Ekonomická fakulta
Faculty of Economics

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích

Ekonomická fakulta

Katedra aplikované informatiky a matematiky

Diplomová práce

Komparativní hodnocení mechanismů konsensu v kryptoměnách

Vypracoval: Bc. Tadeáš Pekárek

Vedoucí práce: doc. Ing. Ladislav Beránek, CSc., MBA

České Budějovice 2023

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Ekonomická fakulta
Akademický rok: 2020/2021

Studijní program: Aplikovaná informatika
Forma studia: Prezenční
Specializace/kombinace: Podniková informatika (AIP)

Podklad pro zadání DIPLOMOVÉ práce studenta

Jméno a příjmení:	**Bc. Tadeáš PEKÁREK**
Osobní číslo:	**E20400**
Adresa:	Švandy Dudáka 689, Strakonice – Strakonice I, 38601 Strakonice 1, Česká republika
Téma práce:	Komparativní hodnocení mechanismů konsensu v kryptoměnách
Téma práce anglicky:	Comparative evaluation of consensus mechanisms in cryptocurrencies
Vedoucí práce:	doc. Ing. Ladislav Beránek, CSc., MBA ***Katedra aplikované matematiky a informatiky

Zásady pro vypracování:

Kryptoměny (např. bitcoin) umožňuje subjektům v síti peer-to-peer dosáhnout shody o stavu blockchainu pomocí sady kryptografických algoritmů a ekonomických pobídek. Bitcoin používá systém vynaložené práce (proof of work), ale existují i jiné konsensuální mechanismy používané jinými kryptoměnami. Výkon kryptoměny závisí na použitém mechanismu konsensu. Cílem práce je provést komparativní hodnocení různých významných mechanismech konsensu u různých kruptoměn. Budou popsány výhody a nevýhody každého mechanismu spolu s jejich aplikacemi. Bude provedena klasifikace do hlavních typů, tyto typy hodnoceny. Závěr bude tvořen diskuzí o otevřených výzvách souvisejících s dostupnými řešeními.
Metodický postup:

- Analyzovat technologie blockchainu a mechanismů konsensu na základě literární rešerše.
- Popis dalších vybraných souvisejících technologií, např. Exonum, Neo.
- Návrh scénaře testování, komparativní analýza a hodnocení mechanismů konsensu
- Zhodnocení, vypracování doporučení a závěrů.

Seznam doporučené literatury:

NARAYANAN, A. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. 1. Princeton: Princeton University Press, 2016. ISBN 978-0691171692.
KENT, P. *Cryptocurrency Mining For Dummies*. 1. Chichester: John Wiley & Sons For Dummies, 2019. ISBN 978-1119579298.
SATOSHI, Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. In: *Bitcoin* [online]. 2008 [cit. 2021-02-28]. Dostupné z: https://bitcoin.org/bitcoin.pdf
WOOD, Gavin. *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER* [online]. In: . [cit. 2021-02-28]. Dostupné z: https://ethereum.github.io/yellowpaper/paper.pdf
TASCA, Paolo. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. In: *LEDGER Journal* [online]. Pittsburgh: University of Pittsburgh, 2019, 2019 [cit. 2021-02-28]. Dostupné z: https://ledgerjournal.org/ojs/ledger/article/view/140
ANTONOPOULOS, Andreas. *Mastering Bitcoin: Programming the Open Blockchain*. 2.vyd. Sebastopol, Kalifornie: O'Reilly Media, 2017. ISBN 978-1491954386.
ANTONOPOULOS, Andreas a Gavin WOOD. *Mastering Ethereum: Building Smart Contracts and DApps*. Sebastopol, Kalifornie: O'Reilly Media, 2018. ISBN 978--1491971949.

Prohlášení

Prohlašuji, že svou diplomovou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury. Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne

Podpis studenta

Poděkování

Tímto bych rád poděkoval vedoucímu své diplomové práce panu doc. Ing. Ladislavu Beránkovi Csc., MBA za jeho rady a připomínky.

Obsah

1 Úvod

Počátkem 21. století přišla na svět technologie, která by mohla radikálně změnit způsob, jakým naše společnost funguje. Blockchain, distribuovaná účetní kniha, kterou využívají kryptoměny, jako je Bitcoin, nabízí potenciál pro decentralizované, transparentní a bezpečné transakční systémy. Nicméně s tímto příslibem přichází i řada technických výzev včetně otázek týkajících se bezpečnosti, škálovatelnosti a energetické účinnosti.

Jedním z klíčových aspektů blockchainových technologií je mechanismus konsensu, metoda, kterou systém používá k ověřování a zaznamenávání transakcí v účetní knize. Existuje celá řada různých konsensních mechanismů, každý s vlastními výhodami a nevýhodami, výběr vhodného mechanismu může mít zásadní dopad na výkonnost a bezpečnost celého systému.

Tato diplomová práce se zaměřuje na komparativní hodnocení různých mechanismů konsensu využívaných v kryptoměnách. Prvotně se práce zabývá popisem samotné technologie distribuované účetní knihy, poté podrobným zkoumáním a popisem různých vybraných konsensních mechanismů rozdělených do několika skupin.

Další část práce se zabývá podrobnou analýzou a komparativním hodnocením v teoretické části popsaných konsensních mechanismů se zaměřením na bezpečnostní rizika, otázky centralizace, energetickou náročnost a dopad na životní prostředí, škálovatelnost, výkonnost a ekonomická rizika. Toto hodnocení zahrnuje vybraná kritéria hodnocení, zranitelnost proti kybernetickým útokům, bodové a vážené hodnocení a přehled výhod a nevýhod jednotlivých mechanismů.

V rámci hodnocení jsou rovněž zkoumány dostupné simulátory konsensních mechanismů jako je BlockSim a TangleSimulator, které jsou využity k testování různých mechanismů v navržených scénářích.

Závěr práce tvoří sada metodologických návrhů testovacích scénářů konsensních mechanismů a doporučení pro možné budoucí implementace a vývoj v této oblasti.

1.1 Cíle práce

Cílem této diplomové práce je provést komparativní hodnocení různých mechanismů konsensu využívaných v kryptoměnách. Tyto mechanismy jsou klíčové pro dosažení shody o stavu distribuované účetní knihy v decentralizovaných peer-to-peer sítích.

Cíle práce jsou následující:

Literární rešerše technologie distribuované účetní knihy a konsensních mechanismů:
Poskytnout detailní porozumění o fungování těchto technologií a jak ovlivňují a charakterizují kryptoměny. V této části budou dále detailně popsány a zmapovány vybrané konsensní mechanismy rozdělené do vlastních kategorií.

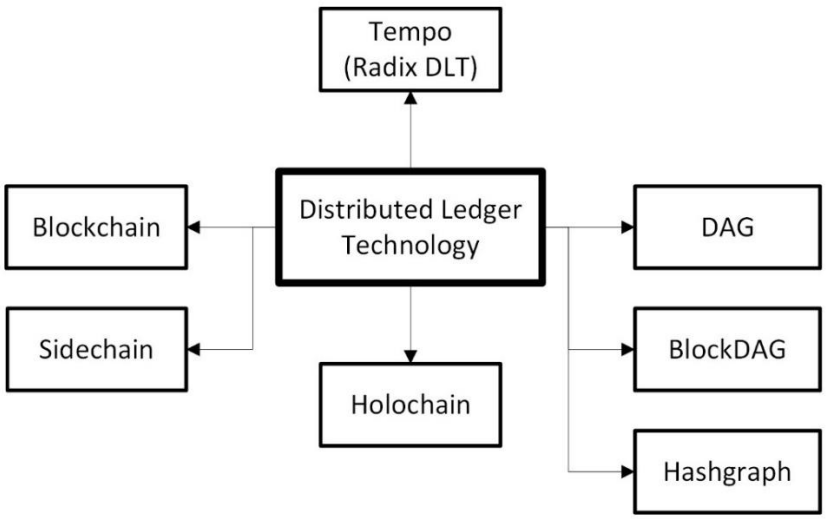
Popis a analýza vybraných souvisejících technologií:
V kontextu konsensních mechanismů je dalším z cílů analyzovat související technologie (kryptoměny), které dané mechanismy implementují.

Analýza a komparativní hodnocení mechanismů konsensu:
Provést srovnávací analýzu a hodnocení konsensních mechanismů dle zvolených kritérií, popsat výhody a nevýhody jednotlivých mechanismů a rizika, která s mechanismy souvisí.

Metodický návrh sady testovacích scénářů:
Na základě předchozích bodů je cílem navrhnout sadu testovacích scénářů konsensních mechanismů a některé z nich se pokusit otestovat pomocí dostupných nástrojů pro simulaci konsensních mechanismů.

2 Technologie distribuované účetní knihy

Technologie distribuované účetní knihy (Distributed Ledger Technology, DLT) je ve své podstatě vysoce dostupnou digitální databází sdílenou v nedůvěryhodném prostředí, která na rozdíl od tradičních databází není spravována a distribuována žádnou centrální autoritou, ale jednotlivými uzly sítě. K distribuci dat dochází peer-to-peer (klient-klient) a každý uzel si udržuje aktuální kopii účetní knihy lokálně. Nedůvěryhodné prostředí je charakteristické náhodnými výskyty byzantských chyb (nedostupné uzly, škodlivé chování uzlů, zpoždění sítě). Data se do účetní knihy přenášejí transakcemi, které obsahují adresy odesílatele a příjemce, částku, transakční poplatek, časové razítko, digitální podpis a další údaje nebo data (metadata, programový kód, chytré smlouvy) v závislosti na konkrétním případu použití. Validaci transakcí probíhá sítě základě digitálních podpisů. Vzhledem k absenci centrální autority je nutné se dohodnout na pořadí transakcí a dosáhnout konzistentního stavu účetní knihy, k tomu slouží konsensní mechanismy, bez kterých by celý tento systém nemohl fungovat. Mechanismy konsensu zajišťují, že do účetní knihy budou přidány pouze platné transakce, jež se stanou součástí trvalého záznamu a stejná transakce nebude přidána více než jedenkrát (double-spending problem). V závislosti na požadavcích a konkrétních případech užití mohou být k dosažení shody použity různé mechanismy, které jsou v této práci zmapovány a popsány. [1] [2]



Obrázek 1 – Přehled Distributed Ledger Technology (vlastní zpracování)

2.1 Blockchain

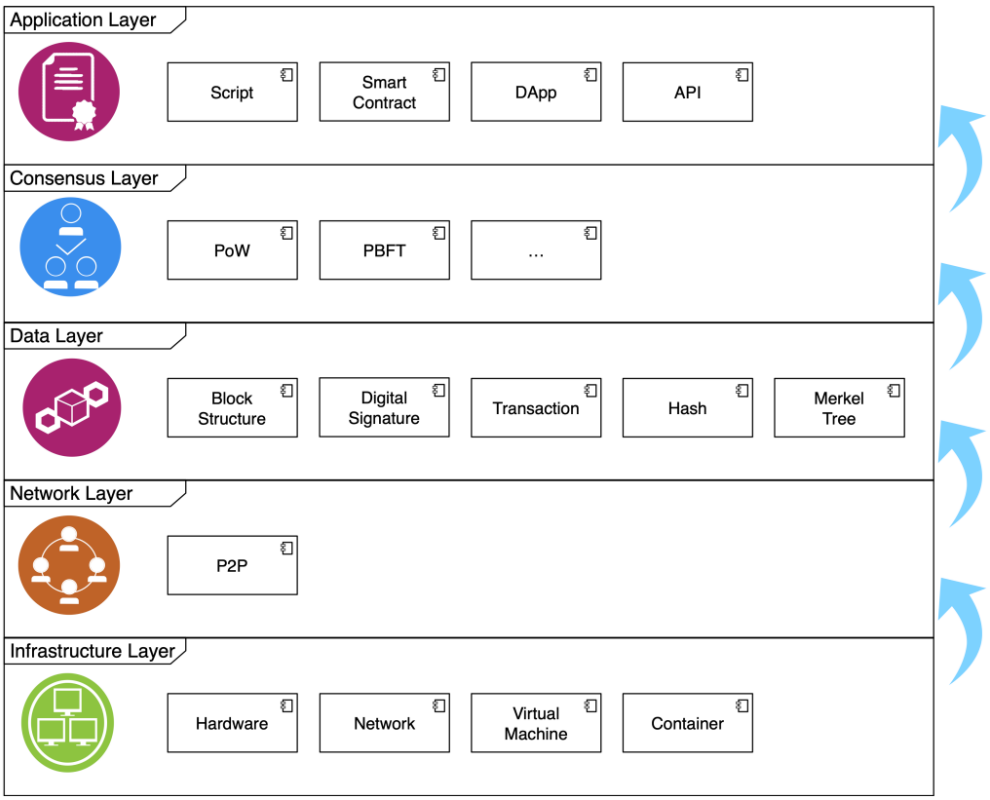
Blockchain je nejrozšířenějším typem distribuované účetní knihy, a to hlavně ve světě kryptoměn. Jedná se o distribuovanou a decentralizovanou databázovou strukturou spolehlivě uchovávající transakční záznamy, které je nemožné nebo velmi obtížné jakýmkoliv způsobem zpětně měnit nebo s nimi manipulovat. Název blockchain (v překladu „řetěz bloků“) vychází ze způsobu ukládání dat do bloků. Transakce v blocích jsou uchovávány v datové struktuře Merkle tree a kromě časového razítka obsahuje každý blok ještě hash toho předchozího, čímž je dosaženo vzájemného lineárního propojení. Distribuce dat probíhá peer-to-peer, uzly mezi sebou komunikují a lokálně uchovávají kopii blockchainu v aktuálním stavu, čímž vytváří redundanci a udržují věrohodnost. K interakci mezi uzly sítě dochází za pomoci kryptografie, transakce je uzlem digitálně podepsána a vysílána do sítě, kde na základě digitálního podpisu (asymetrická kryptografie) dochází k její validaci (ověření vlastnictví) ostatními uzly před zařazením do bloku, tímto způsobem je zajištěno, že se sítí budou šířit pouze validní transakce. Vzhledem k absenci centrální autority je nutné dojít mezi uzly ke konsensu o stavu blockchainu, toto zajišťují implementované konsensní mechanismy deklarující způsob dosažení shody, které jsou předpokladem funkčnosti celého systému. [3]


```
{
    "hash" : "0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4",
    "confirmations" : 35561,
    "size" : 218629,
    "height" : 277316,
    "version" : 2,
    "merkleroot" : "c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e",
    "tx" : [
        "d5ada064c6417ca25c4308bd158c34b77e1c0eca2a73cda16c737e7424afba2f",
        "b268b45c59b39d7596147577l8b9918caf0ba9d97c56f3b91956ff877c503fbe",

        ... 417 more transactions ...

      ],
    "time" : 1388185914,
    "nonce" : 924591752,
    "bits" : "1903a30c",
    "difficulty" : 1180923195.25802612,
    "chainwork" : "0000000000000000000000000000000000000000000000934695e92aaf53afa1a",
    "previousblockhash" : "000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569"
}
```


Obrázek 2 – Struktura bloku v blockchainu Bitcoinu [3]

Kromě decentralizace patří mezi další zásadní funkce blockchainu integrita dat, která je zajištěna kryptografickými funkcemi, zejména hashování a digitální podepisování, které umožňuje ověřit autenticitu a nedotknutelnost dat. Žádnou transakci ani blok nelze zpětně pozměnit, data jsou odolná vůči manipulaci, to s sebou přináší i vysokou míru zabezpečení. I když je fakt, že transakce v blockchainu jsou ireverzibilní a nelze je zpětně změnit, existují způsoby, jak s nimi pracovat, například prostřednictvím chytrých smluv, které umožňují definovat podmínky a situace, za kterých se transakce vrátí nebo zruší. Decentralizace a kryptografie dává uživatelům sítě větší svobodu a kontrolu nad digitálními aktivy a také poskytuje jistou míru anonymity.

