/⟩.

[27] Index, HashRate (ed.). *Bitcoin Mining Pools Comparison* [online]. [cit. 2025-4-28]. Dostupný z: ⟨https://hashrateindex.com/hashrate/pools⟩.

[28] Team, Lightspark (ed.). *Bitcoin Mining Pools in 2025: How They Work Top Pools by Hashrate - Lightspark* [online]. 2025 [cit. 2025-4-28]. Dostupný z: ⟨https://www.lightspark.com/blog/bitcoin/bitcoin-mining-pools-explained-a-beginners-guide⟩.

[29] LABS, NADCAP (ed.). *Why Does Bitcoin Have a 10-Minute Block Time?* [online]. [cit. 2025-4-28]. Dostupný z: ⟨https://www.nadcab.com/blog/block-time-in-bitcoin⟩.

[30] Coinbase (ed.). *What is a fork?* [online]. [cit. 2025-4-29]. Dostupný z: ⟨https://www.coinbase.com/learn/crypto-basics/what-is-a-fork⟩.

[31] Coinbase (ed.). *What is the difference between a blockchain soft fork and a hard fork?* [online]. [cit. 2025-4-29]. Dostupný z: ⟨https://www.coinbase.com/learn/crypto-glossary/what-is-the-difference-between-a-blockchain-soft-fork-and-a-hard-fork⟩.

[32] River (ed.). *What Are Bitcoin Forks?* [online]. [cit. 2025-4-29]. Dostupný z: ⟨https://river.com/learn/what-are-bitcoin-forks/⟩.

[33] CoinMarketCap (ed.). *Stale Block* [online]. [cit. 2025-4-30]. Dostupný z: ⟨https://coinmarketcap.com/academy/glossary/stale-block⟩.

[34] Team, The Investopedia (comp.). *What Does Proof-of-Stake (PoS) Mean in Crypto?* [online]. 2024 [cit. 2025-5-2]. Dostupný z: ⟨https://www.investopedia.com/terms/p/proof-stake-pos.asp⟩.

[35] Coinbase (ed.). *What is "proof of work" or "proof of stake"?* [online]. [cit. 2025-5-2]. Dostupný z: ⟨https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake⟩.

[36] Team, The Investopedia (comp.). *51% Attack: Definition, Who Is At Risk, Example, and Cost* [online]. 2024 [cit. 2025-5-3]. Dostupný z: ⟨https://www.investopedia.com/terms/1/51-attack.asp⟩.

[37] Hacken; Bartosz, Barwikowski (ed.). *51% Attack: The Concept, Risks Prevention* [online]. 2024 [cit. 2025-5-3]. Dostupný z: ⟨https://hacken.io/discover/51-percent-attack/⟩.

[38] Thales company, Immperva a (ed.). *Sybil Attack* [online]. [cit. 2025-5-3]. Dostupný z: ⟨https://www.imperva.com/learn/application-security/sybil-attack/⟩.