Významnou výzvou blockchainu pro jeho další rozvoj a využití je škálovatelnost, protože se s narůstajícím počtem transakcí a uzlů zvyšuje i náročnost na síťovou kapacitu a efektivitu. S ohledem na asymetrickou kryptografii patří k nevýhodám ztráta privátního klíče, který není možné žádným způsobem dopočítat z veřejného zpět, to vede k nenávratné ztrátě přístupu k digitálním aktivům. [4] [5]



Obrázek 3 - Blockchain architektura [6]

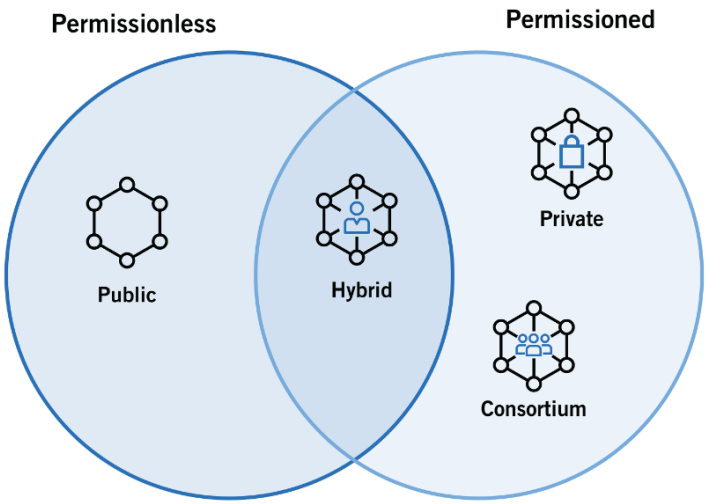
Klasifikace typů blockchainu

Rozdělení blockchainu lze provést na základě dvou kritérií (obr. 4). Prvním kritériem je oprávnění, které určuje, kdo má právo k blockchainu přistupovat a kdo se smí účastnit konsensu. Podle tohoto kritéria se blockchainy dělí na dvě kategorie:

- bez povolení (permissionless)
- s povolením (permissioned)

Druhým kritériem pro rozdělení blockchainu je na základě jeho typu, který určuje, jakým způsobem jsou v blockchainu data ukládána a zpracovávána. Podle tohoto kritéria se blockchainy dále rozdělují na:

- veřejné (public)
- privátní (private)
- konsorciální (consortium)
- hybridní (hybrid)



Obrázek 4 – Rozdělení blockchainu [7]

Blockchainy dle oprávnění

Blockchainy bez povolení (permissionless) jsou decentralizované a otevřené, to znamená, že účastník pro připojení do sítě nepotřebuje žádat žádnou autoritu o povolení, každý uživatel smí svévolně bez omezení přistupovat k informacím, realizovat transakce a účastnit se procesu konsensu.

Na druhé straně blockchainy s povolením (permissioned) jsou jistým opakem, nad sítí běží autorizační vrstva, která rozhoduje o tom, kdo se smí do sítě připojit a jaká získá práva.

Oba typy blockchainu mají své výhody, nevýhody a účely použití. Blockchainy bez povolení nabízejí na úkor výkonnosti a efektivity větší míru anonymity a decentralizace. Naproti tomu blockchainy s povolením jsou rychlejší a více škálovatelné, ale také více centralizované a méně transparentní. [7] [8]

Veřejný blockchain

Do sítě veřejného blockchainu se může bez povolení připojit každý s přístupem k internetu a stát se plnohodnotným uživatelem (uzlem) sítě, validovat bloky nebo realizovat transakce. Veřejný blockchain nemá omezení, je plně autonomní, necenzurovatelný a transparentní, každý má přístup ke všem transakčním záznamům. Vzhledem k tomu, že značná část veřejných blockchainů využívá k dosažení shody v sítí konsensuální algoritmus Proof of Work, je hlavní nevýhodou nízká energetická účinnost a také je v porovnání s ostatními typy pomalejší, nicméně nabízí úplnou decentralizaci a vysokou míru zabezpečení. Je také nutné zmínit, že veřejný blockchain nabízí nikoliv anonymitu, ale pouze pseudonymitu, to znamená, že v případě propojení konkrétní adresy na blockchainu s fyzickou osobou přestává být aktivita v síti kvůli transparentnosti záznamů anonymní. Veřejné blockchainy také nabízejí kromě přenosu aktiv možnost využití takzvaných chytrých smluv (smart contracts), což jsou smlouvy napsané jako programový kód, které se automaticky plní po splnění určitých podmínek. Tento koncept rovněž umožňuje vytváření různých decentralizovaných aplikací (dApps) právě na základě chytrých smluv.

Nejznámějším představitelem veřejného blockchainu je úplně první kryptoměna Bitcoin publikovaná v roce 2009 anonymní osobou (či osobami) pod pseudonymem Satoshi Nakamoto. Mezi další příklady veřejného blockchainu patří Ethereum, Litecoin a další. [9] [10]

Privátní blockchain

Do sítě privátního blockchainu se na rozdíl od veřejného smí připojit pouze autorizovaní uživatelé a síť je většinou řízena soukromou organizací, která ji plně kontroluje. Jedná se o částečně decentralizovaný až spíše centralizovaný blockchain s povolením, kde se jednotlivé uzly musí řídit nastavenými pravidly, a ne každý má

možnost auditovat všechny transakční záznamy. Tento typ blockchainu je vhodný pro podniková řešení vzhledem k nízké energetické náročnosti, vysokému standardu soukromí v rámci organizace (ochrana citlivých dat, transakcí), rychlosti transakcí, nízkým poplatkům a vysoké efektivitě. Privátní blockchainy jsou navrženy tak, aby plnily specifickou funkci. Vzhledem k tomu, že se jedná o typ blockchainu s povolením, využívají se zde jednodušší konsensní mechanismy jako je například Proof of Authority, kde je konsensu dosahováno důvěrou v určitou autoritu, nicméně tyto typy mechanismů jsou méně bezpečné a zranitelné vůči potencionálním útokům. [9] [11]

Konsorciální blockchain

Konsorciální blockchain je svojí podstatou velmi podobný privátnímu s tím rozdílem, že vliv nemá pouze jedna organizace, ale celá skupina subjektů, čímž se blockchain stává oproti privátnímu více decentralizovaným. Z každé skupiny je vybrán uzel, který má oprávnění číst a zapisovat transakce, povolovat nebo omezovat ostatní účastníky, ovšem nemůže sám přidávat bloky. K přidání bloku může dojít až po shodě všech nebo alespoň většiny vybraných uzlů. Pokud nedojde ke shodě minimálního počtu stanovených uzlů, blok nebude přidán, tímto je zajištěno, že žádný uzel nemůže zneužit svého vyššího postavení v síti. Tento mechanismus dosažení konsensu využívaný v konsorciálních blockchainech se nazývá Proof of Vote neboli hlasovací konsensus. Konsorciální blockchain je výbornou technologií pro společnosti na podnikové úrovni, kde je potřeba při zpracování dat nebo podnikových procesů spolupráce několika subjektů. [12] [13]

Hybridní blockchain

Hybridní blockchain je kombinací těch nejlepších funkcí privátního a veřejného blockchainu, není přístupný pro všechny (kontrolovaný přístup), nicméně stále nabízí transparentnost, integritu, bezpečnost i soukromí. Architektura je přizpůsobitelná a většinou se liší v závislosti na případu užití, jakmile účastníci získají přistup, mohou se zapojit do všech aktivit sítě, rozhodovat jaké transakce budou zveřejněny, nebo kdo se na síti bude podílet. Identita účastníků sítě je soukromá. [14]

Vlastnosti	Veřejný	Privátní	Konsorciální	Hybridní
Přístup	Bez povolení	S povolením	S povolením	S povolením
Vlastnictví	Decentralizované – veřejné	Centralizované – jedna organizace	Částečně centralizované – více organizací	Částečně centralizované – uživatelé s přístupem
Účast na konsensu	Kdokoliv	Autorizované uzly v rámci jedné organizace	Autorizované uzly v rámci více organizací	Kdokoliv s přístupem
Transparentnost	Úplná	V rámci organizace	V rámci organizací	Dle nastavených pravidel
Rychlost transakcí	Nízká	Vysoká	Vysoká	Vysoká
Transakční poplatek	Vysoký	Nízký	Nízký	Nízký
Škálovatelnost	Nízká	Vysoká	Vysoká	Vysoká
Efektivnost	Nízká	Vysoká	Vysoká	Vysoká
Neměnnost	Ano	Částečná	Částečná	Ano
Příklad využití	Bitcoin	Hyperledger	Quorum	XinFin

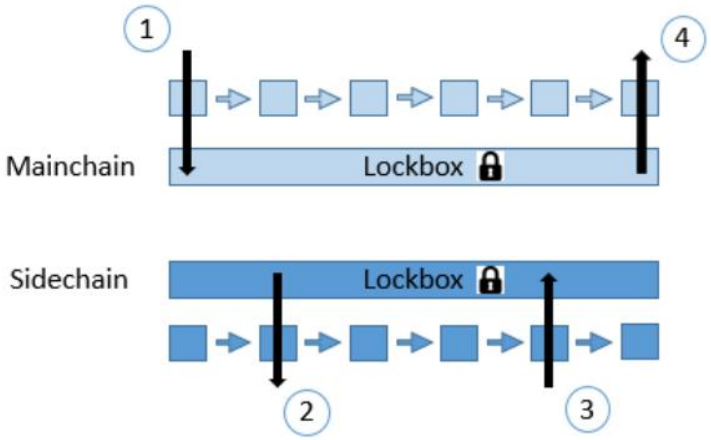
Tabulka 1 – Porovnání jednotlivých typů blockchainu (vlastní zpracování)

2.2 Sidechain

Sidechain je samostatná vedlejší blockchainová síť napojená na hlavní blockchain (mainchain) pomocí takzvaného dvousměrného mostu (two-way peg, 2WP), z kterého může dědit vlastnosti, ale konsensní mechanismus má svůj vlastní. Oba blockchainy mají logický lockbox umožňující jejich propojení. Obousměrný přenos aktiv mezi nimi funguje následovně (obr. 5): aktivum jsou uzamčeno v mainchain lockboxu a hodnotový ekvivalent je uvolněn na sidechainu. Poté je aktivum k dispozici v rámci sidechainu s vlastními pravidly a charakteristikami, nicméně mainchain je stále zdroj pravdy. Přenos aktiv ze sidechainu na mainchain funguje na stejném principu.

Sidechain umožňuje využít potenciál blockchainu v oblastech, kde by jeho použití bylo obtížné. Lze jej například využít v případě vytvoření speciálního tokenu s odlišnými vlastnostmi od kryptoměny mainchainu nebo zpracování vysokého počtu mikrotransakcí. Výhodou je, že prováděné operace v rámci sidechainu nemají vliv na mainchain. Sidechain je také využít jako experimentální platformu pro vývoj a testování

nových technologií nebo jej napojit na další sidechain, a to vše bez jakéhokoliv zásahu do mainchainu. Naopak nevýhodou je vzhledem k nižšímu počtu účastníků konsensu zranitelnost k potencionálnímu útoku na síť a nižší míra decentralizace. [15] [16]

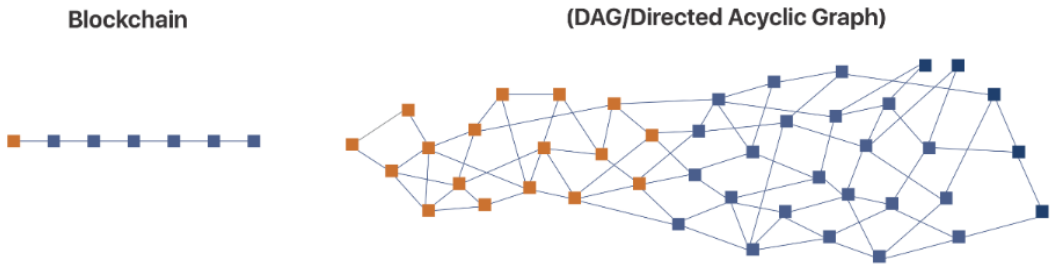


Obrázek 5 – Two-way peg – oboustranný přenos aktiv mezi mainchainem a sidechainem [16]

2.3 DAG

DAG (Directed Acyclic Graph) je technologií distribuované účetní knihy, která vznikla jako alternativa k blockchainu, nicméně od jeho architektury se zásadně liší (obr. 6). DAG je technologie založená na acyklickém orientovaném grafu, který umožňuje zaznamenávat a ověřovat transakce, z matematického hlediska jsou vrcholy propojené hranami v jednosměrném acyklickém grafu, kde vrcholy reprezentují jednotlivé transakce a hrany vazby mezi nimi. Oproti blockchainu, kde bloky na sebe odkazují lineárně, může být jedna transakce v DAG struktuře spojena s více předchozími transakcemi, které jsou navzájem provázány, to znamená, že DAG není omezen na lineární uspořádání záznamů. To umožňuje větší flexibilitu, zrychlení procesu ověřování transakcí, a hlavně masivní škálovatelnost. Každá nová transakce musí být podepsána soukromým klíčem odesílatele a po odeslání do sítě dochází k jejímu ověření ostatními uzly, ty zkontrolují, zda se nejedná o konfliktní transakci (dvě transakce skládající se ze stejného vstupu). V případě výskytu konfliktní transakce musí uzly na základě konsensu rozhodnout o tom, která z nich bude platná a začleněná do grafu.

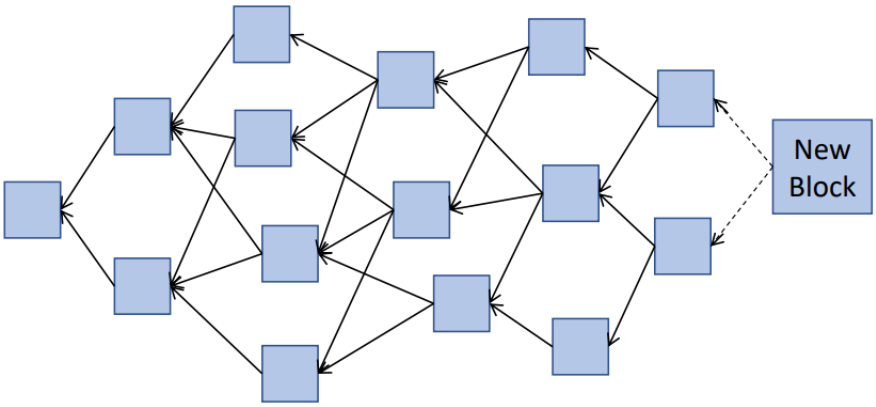
V DAG může ověřování transakcí fungovat paralelně a nezávisle na sobě, což umožňuje vysokou propustnost s extrémně nízkými transakčními poplatky, které blockchain nemůže konkurovat, ovšem stejně jako blockchain i DAG má své slabé stránky, a to zejména v tom, že se jedná o poměrně novou technologii a v porovnání s blockchainem je stále pozadu z hlediska decentralizace a bezpečnosti. V případě nízkého počtu transakcí v síti se rychlost ověřování rapidně snižuje, což s sebou přináší významná bezpečnostní rizika. [17] [18]



Obrázek 6 – Blockchain vs DAG [19]

2.4 BlockDAG

BlockDAG (Block Directed Acyclic Graph) je specifickou hybridní implementací DAG a blockchainu a jedná se spíše o rámcem než samostatným řešením. Transakce jsou uspořádány v blocích, které jsou v DAG struktuře reprezentovány vrcholy grafu a mohou odkazovat na více předchozích, čímž vzniká problém v podobě vysoké míry osiřelých bloků, a tím pádem konfliktních transakcí (double-spending problem). Pokud by se v síti objevily osiřelé bloky mohlo by to vést k rozštěpení sítě a vzniku nekonzistentních stavů. Pro zachování konzistence je potřeba jednotlivé bloky systematicky řadit, k čemuž slouží různé mechanismy a řadící protokoly, jako jsou například GHOST nebo PHANTOM, které tento problém eliminují, to umožňuje potvrzovací časy v nižších sekundách a velkou transakční propustnost. [20] [21] [22]



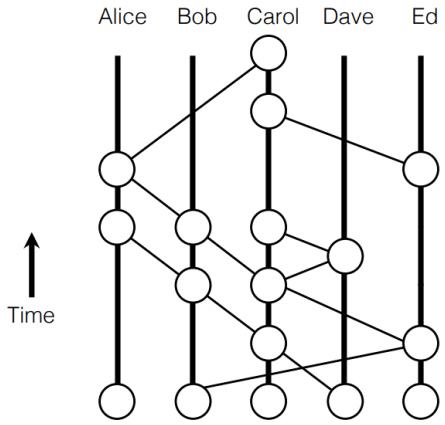
Obrázek 7 – BlockDAG [23]

2.5 Hashgraph

Hashgraph je distribuovaná účetní kniha založená na principu grafu událostí (DAG), kde každá událost má své časové razítko a odkazuje na všechny předchozí události, které k ní vedou. Ke konsensu dochází jiným způsobem než u předchozích DLT. Hashgraph není jeden řetězec, všechny informace jsou zašifrovány v účetní knize a ověřování transakcí se účastní každý uzel. Rychlý přenos informací v síti zajišťují gossip protokoly, díky čemuž každý uzel v síti ví to, co všichni ostatní, proto není zapotřebí ověřování za pomoci výpočetního výkonu, síť využívá algoritmy a automatizaci k udržování aktuálního stavu účetní knihy. Pokud se tedy v síti objeví nová transakce, každý uzel šíří událost (informace o nové transakci v síti) náhodně se sousedními uzly, po krátkém čase má informaci o dané transakci celá síť. Do účetní knihy je transakce přidána mechanismem virtuálního hlasování, kdy jednotlivé uzly sítě transakci ověří. Hashgraph mechanismus konsensus je postaven na asynchronní byzantské toleranci chyb (Asynchronous Byzantine Fault Tolerance, ABFT), který je v porovnání s jinými mechanismy více efektivní a rychlejší, shody je dosaženo bez nutnosti těžby a mechanismus je schopen tolerovat až 1/3 zlomyslných uzlů, kteří se proces pokusí narušit.

Mezi největší výhody tohoto řešení patří zejména vysoký výkon, efektivita, propustnost, škálovatelnost, férovost a zabezpečení. Hashgraph dokáže zpracovat statisíce transakcí za vteřinu s minimálními náklady a požadavky na výpočetní výkon, ovšem nejedná se o open-source technologii, vývojáři nemají možnost vytvářet své

vlastní verze, vyvstává tedy otázka, jak moc je celý tento systém decentralizovaný. [24] [25] [26]



Obrázek 8 – Gossip graf historie komunikace [26]

2.6 Holochain

Holochain se od předchozích DLT zásadně liší, jedná se o open-source rámec sloužící jako peer-to-peer síťový protokol pro širokou škálu decentralizovaných aplikací (dApps), kde se nenachází žádný prostředník (server), místo toho aplikace běží přímo na uživatelských zařízení, každý uživatel má lokálně uloženou její kopii a podílí se tak na hostingu. Každá aplikace má svá vlastní ověřovací pravidla, která definují, jak mají vypadat validní data. Všichni uživatelé mají stejné pravomoci a povinnost, díky čemuž aplikace funguje bezpečně i bez prostředníka. Tyto pravidla se chovají jako „DNA“, umožňují uživatelům fungovat jako organismus. Holochain nedisponuje žádným globálním konsensem, hlavní komponentou systému je uživatel sítě, který si zapisuje změny do svého vlastního stavu v jasném pořadí událostí. Změny jsou publikovány do takzvané distribuované hashovací tabulky (Distributed Hash Table, DHT), což je ve své podstatě sdílená databáze pro všechny uživatele dané aplikace, kteří pomocí kryptografie data ověřují, ukládají a distribuují jejich kopii. V případě detekování škodlivého chování je uzel ostatními izolován.

Holochain nabízí lepší přenos a ukládání dat, dokonce i zařízení jako chytré telefony mohou být součástí sítě, což umožňuje masivní škálovatelnost. Z hlediska spotřeby elektrické energie je Holochain oproti tradičnímu blockchainu energeticky

účinný, jelikož neprovádí žádné náročné výpočetní operace. Výhodou je také vysoká míra konfigurovatelnosti, každá aplikace může využívat jiné protokoly. Holochain je svými unikátními vlastnostmi vhodným řešením pro decentralizované aplikace, které využívá vysoký počet uživatelů – kolaborativní aplikace, sociální sítě, peer-to-peer platformy a podobně. [27] [28] [29]

2.7 Tempo (Radix DLT)

Tempo je distribuovaná účetní kniha, za kterou stojí společnost Radix DLT. Tempo umožňuje zaznamenávat transakce s časovými razítky v daném pořadí s primárním zaměřením na horizontální škálování neboli schopnost efektivně zvládat vysoký nárůst uživatelů sítě. Tempo se skládá z několika částí, jako jsou instance účetní knihy univerza, shardy, logické hodiny a hashgraph komunikační protokol. Univerzum je celkový prostor, ve kterém se jednotlivé události (transakce) nazývají atomy. Tento prostor se skládá z mnoha samostatných shardů distribuovaných v síti, které obsahují atomy v určitém časovém období. Konsensu Tempo dosahuje pomocí digitálních podpisů a časových razítek, takzvaných logických hodin (Lamport‘s logical clock), kdy každý uzel v síti má své „počítadlo“ (logické hodiny), které se zvyšuje s každou jím validovanou událostí. Události jsou uzlem dále šířeny po připojení hodnoty jeho logických hodin, takto postupují všechny uzly sítě, výsledkem je poté sada hodnot logických hodin (časový důkaz) a uspořádaný záznam událostí. Komunikace a šíření událostí je stejně jako u Hashgraphu dosaženo pomocí gossip protokolu. Časové důkazy jsou velmi důležité v případě konfliktních událostí. Pokud se taková událost objeví, uzel shromáždí časové důkazy týkající se dané události od jiných uzlů a rozhodne, která událost je validní, ostatní uzly dojdou stejným způsobem k totožnému závěru, čímž je dosaženo konsensu. Pro případ, že by nějaký uzel chtěl podvádět, se ke každému časovému důkazu připojuje digitální podpis jako takzvaný závazek (kryptografický hash), ten pomáhá poctivým uzlům k odhalení možného podvodu.

Tempo DLT lze využít jak pro veřejná, tak i privátní řešení (dApps, tokeny, transakce apod.), nevyžaduje žádný extrémní výpočetní výkon a dokáže plnohodnotně fungovat i na chytrém telefonu. Díky využití technologie shardingu a komunikačního gossip protokolu je možné rychle a efektivně zpracovávat vysoké množství transakcí,

nicméně stále zde hrozí centralizační riziko v případě, že významné množství uzlů sítě ovládá jedna organizace nebo skupina. [30] [31] [32] [33] [34]

3 Konsensní mechanismy

Konsensní mechanismy se používají v distribuovaných systémech k dosažení shody o stavu mezi jednotlivými uzly sítě. Zajišťují, že ke shodě dojde i v případě selhání či škodlivého chování části uzlů a jsou přímo odpovědny za udržování integrity a bezpečnosti celého systému. Konsensu je dosaženo řadou kroků, které se liší v závislosti na použitém algoritmu.

Výběr správného mechanismu konsensu je bezpochyby nejdůležitější složkou každé distribuované účetní knihy, protože určuje, jak budou transakce ověřovány, zaznamenávány a zabezpečeny. Je odpovědný za to, aby síť dosáhla shody o pořadí a platnosti transakcí. Různé mechanismy mají různé kompromisy, pokud jde o faktory jako je například výkon, bezpečnost, škálovatelnost, decentralizace a energetická účinnost. Výběr mechanismu závisí na specifických cílech a požadavcích na síť a hraje klíčovou roli v kontextu kryptoměn.

Je důležité poznamenat, že existuje velké množství principiálně stejných konsensních mechanismů, jejichž pravidla a postupy se mohou v různých projektech lišit v závislosti na požadavcích či případu užití.

V této kapitole jsou vybrané a popsané konsensní algoritmy s úspěšnou reálnou implementací, které jsou rozřazeny do následujících kategorií (tab. 2):

Algoritmy založené na důkazech		
Konsensní mechanismus	**Zkratka**	**Rok uvedení**
Tradiční algoritmy založené na důkazech a jejich odvozené varianty		
Proof of Work	PoW	2009
Delayed Proof of Work	DPoW	2016
Proof of Stake	PoS	2012
Delegated Proof of Stake	DPoS	2014
Leased Proof of Stake	LPoS	2017
Secure Proof of Stake	SPoS	2019
Proof of Importance	PoI	2015
Proof of Capacity	PoC	2014
Proof of Space-Time	PoST	2016
Proof of Retrievability	PoR	2007
Alternativní algoritmy založené na důkazech		
Proof of Burn	PoB	2012
Proof of Activity	PoAc	2013
Proof of Elapsed Time	PoET	2016
Proof of Authority	PoAu	2017
Fault Tolerance algoritmy		
Byzantine Fault Tolerance		
Practical Byzantine Fault Tolerance	PBFT	1999

Delegated Byzantine Fault Tolerance	DBFT	2014
Asynchronous Byzantine Fault Tolerance	ABFT	2018
Federated Byzantine Agreement – Stellar Consensus Protocol	FBA/SCP	2015
Crash Fault Tolerance		
Paxos	Paxos	1998
Fast Paxos	FPaxos	2005
Raft	Raft	2014
DAG algoritmy		
Tangle	Tangle	2018

Tabulka 2 – Přehled konsensních mechanismů

3.1 Tradiční algoritmy založené na důkazech a jejich odvozené varianty

Algoritmy založené na důkazech jsou obecně třídou konsensních mechanismů, v nichž účastníci prokazují, že k dosažení konsensu a vynaložili nějaké zdroje. Tyto důkazy mohou mít mnoho podob, ale vždy slouží k tomu, aby prokázaly, že účastník konsensu svojí investicí přispěl k dosažení shody, a tím zabezpečení sítě.

Tato kapitola má za cíl popsat vybrané tradiční algoritmy založené na důkazech a jejich odvozené varianty uvedené v podkapitolách. Mezi tři hlavní typy algoritmů a jejich varianty patří Proof of Work, který od účastníků za účelem dosažení konsensu vyžaduje provádět náročné výpočetní operace, Proof of Stake, kde účastníci drží a vsází určité množství nativní kryptoměny a Proof of Capacity, jehož účastníci musí prokázat investici do sítě v podobě úložného prostoru.

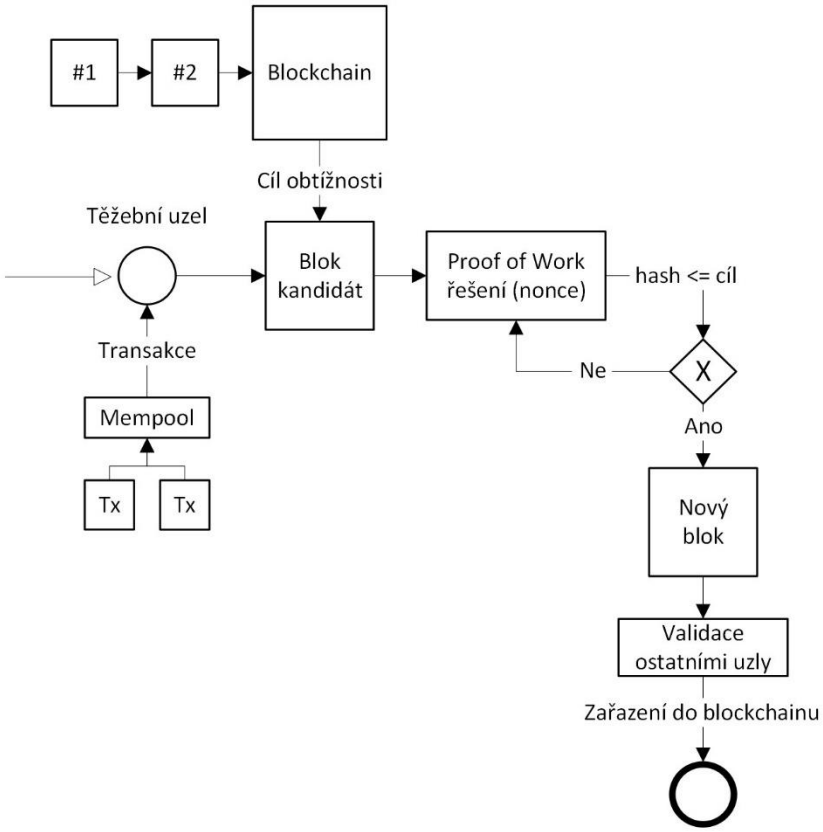
3.1.1 Proof of Work

Proof of Work (PoW) je jedním z nejrozšířenějších konsensních mechanismů, který se využívá v kryptoměnách. Tento mechanismus využívá značného množství výpočetního výkonu k nalezení matematického řešení, tzv. „hádanky“, která je poté zpětně velmi jednoduchá ke kontrole. Původně byl tento mechanismus navržen v roce 1993 jako anti-DoS a anti-spam systém. V roce 2009 se stal masivně populárním díky

první kryptoměně Bitcoin, jehož konsensní mechanismus je postavený právě na Proof of Work anti-DoS a anti-spam systému Hashcash Adama Backa z roku 1997.

V síti využívající PoW konsensus uzly soutěží mezi sebou o to, kdo z nich získá právo přidat nový blok (obr. 9). Tyto uzly se nazývají těžaři a jejich úkolem je najít pomocí hashovací funkce hlavičku bloku, jejíž velikost bude vyhovovat obtížnostnímu cíli sítě (target). Těžaři nejdříve sestaví svého kandidáta na blok, který obsahuje transakce čekající na zahrnutí do bloku (mempool) v Merkle tree struktuře, hash předchozího bloku a další náležitosti, jako je například čas a obtížnost. Kandidát na blok dále obsahuje pole zvané nonce („number only used once“) sloužící právě těžařům, kteří toto číselné pole upravují a hashují hlavičku bloku, dokud nenajdou správné řešení vyhovující dané obtížnosti sítě. Kdo nalezne správnou hodnotu nonce jako první, rozešle řešení ostatním uzlům, kteří ho jednoduše zpětně ověří a vítězný uzel získá právo přidat blok, čímž potvrdí všechny vybrané transakce a získá předem stanovenou odměnu včetně všech transakčních poplatků. Odměna slouží jako motivace uzlů využít svůj výpočetní výkon k zabezpečení sítě.

Proof of Work je mechanismus, který poskytuje vysokou úroveň zabezpečení sítě tím, že vyžaduje vysokou úroveň výpočetního výkonu. K provedení útoku na PoW je nutné ovládat nadpoloviční většinu veškerého výpočetního výkonu sítě (tzv. 51 % Attack), což je pro většinou nákladná záležitost, proto se z ekonomického hlediska spíše vyplatí investovat do zabezpečení sítě než snaze jí poškodit. Nevýhodou PoW je vysoká spotřeba elektrické energie a náklady na speciální těžební hardware (ASIC miner). Například v roce 2021 spotřeba elektrické energie pro těžbu Bitcoinu činila zhruba 107 TWh, což je v porovnání s 85 TWh České republiky vysoké číslo. Kromě toho jsou transakce v PoW síti pomalé a nákladné v porovnání s většinou ostatních konsensních mechanismů. [3] [35] [36] [37] [38]



Obrázek 9 – Proof of Work flowchart (vlastní zpracování)

3.1.1.1 Delayed Proof of Work

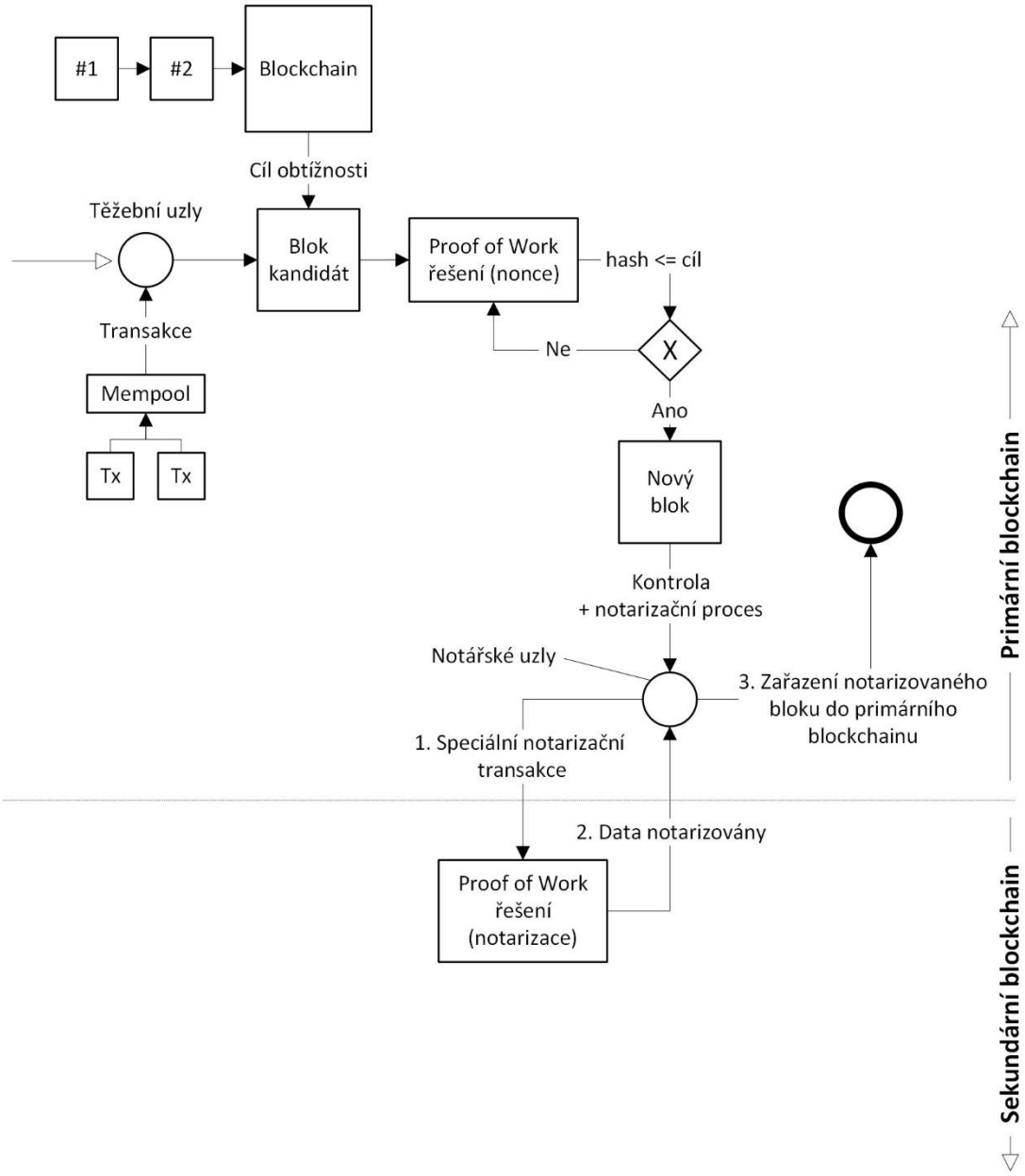
Delayed Proof of Work (DPoW) je konsensní mechanismus, který využívá zabezpečení sekundárního Proof of Work blockchainu pro ochranu primárního blockchainu. Tento koncept byl poprvé implementován v multi-chain kryptoměně Komodo (KMD) a využívá zabezpečení PoW Sítě Litecoinu (do roku 2021 Bitcoin).

Transakční data z primárního blockchainu (Komodo) jsou pravidelně zálohována na sekundárním blockchainu (Litecoin, dříve Bitcoin) pomocí 64 notářských uzlů (obr. 10). Notářské uzly jsou speciální typ těžebního uzlu, který je zvolen na základě váženého hlasování podle vlastnictví kryptoměny Komodo (KMD), tímto způsobem jsou všechna data chráněna výpočetním výkonem sekundárního PoW blockchainu.

Záloha rovněž slouží i jako způsob řešení konfliktů sítě, protože DPoW se neřídí pravidlem nejdelšího řetězce, které je typické pro PoW sítě. Tento způsob dosažení konsensu nevyžaduje vysoký výpočetní výkon ani spotřebu elektrické energie, ale stále

závisí na sekundární PoW síti, která energii spotřebovává, to znamená, že energetická účinnost DPoW je diskutabilní.

Díky DPoW je síť odolnější proti 51 % útoku, neboť útočník by musel ovládnout obě sítě současně. Tento mechanismus poskytuje zvýšenou bezpečnost a odolnost proti útokům, aniž by přímo zvyšoval energetickou náročnost primárního blockchainu. [39] [40] [41]



Obrázek 10 – Komodo Delayed Proof of Work flowchart (vlastní zpracování)

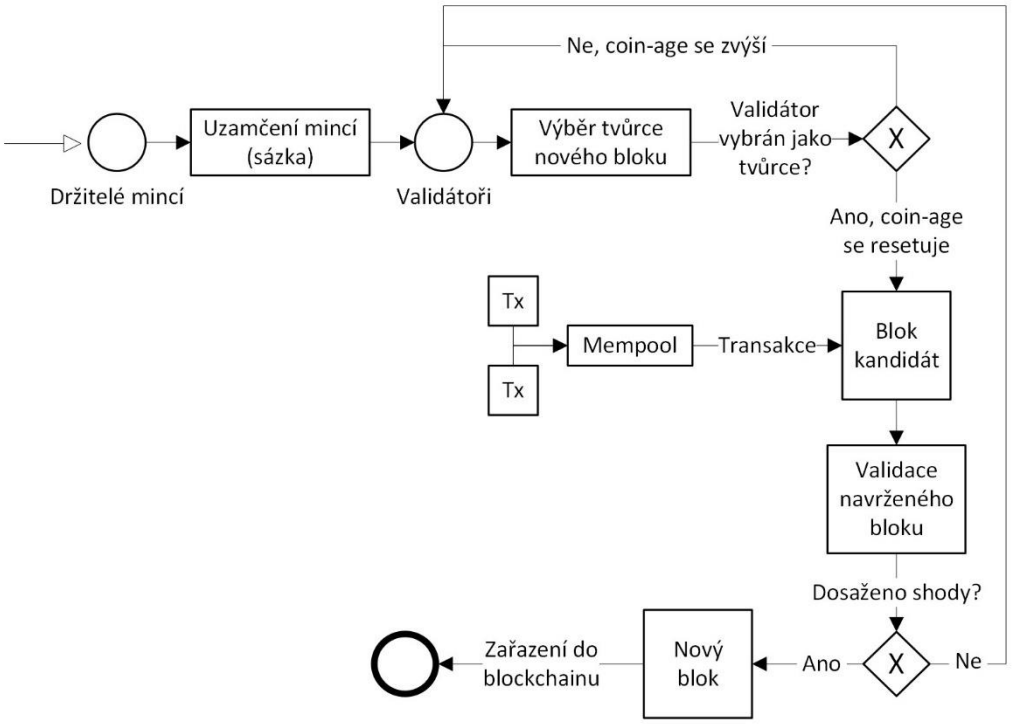
3.1.2 Proof of Stake

Proof of Stake (PoS) byl poprvé implementován v roce 2012 kryptoměnou Peercoin jako alternativa k Proof of Work kvůli jeho nedostatkům v oblasti škálovatelnosti a energetické efektivity. Společně s PoW patří PoS k nejrozšířenějším konsensním mechanismům.

V PoS síti uzly soutěží spíše ekonomicky místo využití výpočetního výkonu pro řešení složitých matematických problémů. Uzly, které se chtějí podílet na konsensu (validátoři), uzamknou své mince jako kolaterál (staking), čímž získávají šanci stát se příštím tvůrcem nového bloku na základě důkazu o vlastnictví (obr. 11) a získat tak odměnu v podobě transakčních poplatků a nově emitovaných mincí. Pravděpodobnost výběru validátora se zvyšuje s množstvím uzamčené kryptoměny.

Většina PoS implementací zohledňuje atribut stáří uzamčených mincí (coin-age), aby eliminovaly centralizaci procesu dosažení konsensu. Pakliže je uzel vybrán jako tvůrce, jeho coin-age se po vytvoření nového bloku resetuje. Pro přidání navrženého bloku do blockchainu musí nejdříve projít schvalovacím procesem, kterého se účastní ostatní validátoři dle podílu uzamčené kryptoměny v síti. Pokud by se tvůrce bloku pokusil podvádět nebo poškodit síť, jeho blok by byl zamítnut a přišel by tím o svůj kolaterál. Útočník pro úspěšný útok potřebuje většinový podíl mincí v síti (51 % útok), což je z ekonomického hlediska velmi náročné a u větších sítí typu Ethereum spíše nemožné.

PoS je z hlediska účasti na konsensu přístupnější širšímu spektru uživatelů, jelikož nevyžaduje nákladný těžební ani žádný jiný speciální hardware. Uzel se může stát validátorem i s minimální investicí do nativní kryptoměny. Absence těžby snižuje náklady na energii v porovnání s PoW až o 99 %. Dále PoS umožňuje rychlejší a efektivnější transakce, což vede k vyšší škálovatelnosti sítě. Ovšem některé implementace PoS můžou mít sklon k centralizaci, zejména pokud síť ovládá malý počet bohatých validátorů. Například burzy, které vlastní velké množství mincí investorů, mohou potencionálně představovat bezpečnostní riziko. [42] [43] [44]



Obrázek 11 – Proof of Stake flowchart (vlastní zpracování)

3.1.2.1 Delegated Proof of Stake

Mezi jednu z variant konsensního algoritmu Proof of Stake patří Delegated Proof of Stake (DPoS). Poprvé byl tento algoritmus implementován v roce 2014 Danielem Larimerem v projektu decentralizované směnárny BitShares. DPoS funguje na základě principů PoS, nicméně zde ale existuje několik klíčových rozdílů.

Validátoři v DPoS jsou skupina delegátů, které volí držitelé kryptoměny. Pouze delegáti jsou zodpovědní za ověřování transakcí, vytváření bloků a celkové řízení a zabezpečení sítě. V důsledku toho je tento algoritmus více centralizovaný než původní PoS, avšak za cenu nižší decentralizace nabízí vysokou škálovatelnost a rychlost. Validátoři jsou motivováni plnit svojí funkci čestně, jinak budou držiteli kryptoměny odstraněni.

Mezi významné představitele DPoS patří decentralizovaná blockchain platforma EOS, která byla spuštěna v roce 2018 společností Block.one, jejímž jedním ze zakladatelů je již zmíněný Daniel Larimer. EOS slouží jako platforma pro vývoj, hostování a provozování dApps. Decentralizované aplikace fungují jako počítačový kód na EOS blockchainu na platformě EOSIO pomocí chytrých kontraktů (smart contracts).

Aby mohli uživatelé využívat EOS dApps, musejí nejdříve vlastnit EOS tokeny, které slouží jako platidlo za výpočetní zdroje v podobě CPU, RAM a úložiště. [45] [46] [47] [48]

3.1.2.2 Leased Proof of Stake

Další významnou variantou Proof of Stake algoritmu je Leased Proof of Stake (LPoS), který byl poprvé implementován platformou Waves v roce 2017. LPoS principiálně funguje podobně jako PoS, ale přináší klíčovou inovaci v podobě možnosti pronájmu kryptoměny.

Držitelé kryptoměny mohou pronajmout svůj podíl plným uzlům (full nodes) v případě, že se sami nechtějí stát plnými uzly a získat procentuální podíl z odměny v případě nalezení nového bloku. Full nodes jsou uzly odpovědné za ověřování transakcí a řízení sítě. Je třeba zmínit, že pro provozování plného uzlu je nutné disponovat alespoň 1 000 tokeny kryptoměny WAVES. Pronajaté kryptoměny jsou, podobně jako při stakingu, uzamčeny na vlastníkově adrese ve prospěch zvoleného plného uzlu (lease transakce), což zabraňuje jejich přesunu, avšak stále zůstávají ve vlastnictví pronajímatele, který může pronájem kdykoliv zrušit. Tento způsob umožňuje komukoliv se podílet na údržbě sítě. Samozřejmě zde opět platí, čím více vlastní plný uzel kryptoměny WAVES (včetně pronajaté), tím větší šanci má být vybrán jako tvůrce nového bloku.

LPoS má potenciál pro vyšší decentralizaci, protože umožňuje uživatelům s menšími prostředky zapojit se do správy sítě, na druhou stranu potencionálně existuje riziko centralizace, kdy by bohaté uzly, které vlastní velké množství tokenů (vlastní i pronajaté), mohly ovládat část sítě. [49] [50]

3.1.2.3 Secure Proof of Stake

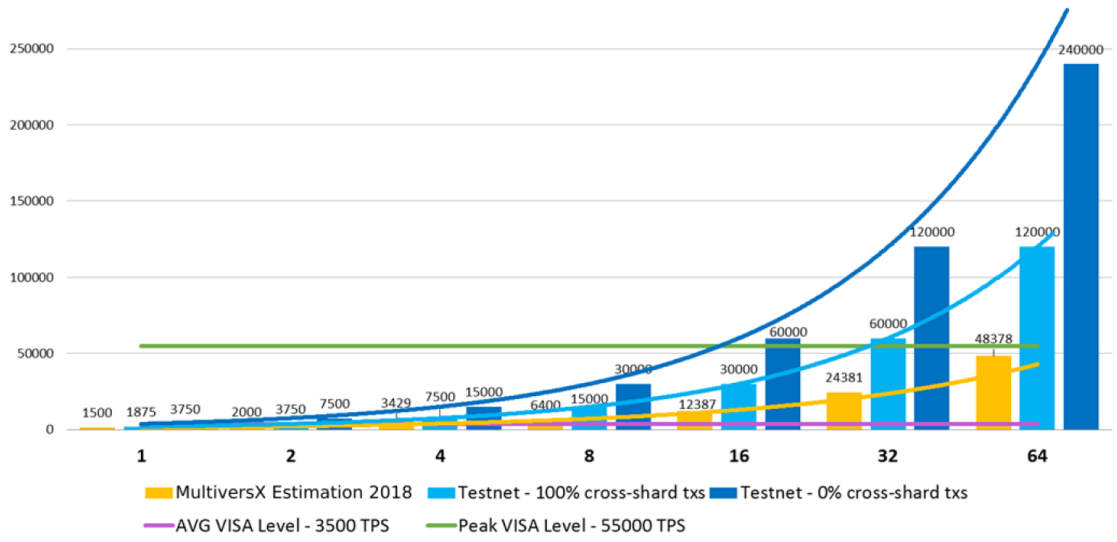
Secure Proof of Stake (SPoS) algoritmus je kombinací PoS a systému reputace, který nabízí více decentralizované a bezpečné řešení dosažení shody. Validátoři jsou k vytváření nových bloků vybíráni na základě množství vsazené kryptoměny a skóre

jejich reputace, které se určuje dle chování v minulosti. Tento systém zohledňuje faktory, jako je počet vytvořených bloků, celková dostupnost a potencionální škodlivé chování a podobně. Rozdíl oproti původnímu PoS je mimo to, jakým způsobem jsou validátoři vybíráni i implementace technologie adaptivního shardingu, což je rozdělení sítě na menší části.

SPoS algoritmus byl poprvé představen v projektu Elrond Network (nyní MultiversX) v roce 2019 s cílem vytvořit bezpečnou a vysoce škálovatelnou platformu, to se jim díky shardingu v SPoS podařilo, síť aktuálně umožňuje 30 000 transakcí za vteřinu (teoreticky škálovatelné až na 100 000/s) za velmi nízký poplatek a generování nových bloků každých 6 sekund.

MultiversX SPoS je založen na technologii shardingu, kdy je celá síť rozdělná na několik nezávislých paralelně propojených shardů a každý shard má svoji skupinu validátorů, kteří zpracovávají transakce a bloky v rámci svého shardu. Celý proces poté funguje tak, že bloky ze všech shardů jsou zasílány do metachainu, což je hlavní blockchain udržující celkovou bezpečnost a synchronizaci mezi jednotlivými shardy. Metachain validátoři bloky ze shardů validuje a na základě shody z nich vytváří finální bloky, které jsou poté zařazeny do blockchainu. Pro zařazení do blockchainu musí dojít ke shodě 2/3 + 1 validátorů v časovém limitu 6 vteřin. Validátoři jsou do shardů a metachainu vybírány náhodně z poolu validátorů na základě jejich sázky a reputace. Jejich počet se dynamicky mění dle potřeb sítě. Aby se zamezilo centralizaci, jsou validátoři vybíráni na určitou dobu, v MultiversX se tato doba nazývá epocha a trvá určitý počet bloků.

SPoS algoritmus není široce rozšířený a v kombinaci se shardingem je mnohem komplexnější než klasický Proof of Stake nebo Proof of Work, nicméně nabízí vysokou škálovatelnost, nízké poplatky za transakce a spravedlivé rozdělení moci v síti na základě důkazu o vlastnictví a chování v minulosti, díky čemuž je bezpečný proti široké škále potencionálních útoků. [51] [52] [53]



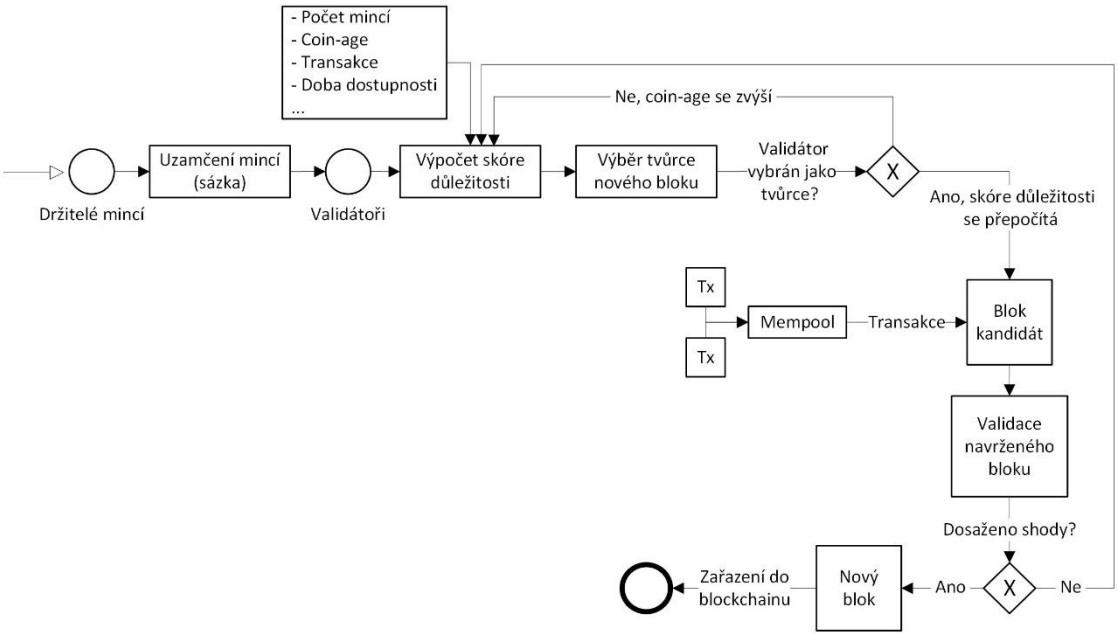
Graf 1 – SPoS MultiversX propustnost v porovnání s globální rychlostí sítě [53]

3.1.2.4 Proof of Importance

Proof of Importance (PoI) je algoritmus založený na Proof of Stake, který zohledňuje chování uživatele v minulosti. Každý uživatel má skóre důležitosti, které se zvyšuje na základě počtu provedených transakcí, jejich frekvence a množství vsazené kryptoměny. Skóre důležitosti je vypočítáváno specifickým algoritmem sítě, čím vyšší skóre uzel má, tím vyšší má šanci se stát tvůrcem nového bloku.

Proof of Importance byl poprvé představen platformou NEM (New Economy Movement) v roce 2015. PoI se liší od PoS v tom, že šance stát se validátorem (v NEM síti harvester) nezávisí pouze na vsazeném množství kryptoměny, ale také na reputaci v síti (skóre důležitosti). Uzel musí dosáhnout minimálního vkladu 10 000 XEM (nativní kryptoměna NEM) a splnit další podmínky ohledně realizovaných transakcí, aby se mohl stát validátorem na základě skóre důležitosti. Vklad se vypočítává 10 % každých 24 hodin z celkového stavu adresy, to znamená, že pokud například uzel vlastní 20 000 XEM, po 24 hodinách jeho vklad činí 2000 XEM, po 48 hodinách pak 3800. Dalším předpokladem jsou realizované transakce alespoň v hodnotě 1000 XEM za posledních 30 dnů na adresy, které mají rovněž splněn cíl vsazení v hodnotě 10 000 XEM. Pokud uzel tyto podmínky splní, je způsobilý ověřovat transakce a stát se v budoucnu validátorem na základě skóre jeho důležitosti.

PoI na rozdíl od PoS motivuje uživatele k větší aktivitě a podpoře ekosystému, což přispívá k jeho rostoucí hodnotě a udržitelnosti. Oproti PoS, kde bohatí uživatelé pouze shromažďují kryptoměnu ve své peněžence a získávají větší část odměn, PoI preferuje uživatele, kteří jsou v síti aktivní, což zvyšuje její efektivitu a stabilitu. [54] [55]



Obrázek 12 – Proof of Importance flowchart (vlastní zpracování)

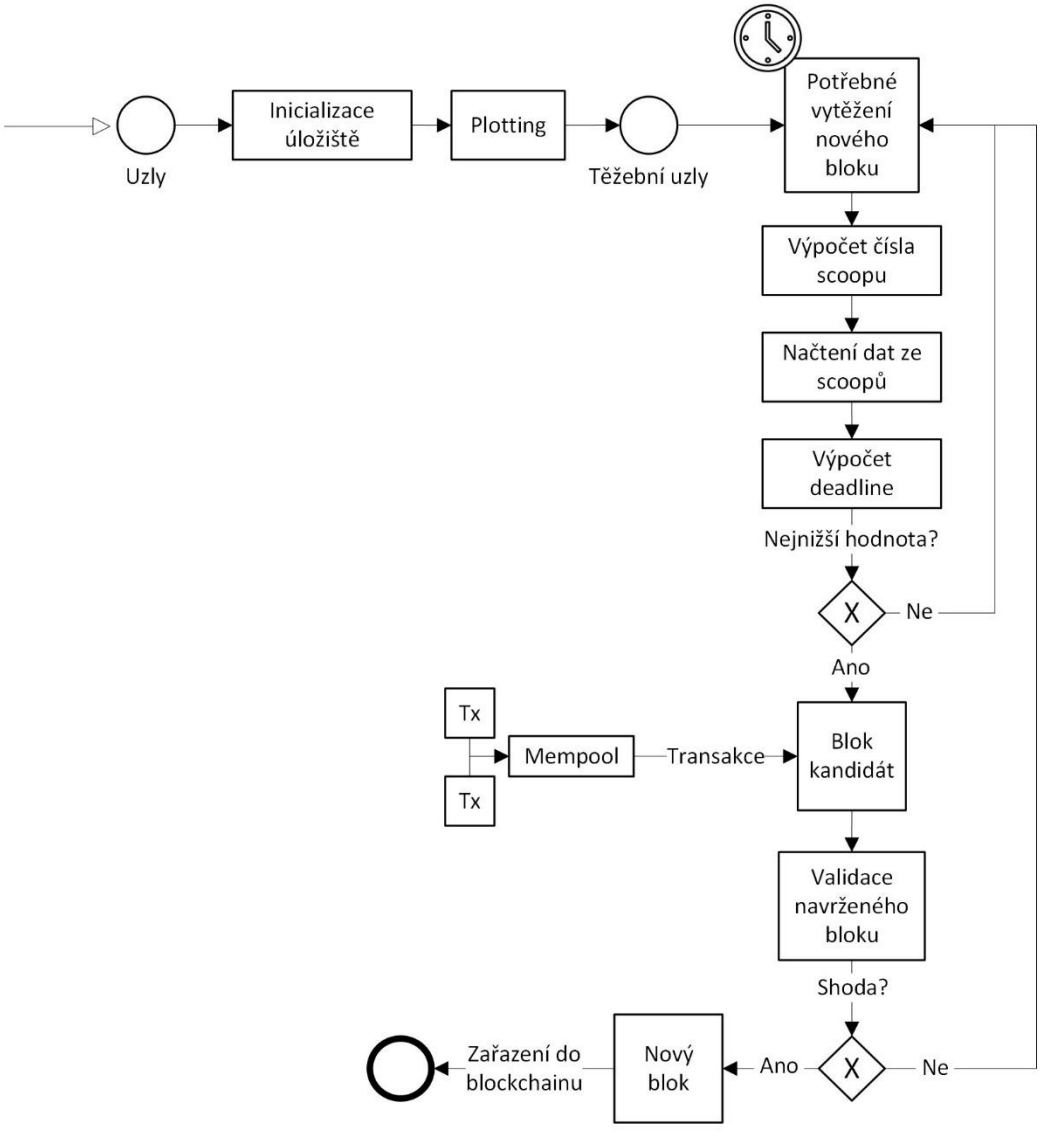
3.1.3 Proof of Capacity

Proof of Capacity (PoC) známý také pod názvem Proof of Space nebo Proof of Storage je konsensní mechanismus, který umožňuje těžbu kryptoměn pomocí volného místa na disku. Účastníci konsensu prokazují, že pro síť alokovali úložný prostor na pevném disku. Proces zahrnuje alokaci dat zvanou plotting, ve které těžební uzel jednorázově vypočítá kapacitně náročný data set možných hodnot nonce zahrnující i těžařovu adresu, čímž je docíleno toho, že má každý svůj unikátní data set. Čím větší kapacita disku, tím větší množství hodnot řešení a vyšší šance vytěžení nového bloku.

Každá nonce v data setu má 8192 hashů (0-8191), které jsou za sebou řazeny po dvojicích do takzvaných scoops. Těžební proces spočívá v tom, že se nejdříve vypočítá číslo scoopu, které se použije u všech noncí, vypočítá se deadline hodnota a nejnižší

odešle do sítě. Deadline je čas, který musí uplynout od vytvoření posledního bloku, než je těžařovi umožněno vytvořit nový. Uzel s nejnižším deadlinem získává povolení k vytvoření bloku.

První kryptoměnou implementující Proof of Capacity byl v roce 2014 Burstcoin (nyní Signum) s cílem vytvořit alternativní energeticky účinný způsob těžby. PoC může využívat jakýkoliv kapacitní prostor, který se dá zpětně znovu využít ke svému původnímu účelu narozdíl například od ASIC minérů pro těžbu bitcoinu, které mají pouze jediné specifické využití. PoC je energeticky účinnější než PoW a hardware není nutné stále upgradovat. Na druhou stranu rostoucí popularita PoC může vést k šíření těžebního malwaru na běžných zařízeních. [56] [57]



Obrázek 13 – Proof of Capacity flowchart (vlastní zpracování)

3.1.3.1 Proof of Space-Time

Proof of Space-Time (PoST) je konsensuální algoritmus, který kombinuje Proof of Capacity a Proof of Time za účelem vytvoření mechanismu šetrného k životnímu prostředí s nižší spotřebou energie, ale zároveň poskytuje vysokou míru zabezpečení a decentralizace.

PoST se od PoC liší v tom, že kromě alokovaného místa na disku musí uzel prokázat síti i čas, to znamená, že musí vyčlenit konkrétní kapacitu svého úložného místa a souhlasit s tím, že bude po určitý čas vyhrazena pro síť. Poté je uzlu sítí vygenerována takzvaná challenge (výzva), to je kapacitně náročné množství dat uložené v alokovaném úložném prostoru po stanovenou dobu, tento proces se nazývá plotting. Po určité době (většinou 1 minuta) musí uzel poskytnout Proof of Space-Time, to je kryptografický důkaz o tom, že uzel challenge skutečně po stanovenou dobu ukládá na disku. Po ověření důkazu se uzel smí účastnit procesu konsensu a za svojí investici do zabezpečení sítě může získat odměnu.

S implementací Proof of Space-Time přišel poprvé v roce 2017 projekt Filecoin, který slouží jako decentralizovaná úložná síť, která uživatelům umožňuje za odměnu pronajmout svůj úložný prostor jiným uživatelům. Filecoin k integritě a dostupnosti dat využívá PoST v kombinaci s Proof of Replication, který je se specifickými use-case v zásadě stejný jako Proof of Retrievability. Uživatelská data jsou šifrována, rozdělena na malé bloky a decentralizovaně uložena na síti. Ve své podstatě je Filecoin decentralizované cloudové řešení.

Proof of Space-Time nabízí energeticky a nákladově méně náročný způsob dosažení konsensu než Proof of Work s vysokou mírou decentralizace vhodný právě pro decentralizované distribuované úložné systémy. Na druhé straně je náročný na úložný prostor, mnohem víc komplexní a k vytvoření důkazu se musí provádět složité výpočty, což může ztížit škálovatelnost sítě. PoST se stále vyvíjí a závisí na časově synchronizovaných sítích, to může vést k náchylnosti k útokům spojených s manipulací času. [58] [59] [60] [61]

3.1.3.2 Proof of Retrievability

Proof of Retrievability (PoR) je podobně jako Proof of Space-Time algoritmus používaný v peer-to-peer decentralizovaných úložištích jako důkaz, že konkrétní data jsou uložena a dostupná. V PoR síti jsou dva hlavní typy účastníků, a sice běžný uživatel a poskytovatel úložného prostoru. Uživatel je uzel, jež na síti data ukládá, poskytovatel úložiště je na druhé straně uzel zavazující se k uložení dat a zachování jejich integrity.

Uživatel nejdříve rozdělí svá data na bloky, zašifruje je a distribuuje poskytovatelům, tímto je zajištěno, že i při ztrátě některých částí dat je bude možné obnovit. Aby si byl uživatel jistý, že poskytovatelé data stále mají, zasílá jim periodicky výzvu, což jsou zašifrované datové části. Poskytovatelé musejí na výzvy reagovat důkazem o znovunačtení (Proof of Retrievability), to jsou metadata, kterými prokážou, že konkrétní data mají stále uložená a dostupná, za což získají odměnu. Proof of Retrievability ověří síť a spolu s výzvou přidá do nového bloku v blockchainu, ten mimo jiné obsahuje i další informace o poskytovateli včetně množství zaplacené a odměněné kryptoměny, blockchain zde slouží jako záznam s informacemi o ukládání.

Teoretický koncept PoR byl poprvé představen ve výzkumné práci Proof of Retrievability: Theory and Implementation v roce 2007, později se objevil v návrhu projektu Permacoin, nicméně se nikdy nerealizoval. Aktuálně je konsensus na principu Proof of Retrievability implementován například v projektu decentralizované cloudové úložné platformy Storj, jež výměnou za odměnu v podobě kryptoměny umožňuje pronajímat úložný prostor. [62] [63] [64] [65]

3.2 Alternativní algoritmy založené na důkazech

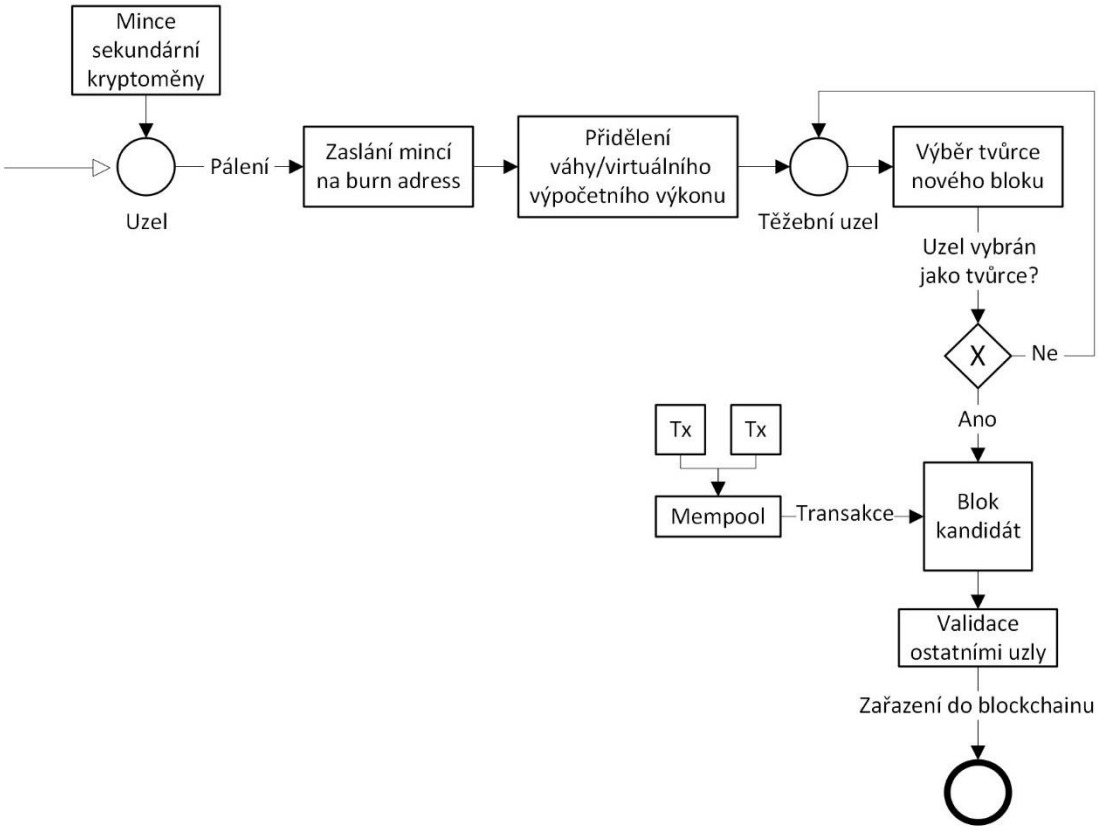
Skupina alternativních algoritmů založených na důkazech se týká konsensních mechanismů, které nezapadají do třídy tradičních algoritmů založených na důkazech. Jedná se o jedinečné nebo hybridní mechanismy, které se snaží řešit některé slabiny a omezení tradičních algoritmů, nicméně na druhou stranu jsou oproti nim méně testovány a implementovány, což může mít za následek ztížení posuzování jejich účinnosti nebo bezpečnosti.

3.2.1 Proof of Burn

Proof of Burn (PoB) je algoritmus založený na myšlence „spálení“ cenného aktiva, kryptoměny, výměnou za možnost účastnit se konsensu. Uzly v PoB síti musí poslat určité množství kryptoměny na adresu pro pálení tokenů (burn address), což je neutratitelná, nevyčerpatelná adresa, od které nikdo nevlastní privátní klíč, veškerá kryptoměna je na této adrese navždy uzamčená – spálená. Transakce je na blockchainu zaznamenána a slouží jako důkaz závazku vůči síti. Na základě množství spálených mincí je uzlu přidělen odpovídající váha nebo pomyslný výpočetní výkon a může se účastnit procesu konsensu. Čím více kryptoměny uzel spálí, tím větší má pravděpodobnost se stát tvůrcem nového bloku. Samotný výběr je náhodný a pravděpodobnost úměrná váze. Stejně jako stárne těžební hardware, i tento pomyslný výkon / váha s novými bloky v čase klesá, je deflační. Toto nutí těžební uzly pálit kryptoměnu pravidelně, svojí investicí do sítě ji udržují agilní.

Původní návrh PoB byl představen v roce 2012 a prvním projektem, který Proof of Burn konsensus implementoval, je Slimcoin spuštěný v roce 2014 s cílem se stát energeticky účinnou alternativou k Bitcoinu. Pálením kryptoměny získává těžařova adresa speciální atribut Effective Burnt Coins („efektivní spálené mince“), který mu po určitou dobu za svojí investici do sítě umožňuje se účastnit konsensu. Slimcoin mimo PoB využívá ještě Proof of Work a Proof of Stake konsensní mechanismy, to znamená, že pokud se uzel nechce účastnit PoB konsensu, může využít hardware k těžbě nativní kryptoměny, nebo ji nakoupit a jít cestou PoS.

PoB konsensus sám o sobě nevyžaduje, aby uzly vykonávaly náročné výpočetní operace a tím spotřebovávaly značné množství energii, nicméně původ pálených kryptoměn může pocházet z PoW sítí (například bitcoin), poté je energetická nenáročnost tohoto algoritmu sporná. Pálení mincí sítí s pevně stanoveným konečným množstvím kryptoměny, jako je právě již zmíněný bitcoin, lze považovat za plýtvání zdroji, jelikož hardware lze pořídit nový, ale kryptoměna s konečným počtem je nenávratně ztracena. PoB motivuje těžaře se do projektu zapojit po delší dobu, vzdávají se krátkodobého zisku ve prospěch možného dlouhodobého. [66] [67] [68]



Obrázek 14 – Proof of Burn flowchart (vlastní zpracování)

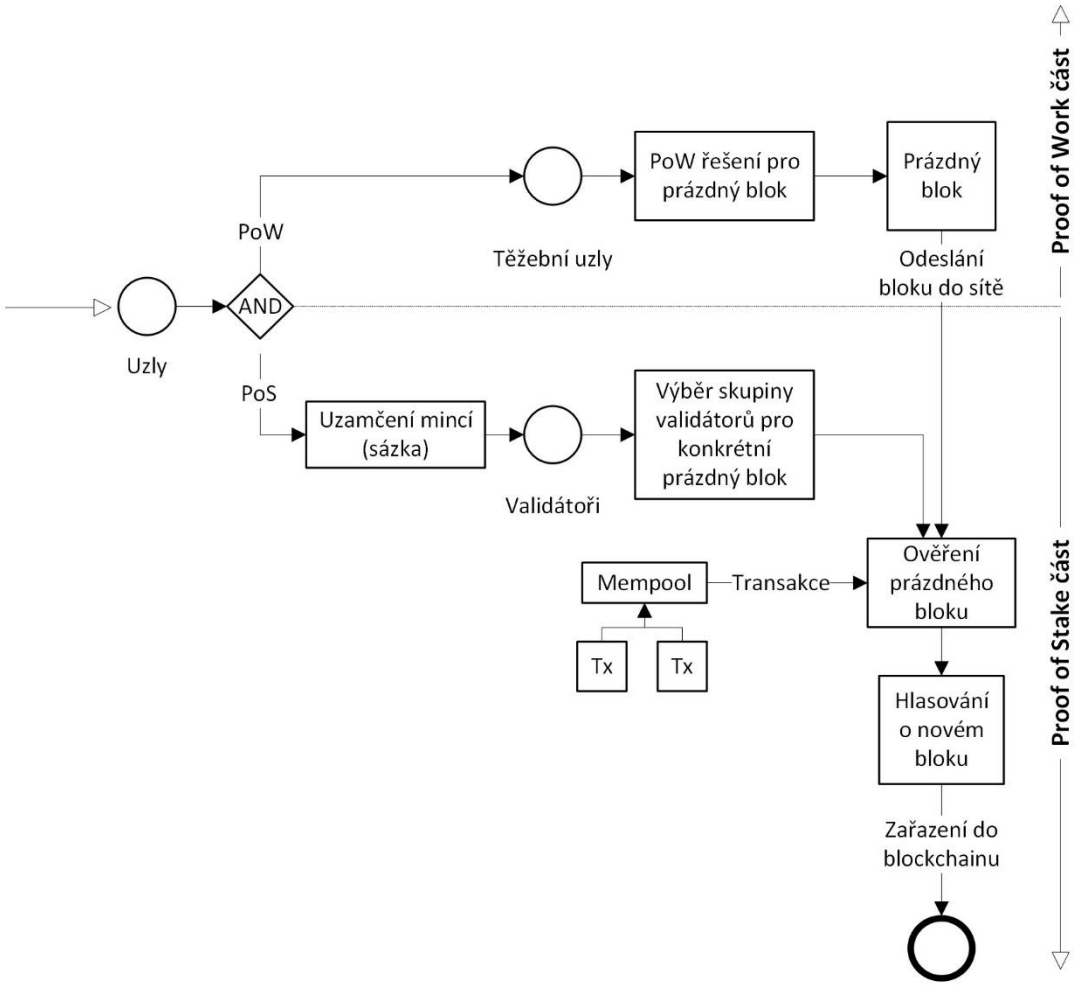
3.2.2 Proof of Activity

Proof of Activity (PoAc) je hybridní konsensní mechanismus, který kombinuje prvky Proof of Stake a Proof of Work. Síť k zabezpečení využívá malé množství výpočetního výkonu (těžaři – PoW) a poté přechází k hlasování o přidávaných blocích (validátoři – PoS). Oba typy uzlů na řešení spolupracují, těžaři nejdříve najdou PoW řešení prázdného bloku, který neobsahuje žádné transakce, slouží jen jako šablona s informacemi. Tento prázdný blok odešlou do sítě a přichází na řadu PoS, kdy je dle hlavičky bloku náhodně vybrána k podpisu skupina validátorů na základě uzamčeného podílu v síti, kteří o bloku hlasují a přidávají transakce. Pokud mezi validátory nedojde ke shodě a někteří z nich blok nepodepíšou, přichází se svojí sadou validátorů na řadu další prázdný vítězný blok v pořadí. Odměna se dělí mezi těžaře a validátory po úspěšném zařazení bloku do blockchainu.

Koncept Proof of Activity se poprvé objevil v roce 2013 v návrhu kryptoměny Memcoin$_2$, o rok později byl tento návrh převzat společností Company 0, která na jeho

základě v 2016 spustila první velký kryptoměnový projekt Decred založený na PoAc. Decred v PoS části konsensu implementuje ticket voting, validátor si výměnou za DCR (nativní kryptoměna Decred blockchainu) koupí ticket, který je použit v konsensu jako hlas. Po vytěžení prázdného bloku je vybráno náhodně 5 ticketů a jejich vlastníci se účastní procesu validace bloku. Přidáním nového bloku do blockchainu se generuje 20 nových ticketů a proces konsensu se opakuje.

Vzhledem k tomu, že je PoAc hybridní algoritmus, dědí výhody i nevýhody obou algoritmů, kvůli přítomným prvkům PoW v jisté míře spotřebovává zdroje související s těžbou, na druhé straně v kombinaci s PoS je vysoce zabezpečený, jelikož snaha o 51% útok klesá téměř na nulu, je velmi nepravděpodobné, že by útočník vlastnil většinu výpočetního výkonu a mincí kryptoměny zároveň. [69] [70] [71]



Obrázek 15 – Proof of Activity flowchart (vlastní zpracování)

3.2.3 Proof of Elapsed Time

Proof of Elapsed Time (PoET) je alternativa k Proof of Work a částečně i Proof of Stake algoritmu a navržený k použití v blockchainech s povolením jako spravedlivý loterijní systém k získání práva na těžbu. V PoET jsou místo těžebních uzlů validátoři, validátorem se může stát jakýkoliv uzel, který v síti požádá důvěryhodný generátor náhodných čísel o přidělení takzvané čekací doby, jedná se o náhodně dlouhou dobu, po kterou musí uzel čekat, než získá právo vytvořit nový blok, který je poté sítí ověřen a uzel získá odměnu.

PoET je založen na důvěryhodné výpočetní technice TEE (Trusted Execution Environment), která pro uzly generuje náhodné čekací doby, čímž spravedlivě umožňuje se decentralizovaně účastnit konsensu bez nutnosti vysokých pořizovacích nákladů na těžební hardware, čímž se stává energeticky účinným. Tento algoritmus je vhodný pro projekty, které hledají energeticky účinný a spravedlivý způsob zajištění konsensu v síti. PoET však může čelit omezení v případě širokého nasazení v blockchainových sítích bez povolení, kde nelze zaručit důvěryhodnost všech účastníků.

Algoritmus se využívá od roku 2016 v open-source blockchain-as-a-service projektu Hyperledger Sawtooth sloužící jako podniková platforma pro vytváření DLT aplikací a sítí. [72] [73] [74] [75]

3.2.4 Proof of Authority

Proof of Authority (PoAu) je mechanismus, který se zdánlivě podobná Proof of Stake s tím rozdílem, že v PoAu síti je předem vybrána malá skupina uzlů (většinou 5-20) nazývaná autority. Pouze tyto uzly jsou oprávněny ověřovat transakce a vytvářet bloky, které podepisují svým kryptografickým podpisem jako důkaz, že byl blok ověřen důvěryhodnou autoritou. Blok je poté sítí ověřen, zda skutečně došlo k oprávněnému podpisu.

V PoAu síti je proces ověřování transakcí a generování nových bloků centralizovaný a závisí pouze na poctivosti autorit a jejich reputaci. Tento mechanismus konsensu se proto obvykle využívá v privátních nebo konsorciálních blockchainech, kde

jsou vybrané autority známé a důvěryhodné. Autority jsou odměňovány za svou poctivost ve formě kryptoměny nebo nějaké jiné kompenzace.

PoAu je kromě implementace v různých konsorciálních blockchainech také využíván například v síti Kovan, která slouží jako veřejná testovací síť pro Ethereum blockchain k testování a vývoji decentralizovaných aplikací a chytrých smluv před jejich nasazením v hlavní síti. Kovan Testnet napodobuje podmínky hlavní sítě včetně jejího konsensního mechanismu Proof of Stake.

Síť PoAu není decentralizovaná, validátoři bloků jsou známé autority, čímž se rapidně snižuje šance na 51 % útok a zlepšuje se celkové zabezpečení sítě. Transakce jsou rychlejší, efektivnější a mnohonásobně více škálovatelné než v PoW nebo PoS. Svými vlastnostmi je tento mechanismus vhodný pro regulační účely, kdy je potřeba zajistit transparentnost a auditovatelnost. [76] [77] [78] [79]

3.3 Fault Tolerance algoritmy

Algoritmy z třídy Fault Tolerance jsou konsensní algoritmy, které nevyužívají důkazy k dosažení shody. Jsou navrženy tak, aby celý systém udržoval funkčnost a účetní kniha zůstávala konzistentní i v případě výpadku nebo chyb části uzlů. Tyto algoritmy jsou klíčové pro vysokou dostupnost a spolehlivost distribuovaných systémů. Mohou být založeny na různých principech, jako jsou záložní uzly, redundance nebo replikace komponent, ale společný cíl je vždy pro všechny stejný, a sice minimalizace dopadu výpadků a chyb.

V této kapitole jsou popsány dvě základní skupiny algoritmů této třídy – Byzantine Fault Tolerance a Crash Fault Tolerance.

3.3.1 Byzantine Fault Tolerance

Vývoj konsensního mechanismu Byzantine Fault Tolerance (BFT) byl inspirován koncepcí problému byzantských generálů, což je myšlenkový experiment v počítačové vědě představený v roce 1982 autory L. Lamport, R. Shostak a M. Pease. Jedná se o scénář, kde se několik generálů velících svým armádám musí z různých míst domluvit na společném postupu proti nepříteli, nicméně komunikační cesty mezi nimi

jsou nespolehlivé a někteří z generálů mohou být zrádci. Problém spočívá v tom, jak se s loajálními generály domluvit na společném plánu i za předpokladu, že mezi nimi může být zrádce. Jedná se o způsob dosažení konsensu s nespolehlivými účastníky v nedůvěryhodném prostředí.

Mechanismy BFT jsou třídou algoritmů využívaných v distribuovaných systémech s cílem zajistit správnou funkčnost i v případě přítomnosti takzvaných byzantských uzlů neboli chybných či škodlivých uzlů. BFT algoritmy zajišťují konzistenci v distribuovaných systémech i v případě, že část uzlů bude nespolehlivých. Obvykle je k dosažení shody zapotřebí 2/3 + 1 hlasů z celkového počtu uzlů (validátorů). BFT byl implementován v různých formách a systémech, v DLT se využívá k dosažení konsensu o stavu účetní knihy. Algoritmy BFT byly v minulosti nejčastěji využívány v privátních sítích, kde jsou uzly známé a důvěryhodné, to se ovšem s příchodem nově optimalizovaných konsensních mechanismů založených na BFT změnilo. Nové řešení problému byzantských generálů cílí na rovnováhu mezi decentralizací, bezpečností a škálovatelností, čímž se stávají adekvátní alternativou k algoritmům založených na důkazech pro využití ve veřejných DLT. [80] [81]

3.3.1.1 Practical Byzantine Fault Tolerance

Nejrozšířenějším algoritmem ze skupiny BFT je Practical Byzantine Fault Tolerance (PBFT) představený ve stejnojmenném článku z roku 1999 autory M. Castro a B. Liskov, kteří již v té době věřili, že BFT algoritmy budou v budoucnu významným způsobem dosažení shody. PBFT je jedním z prvních algoritmů vycházející z původního návrhu BFT, který řeší nedostatky původního řešení.

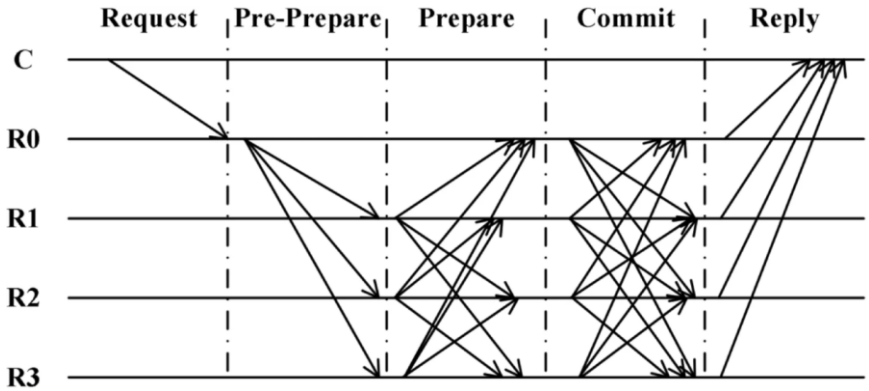
PBFT je mechanismus konsensu, který funguje v asynchronním prostředí, kde uzly nejsou vázány striktním omezením ohledně doby doručení zpráv mezi sebou. Uzly mohou dohodnout na aktuálním stavu i za předpokladu, že je v síti přítomna až 1/3 byzantských uzlů, které se potencionálně mohou chovat škodlivě a pokusit se systémem manipulovat. PBFT obsahuje kromě běžných klientských uzlů další typy, a sice takzvané repliky, to jsou uzly, které udržují kopii účetní knihy (obdobně jako u PoW full nodes), ověřují transakce a účastní se konsensu. Mezi replikami dále dochází k volbě jednoho primárního uzlu (primární replika), který koordinuje komunikaci mezi

ostatními replikami, zajišťuje uspořádání a předávání zpráv, funguje v podstatě jako takový moderátor mezi klientskými uzly a ostatními replikami.

Celý mechanismus konsensu se potom skládá ze tří fází – předpřípravná, přípravná a fáze potvrzení. V předpřípravné fázi vytvoří primární uzel návrh nového bloku obsahující transakce a rozešle jej ostatním replikám (obr. 17), které v přípravné fázi navrhovaný blok ověří a hlasují o jeho přijetí. Pokud 2/3 + 1 replik hlasovaly pro navrhovaný blok, přechází proces do poslední fáze potvrzení, kdy je konečná dohoda vyslána do sítě a blok přidán do blockchainu.

Hlavní výhodou PBFT je absence nutnosti provádět energeticky náročné výpočty, což jej činí energeticky efektivním způsobem dosažení konsensu. Odměna je dělena mezi všechny replikační uzly rovnoměrně. Transakce jsou v PBFT na rozdíl od PoW finální, nevyžadují vícenásobné potvrzení, pokud je navržený blok přijat, pak je konečný. Problémy přichází se škálovatelností, s rostoucím počtem uzlů v síti se zhoršuje komunikace a zvyšuje čas odezvy. PBFT sítě jsou také více zranitelné proti Sybil útokům, kdy útočník ovládá větší počet uzlů.

Open-source blockchain platforma Hyperledger Sawtooth hostovaná Linux Foundation určená pro vývoj dApps podnikové úrovně umožňuje využití různých konsensních mechanismů včetně PBFT v řešeních s konsorciálními nebo privátními blockchainy, kde jsou účastníci sítě důvěryhodní. [82] [83] [84]



Obrázek 16 – PBFT flowchart [84]

3.3.1.2 Delegated Byzantine Fault Tolerance

Delegated Byzantine Fault Tolerance (DBFT) je další algoritmus z třídy BFT a rozšířením PBFT, od kterého se liší tím, že využívá mechanismus delegování podobně jako DPoS.

Poprvé byl algoritmus implementován decentralizovanou platformou NEO v roce 2014 (dříve Antshares), která slouží jako platforma pro chytré kontrakty, dApps a digitální aktiva. DBFT konsensus zde funguje podobně jako systém správy. V síti se nachází obyčejné uzly, to jsou držitelé NEO tokenů, kteří v procesu hlasování periodicky vybírají menší počet svých delegátů (bookkeeping nodes). Delegáti jsou úzkou skupinou uzlů zodpovědných za ověřování transakcí a přidávání bloků do blockchainu. Jeden z delegátů je náhodným výběrem vybrán jako takzvaný řečník (speaker) zodpovědný za vytvoření návrhu bloku. Navržený blok je poté rozeslán ostatním delegátům, kteří jej zkontrolují a poté hlasují. Blok je přijat a přidán do blockchainu, pokud se shodnou 2/3 + 1 delegátů, v opačném případě je vybrán nový řečník a celý proces se opakuje. NEO platforma odděluje práva na správu a práva na využívání sítě. Síť obsahuje dva tokeny – NEO a GAS. NEO je nedělitelný token, který představuje vlastnictví sítě a dává držiteli hlasovací práva. Na druhé straně GAS je token generovaný držitelům NEO, který síť pohání, slouží k platbám za transakce, chytré kontrakty a dApps.

DBFT konsensus v NEO umožňuje vysokou škálovatelnost, tvorba nového bloku zabere zhruba 15 až 20 vteřin s možností až 1000 transakcí za vteřinu, což je v porovnání s PoW Bitcoinu se 7 transakcemi za sekundu mnohonásobně větší počet. Avšak stále se nemůže rovnat s Bitcoinem v decentralizaci, NEO Foundation vlastní velké procento z celkového počtu NEO tokenů, které postupně uvolňují do oběhu a prostředky využívají k rozvoji platformy. Tato skutečnost ovšem znamená, že NEO je zatím částečně centralizovanou platformou.

DBFT přináší několik výhod oproti PBFT a PoW algoritmům, je energeticky nenáročný, jelikož k dosažení shody nevyužívá těžební proces. Z hlediska bezpečnosti eliminuje riziko Sybil útoků, protože útočník by musel získat důvěru ostatních uzlů a být zvolen jako delegát. K nevýhodám patří nižší úroveň decentralizace v porovnání s PoW nebo PoS, což může vést k potencionálnímu zneužití moci. Rovněž s rostoucím počtem uzlů v síti se zvyšuje komplexita komunikace, což může vést k problémům se stabilitou a rychlostí sítě. [85] [86] [87]

3.3.1.3 Asynchronous Byzantine Fault Tolerance

Asynchronous Byzantine Fault Tolerance (ABFT) je algoritmus vyznačující se tím, že k dosažení shody využívá asynchronní komunikaci, to znamená, že zde neexistuje žádná časová hranice pro doručení zpráv mezi uzly, může se stát, že zprávy budou zpožděny. Kdyby například PBFT využíval asynchronní komunikaci, dosažení konsensu by bylo výrazně ztížené nebo nemožné, ABFT ale toto omezení překonává, komunikace mezi uzly není závislá na čase doručení zpráv, to znamená, že probíhá v nepředvídatelném prostředí nepředvídatelně dlouho. Konsensu je dosaženo prostřednictvím kombinace vysílání zpráv a hlasování. Uzel po přijetí zprávy musí dosáhnout konsensu o její platnosti s ostatními, pokud většina hlasuje pro, je zpráva označena za potvrzenou a lze ji použít k aktualizaci celkového stavu systému.

Hedera Hashgraph je nejznámějším a největším představitelem implementace konsensního mechanismu ABFT nazvaného Hashgraph. Hashgraph konsensus k šíření zpráv obsahujících transakce využívá gossip protokol (takzvaně „gossip about gossip“), kdy uzly rozesílají zprávy náhodně vybraným dalším uzlům, čímž se informace o transakcích sítí šíří extrémně rychle. Všechny události obsahující transakce jsou uzly ukládány lokálně v Hashgraph datové struktuře a každá událost je spojena se svojí rodičovskou, čímž je vytvořen DAG událostí. Ke každé události si uzly přidávají časový údaj o tom, kdy k nim informace o transakcích dorazily. Seřazením časů všech uzlů pro každou transakci a následným výběrem jedné hodnoty ze středu seznamu dojde ke správnému určení pořadí transakcí v síti. Konsensu o stavu Hashgraphu je dosaženo pomocí virtuálního hlasování, aniž by si uzly hlasy skutečně posílaly.

Systém hlasování je asynchronní, uzly nemusejí čekat na účast v hlasování, mohou dále zpracovávat zprávy (transakce) i v případě, že jsou některé uzly nedostupné. Aby došlo k dosažení konsensu o pořadí jednotlivých událostí, každý uzel určuje „hlasy“ pro každou událost ve svém lokálním hashgraphu sečtením počtu hlasů, které obdržela od jiných událostí. Hlasy jsou reprezentovány počtem vztahů mezi rodiči a dětmi mezi událostmi. Jakmile uzly sečtou hlasy pro každou událost, tak výsledky porovnají a pokud se většina shodne, je dosaženo konsensu o stavu Hashgraphu.

Mezi hlavní výhody ABFT patří jeho vysoká škálovatelnost a rychlost, Hashgraph ABFT je rychlejší než tradiční BFT algoritmy, potenciálně dokáže zpracovat až stovky tisíc transakcí za vteřinu. Hashgraph je energeticky nenáročný, protože neprovádí žádné složité výpočty a zároveň je férovější než tradiční algoritmy založené

na důkazech, jelikož u Hashgraphu není možné individuálně měnit pořadí transakcí. [26] [88] [89] [90]

3.3.1.4 Federated Byzantine Agreement

Ve Federated Byzantine Agreement (FBA) mechanismu je za ověřování transakcí a dosahování konsensu o stavu DLT odpovědná sada uzlů zvaná kvórum (quorum). Transakce v síti jsou přijímány uzly kvóra, kteří ji validují na základě pravidel stanovených konsensním mechanismem, aby se ujistily, že je platná. Jakmile je transakce ověřena, kvórum může dosáhnout konsensu o přidání transakce do bloku. Techniky konsensu se mohou v konkrétních implementacích lišit.

Stellar Consensus Protocol (SCP) využíván sítí Stellar je první implementací FBA. Mechanismus byl poprvé představen v roce 2015 Stellar Development Foundation ve svém whitepaperu. V SCP je kvórum důvěryhodných uzlů vybíráno sítí na základě více faktorů, jako je jejich sázka nativní kryptoměny Stellar Lumen (XLM), aktivita, reputace, dostupnost a výběr je pravidelně aktualizován. Velikost a složení kvóra se může dynamicky měnit. Jednotlivé uzly kvóra poté vytvoří vlastní segmenty kvóra (quorum slices) složené z jimi vybraných důvěryhodných uzlů. Jedná se o podskupiny uzlů v rámci většího kvóra, které jsou zodpovědné za ověřování transakcí. Jestliže se v síti objeví nová transakce, je náhodně vybrán segment kvóra, v němž uzly spolupracují na jejím ověření, kontrolují podpisy a zůstatky, aby se ujistily, že je platná. Jakmile je transakce segmentem potvrzena, je navržena, aby byla zahrnuta do dalšího bloku a je zaslána ostatním segmentům ke schválení. Schválené transakce jsou přidávány do návrhu bloku, o kterém segmenty kvóra poté hlasují. Blok je přijat a přidán do blockchainu, jestliže se shodne 2/3 + 1 uzlů kvóra. Tento způsob zajišťuje bezpečný a decentralizovaný způsob aktualizace stavu účetní knihy.

Mezi největší výhody SCP patří energetická účinnost, jelikož nevyžaduje provádět náročné výpočetní operace k ověřování transakcí a dosahování shody. SCP také zajišťuje nízkou latenci při ověřování transakcí a dosahování konsensu, což zlepšuje reakci sítě na nové transakce a umožňuje jejich rychlejší zpracování.

SCP síť je navržena jako decentralizované řešení, ale je silně závislá na správném výběru důvěryhodných uzlů a segmentů kvóra, neefektivní výběr může vést k nízké odolnosti proti byzantským chybám. Stellar Development Foundation stále

vlastní více jak 45 % z celkového počtu XLM, vzhledem k tomuto faktu může potenciálně výběr uzlů kvóra, kterých je jen několik desítek, ovlivňovat. SCP umožňuje vysokou škálovatelnost, dokáže zpracovat velké množství transakcí s nízkým poplatkem, čímž je efektivně využitelný ve větším měřítku například pro mikrotransakce. [91] [92] [93] [94]

3.3.2 Crash Fault Tolerance

Crash Fault Tolerance (CFT) je vedle BFT další skupinou algoritmů z třídy Fault Tolerance používaných v distribuovaných systémech, jejichž cílem je zajistit, že systém bude schopen tolerovat selhání určité části uzlů bez narušení jeho funkčnosti.

Rozdíl mezi CFT a BFT je v typu selhání, které mohou tolerovat. BFT předpokládá, že uzly mohou vykazovat byzantské neboli svévolné chování, včetně neúmyslného i úmyslného odesílání nesprávných zpráv. Na druhé straně CFT předpokládá, že uzel může selhat pouze poruchou nebo havárií, což znamená, že přestane fungovat úplně. V tomto případě může být dosaženo konsensu za předpokladu, že funguje nadpoloviční většina uzlů.

BFT je silnější skupinou algoritmů z třídy Fault Tolerance, protože je schopna zvládnout větší rozsah poruch než CFT, nicméně CFT jsou většinou výrazně jednodušší a rychlejší algoritmy, což je činí potencionálně možnou volbou v systémech vyžadujících rovnováhu mezi výkonem a spolehlivostí. [95]

3.3.2.1 Paxos & Fast Paxos

Paxos je skupina CFT konsensuálních algoritmů využívaných k dosažení shody o hodnotě v distribuovaných systémech. Poprvé byl tento algoritmus představen v 90. letech Leslie Lamportem a jeho rozšíření jsou využívány dodnes. Paxos je navržen pro práci v asynchronním prostředí, kde se některé uzly mohou v komunikaci zpožďovat.

Algoritmus využívá tři definované role k dosažení shody o hodnotě. Navrhovatelé (proposers) jsou uzly iniciující proces konsensu odesláním navrhované hodnoty kvóru příjemců neboli akceptorů (acceptors). Příjemci poté na základě

stanovených kritérií navrhovanou hodnotu hlasováním přijmou nebo odmítnou, pro přijetí musí hlasovat nadpoloviční většina. Třetí skupinou uzlů jsou studenti (learners), kteří se od akceptorů dohodnutou hodnotu „naučí“. V tomto okamžiku Paxos zaručuje, že hodnota je konečná a nezmění se, pokud je většina uzlů funkčních a dostupných.

Původní algoritmus Paxos, jak je navrhl Lamport, může být složitý a neškálovatelný, jelikož vyžaduje komunikaci mezi všemi uzly, což s rostoucím počtem uzlů a transakcí v síti povede k vysoké latenci. Nicméně v průběhu let došlo k různým optimalizacím, alternativám a novým rozšířením jako je například Fast Paxos, který tento problém řeší snížením počtu zpráv vyměňovaných mezi uzly, což má za následek rychlejší výkon v porovnání s původním Paxos algoritmem. Místo zpracovávání každého požadavku v samostatném kole Fast Paxos umožňuje zpracování více požadavků najednou, což zvyšuje efektivitu.

Paxos konsensus používá například služba Google Chubby, která je využívána v mnoha interních systémech Googlu ke koordinaci přístupu ke sdíleným zdrojům a ukázala se jako vysoce účinná, nicméně účinnost a spolehlivost Paxos algoritmu závisí na správné implementaci a konfiguraci. V praxi se mohou objevit problémy spojené s výkonem, latencí nebo stabilitou. [96] [97] [98] [99]

3.3.2.2 Raft

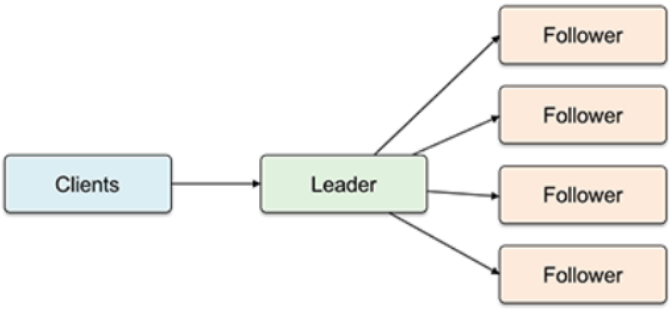
Konsensuální algoritmus Raft (Reliable, Available, Fault-Tolerance) poprvé představil v roce 2014 D. Ongaro a J. Ousterhout jako zjednodušenou alternativu k Paxos a Multi-Paxos. Algoritmus má na základě hlasování určený centrální vedoucí uzel, který je zodpovědný za řízení procesu konsensu, správu a distribuci dat. Všechny ostatní uzly jsou následovníky. Vedoucí uzel je poté zodpovědný za zpracování požadavků a replikaci dat svého stavu následovníkům, kteří vedoucímu aktualizace potvrzují. V případě detekce selhání nebo nedostupnosti vedoucího uzlu je iniciována volba nového, kdy všichni hlasují pro jednoho kandidáta. Vítězem se stane ten, který získá většinu hlasů.

Jakmile je záznam protokolu replikován na většinu uzlů, vedoucí rozešle zprávu o potvrzení všem uzlům v síti, tato zpráva značí, že záznam protokolu je nyní považován za potvrzený. Celý proces tedy funguje cyklicky tak, že vedoucí přijímá požadavky na transakce, které připojuje ke svému místnímu protokolu a poté vysílá

požadavek o připojení záznamu všem ostatním uzlům. Ostatní uzly požadavek zpracují a pokud má nadpoloviční většina konzistentní stav protokolu s vedoucím, odpoví zprávou o úspěšné replikaci a vedoucí považuje transakci za potvrzenou. Pokud uzel přijme konfliktní transakci, žádost odmítne a odešle žádost o volbu nového vůdce.

Raft poskytuje mechanismus zajištění konzistence dat, uzly udržují protokol hodnot, které byly odevzdány systému, když se připojí nový uzel stáhne si tento protokol od vedoucího uzlu a aktualizuje svůj stav. Raft také zahrnuje mechanismus umožňující systému zmenšit velikost protokolu a zlepšit výkon tím, že uchovává pouze nejaktuálnější data a staré záznamy zahazuje. Paxos i Raft jsou oba mechanismy, které garantují shodu na stejné hodnotě i v případě selhání části účastníků. Raft je oproti Paxos a Multi-Paxos jednodušší a více škálovatelný, jelikož nevyžaduje tolik kol komunikace mezi jednotlivými uzly.

Quorum je konsorciální verze Ethereum blockchainu určená pro podniky a organizace k vytváření bezpečných a škálovatelných dApps. Quorum nabízí více mechanismů konsensu včetně Raft, které jsou svými vlastnostmi vhodné pro konsorciální blockchainy. Volba algoritmu může být nakonfigurována tak, aby splňovala specifické požadavky konkrétního use-case, Raft nabízí finalitu transakcí, rychlejší blocktime a vytváření bloků na vyžádání. [100] [101] [102]



Obrázek 17 – Raft [103]

3.4 DAG algoritmy

DAG konsensní algoritmy jsou novou generací algoritmů, které se liší od blockchainových tím, že místo lineárního řazení dat vytváří orientované acyklické grafy. Tyto algoritmy se snaží vytvářet nový způsob distribuovaného konsensu, který nabízí lepší škálovatelnost, efektivitu a jednodušší ověřování transakcí bez nutnosti složitých výpočtů.

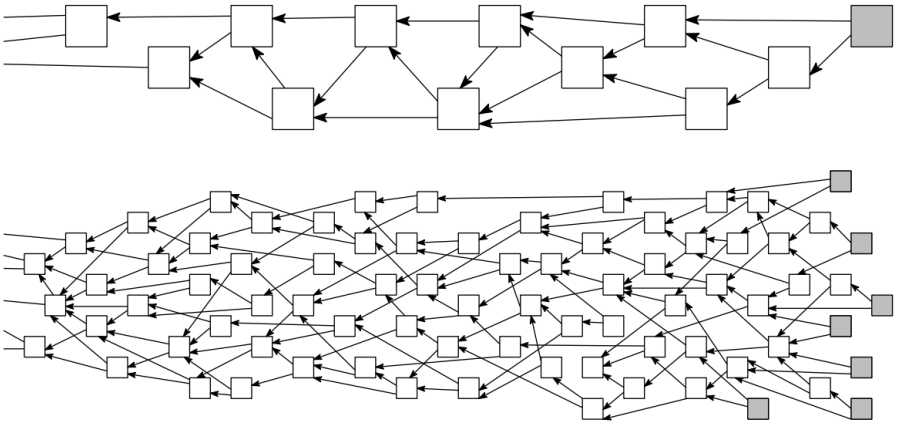
3.4.1 Tangle

Jednou z nejznámějších a nejrozšířenějších implementací DAG konsensních algoritmů je Tangle navržený a implementovaný kryptoměnou IOTA. Tangle je založen na technologii orientovaného acyklického grafu (DAG), čímž se svojí architekturou zásadně liší od mechanismů využívaných v blockchainových sítích. Tangle nesdružuje transakce do bloků, místo toho jsou ukládány v DAG struktuře (obr. 19), kde vrcholy reprezentují jednotlivé transakce a hrany vazby mezi nimi.

Každá transakce v Tangle obsahuje unikátní identifikátor, adresu odesílatele a příjemce, časové razítko, digitální podpis a další včetně odkazu na dvě předchozí transakce. Pokud chce uzel Tangle sítě přidat novou transakci, musí nejdříve potvrdit dvě předchozí neboli rodičovské transakce. Rodičovské transakce jsou vybírány na základě jejich váhy, což je v podstatě míra práce, která byla vynaložena na její vytvoření. Rodičovské transakce jsou uzlem ověřeny a potvrzeny, pokud neobsahují žádné konfliktní informace. Poté je nová transakce propojena s dvěma předchozími a úspěšně začleněna do Tangle DAG struktury. Konsensu je v Tangle dosaženo účasti a realizací nových transakcí uzly sítě, jelikož čím více nově přidaných transakcí, tím více potvrzení získají. Síť se s rostoucím počtem transakcí stává bezpečnější, protože potencionální útočník by musel vynaložit značné úsilí, aby dokázal zpětně dosáhnout konsensu na řetězci transakcí.

Jednou z hlavních výhod Tangle je jeho škálovatelnost, jelikož zpracování transakcí se zrychluje a zefektivňuje s rostoucím počtem uzlů a zejména transakcí v síti, které je možné zpracovávat paralelně. Čím více transakcí je zpracováno, tím více jich může být současně potvrzeno, to je přesný opak blockchainových konsensních

mechanismů. Tangle rovněž umožňuje buď žádné nebo velmi nízké transakční poplatky, protože vyžaduje provedení pouze minimální práce v podobě ověření dvou rodičovských transakcí, svojí podstatou je tedy vhodný například pro mikrotransakce nebo IoT. V aktuální verzi IOTA Tangle se jedná o částečně centralizovaný mechanismus, jelikož spoléhá na centrální autoritu, takzvaného koordinátora, který kontroluje platné transakce a následně jsou validovány celou sítí. To se ovšem má v blízké budoucnosti v IOTA 2.0 změnit a Tangle by se měl stát plně decentralizovaný způsob dosažení konsensu. Ačkoliv Tangle nabízí řadu výhod, stále se jedná o poměrně novou technologii a vývojáři prozatím dávají pořád raději přednost blockchainu. [104] [105] [106]



Obrázek 18 – Tangle – nízká (nahoře) a vysoká (dole) zátěž příchozích transakcí [106]

4 Analýza a komparativní hodnocení konsensních mechanismů

Kapitola 4 je zaměřena na detailní analýzu a komparativní hodnocení vybraných konsensních mechanismů, které sice všechny slouží ke stejnému účelu, což je dosažení shody v decentralizované síti, ale každý z nich má unikátní vlastnosti a kompromisní řešení v oblastech, jako je bezpečnost, decentralizace, škálovatelnost a energetická účinnost.

Součástí kapitoly je analýza rizik spojených s konsensními mechanismy, výběr a definice kritérií, dle kterých jsou jednotlivé mechanismy hodnoceny, přehled zranitelností vůči kybernetickým útokům a poté samotné kriteriální hodnocení včetně bodového a váženého. Závěr kapitoly tvoří přehled výhod a nevýhod jednotlivých mechanismů, který lépe umožňuje porozumět jejich kompromisům.

4.1 Rizika spojená s konsensními mechanismy

Tato kapitola se zaměřuje na rizika spojená s konsensními mechanismy a jejich vliv na decentralizované sítě a blockchainové technologie. Identifikace a pochopení těchto rizik je klíčové pro hodnocení a potencionální implementace konsensních mechanismů.

4.1.1 Bezpečnostní rizika

Bezpečnostní rizika a s tím spojené kybernetické útoky mohou negativně ovlivnit proces dosažení konsensu, čímž může docházet k zpomalování, zastavování nebo cenzuře transakcí, double-spendingu, manipulaci s časovými značkami, a tím k narušení důvěryhodnosti a destabilizaci sítě.

Při hodnocení konsensních mechanismů je důležité brát bezpečnostní rizika v potaz, jelikož slabiny mohou vést ke kompromitaci celé sítě. Úspěšně provedený útok

může mimo jiné negativně ovlivnit celé kryptoměnové odvětví a zpomalit adopci v této oblasti.

V této kapitole je popsáno několik nejznámějších a nejzásadnějších kybernetických útoků pro pochopení, jakým způsobem mohou být sítě napadeny, jak lze takové útoky odhalit a minimalizovat rizika.

Sybil útok

Sybil útok (Sybil Attack) je typ útoku, při kterém se útočník v distribuované síti snaží získat vliv vytvářením a kontrolou velkého počtu falešných uzlů. Falešné uzly mohou útočníkovi umožnit manipulaci ve svůj prospěch například se zdroji sítě, hlasováním a dalšími aspekty. V konsensních mechanismech mohou Sybil útoky zneužít slabých stránek některých algoritmů, které jsou založeny na reputaci či hlasování a narušit tak celkový proces dosažení shody nebo ovládnout celou síť. Nejvíce zranitelné jsou algoritmy, které nevyužívají důkazy, jelikož absence potřeby investovat zdroje (výpočetní výkon, finanční prostředky) k účasti na konsensu činí algoritmus proti Sybil útoku více zranitelným. [107]

51 % útok

V případě 51 % útoku (51 % Attack) získává útočník nadpoloviční většinu (>50 %) zdrojů sítě. Majoritní většina útočníkovi umožňuje potvrzovat a zasílat neplatné transakce, cenzurovat transakce, kontrolovat proces dosažení konsensu nebo vytvářet alternativní řetězce bloků a provádět double-spend útoky. Úspěšný 51 % útok vede k celkovému narušení důvěry v síť a většinou i ke ztrátě hodnoty kryptoměny. Tento typ útoku je nejčastěji spojován s algoritmy využívajícími výpočetní výkon k dosažení shody (Proof of Work). V případě například Proof of Stake je 51 % útok méně pravděpodobný, jelikož útočník by musel vlastnit nadpoloviční většinu kryptoměny sítě, což je samo o sobě nákladné a jeho celková investice by byla tímto útokem ohrožena. Obranou proti 51 % útoku může být dostatečná decentralizace sítě těžařů / validátorů a obecně účastníků konsensu. [108]

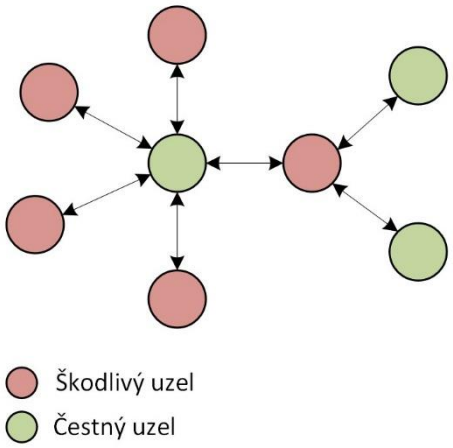
Long-range útok

Long-range útok (Long-range Attack) je typ útoku zaměřený na konsensní algoritmy založené na Proof of Stake, kde útočník, který například v minulosti vlastnil významný podíl kryptoměny sítě, vytvoří alternativní historii sítě neboli řetězec bloků

začínající v dřívějším bodě, aby poté zpochybnil pravdivost hlavního řetězce. Tento alternativní řetězec útočník prodlužuje až do současnosti, dokud není delší než hlavní, čímž se dle základního pravidla blockchainu stává nejdelší řetězec platným. Long-range útok je obtížné detekovat, proto existují některá opatření, která mohou provedení tohoto útoku ztížit nebo znemožnit. Mezi tato opatření patří takzvané checkpoints, to jsou pevně stanovené body v historii, které nelze měnit, dále požadavek na minimální stáří mincí uzamčených mincí nebo náhodný výběr. [109] [110]

Eclipse útok

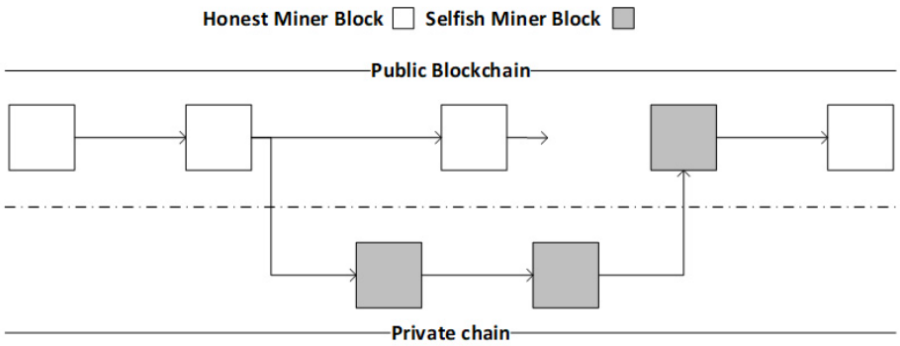
Eclipse útok (Eclipse Attack) je typem útoku na distribuovanou síť, při které útočník izoluje konkrétní uzel od zbytku sítě tak, že ovládne všechna jeho přímá spojení. Útočník nejdříve naváže s uzlem spojení například pomocí skupiny vytvořených škodlivých uzlů a izoluje jej kontrolou většiny přímého spojení. Tímto způsobem může poté manipulovat a podvrhovat informace, které uzel odesílá a přijímá nebo provádět různé další útoky jako je třeba double-spending. Pro ochranu sítí před Eclipse útoky mohou pomoci implementovaná opatření ztěžující možnost ovládnutí spojení cílového uzlů, jako je náhodný výběr, kdy se uzel při každé synchronizaci připojuje k ostatním uzlům náhodně, zvýšení požadovaného počtu připojení nebo implementace reputačního systému. Eclipse útok se může vyskytovat u většiny konsensních mechanismů, kde dochází k peer-to-peer komunikaci. [111]



Obrázek 19 – Eclipse útok (vlastní zpracování)

Selfish mining

Selfish mining je útok primárně zaměřený na Proof of Work konsensní algoritmy, jehož cílem je pro útočníka získat větší odměnu tajnou těžbou než ostatní poctiví těžaři v síti. Útočník (nebo skupina) začne tajně těžit bloky, aniž by je zveřejňoval v síti, místo toho vytváří svůj vlastní privátní řetězec, o kterém ostatní těžaři v síti nevědí. Tímto způsobem pokračuje v tajné těžbě ve snaze získat náskok před hlavním řetězcem. Když útočník získá dostatečný náskok, zveřejní svůj privátní řetězec a ostatní uzly, které se řídí pravidlem nejdelšího řetězce, jej přijmou jako hlavní a útočník získá odměny za těžbu bloků. Úspěšný útok naruší férovost v získávání odměn za těžbu, způsobí ztrátu důvěry v síti a pokles hodnoty. [112]



Obrázek 20 – Selfish mining [113]

Nothing-at-Stake problem

Nothing-at-Stake je problém spojený s konsensními algoritmy Proof of Stake a spočívá v tom, že v průběhu mohou vznikat různé verze blockchainu (tzv. forks) a validátoři nemají důvod současně nepodpořit všechny forky najednou, jelikož například na rozdíl od Proof of Work, kde těžaři musí vynaložit energii a výpočetní výkon k nalezení bloku, což by při podpoře více forků znamenalo rozdělit svůj výkon, v PoS žádné takové omezení není. Nothing-at-Stake problém může vést k nejistotě ohledně správné verze blockchainu a ztížení dosažení konsensu, to může vést ke ztrátě důvěryhodnosti a hodnoty kryptoměny. Tento problém je řešen v novějších implementacích Proof of Stake ztrátou podílu nebo jistou formou penalizace v případě podpory více forků blockchainu. [114]

Timejacking útok

Timejacking je útok mířený na manipulaci s časovými značkami, který má za cíl způsobit nekonzistenci v řetězci, aby se zdálo, že blok byl vytvořen dříve nebo později a ovlivnit tak proces těžby či sázek a distribuci odměn, nebo se útočník může snažit ovlivnit časové servery, které uzly používají k synchronizaci času. Nekonzistence v řetězci mezi různými verzemi může vést k forku sítě a případnému double-spend útoku nebo zpožďování a ztrátě transakcí. Dále může úspěšný Timejacking útok zvýšit zranitelnost vůči jiným útokům, jako je například 51 % nebo Sybil útok. Timejacking je relevantní pro mechanismy, které závisí na přesném časování a synchronizaci uzlů v síti. Ačkoliv se jedná o vážné riziko, existují jistá opatření, která mohou šanci na úspěšné provedení tohoto typu útoku eliminovat. Mezi tato opatření patří použití více časových serverů pro synchronizaci času v síti, nebo zavedení bezpečnostních prvků, které detekují a odmítnou bloky s podezřelými časy. [115]

Denial of Service

Denial of Service (DoS) a Distributed Denial of Service (DDoS) jsou útoky na síť nebo jednotlivé uzly, jejichž cílem je způsobit přetížení a zamezit tak provádění transakcí, připojení uzlů, nebo omezení schopnosti účastnit se konsensu. Při DoS útoku může útočník zaplavovat síť velkým množstvím nových nelegitimních transakcí, které vedou k zpožďování nebo neschopnosti zpracovat legitimní transakce, čímž dochází k snížení celkové výkonnosti sítě a ovlivnění její spolehlivosti a důvěryhodnosti. Útočníci mohou také využít DoS útok k zvýšení podílu na konsensu, čímž se zvyšuje riziko útoku typu 51 %. Proti DoS útoku se sítě mohou bránit technikami, jako je například rate limiting (omezení příchozích a odchozích dat), přijímání pouze ověřených transakcí, nebo zavedení bezpečnostních mechanismů detekujících podezřelé chování. [116]

Koluzní útok

Koluzní útok je strategie, při které se skupina uzlů v síti domluví, aby získala kontrolu nad konsensem. Toho může být dosaženo zejména v sítích využívající mechanismy založené na Proof of Stake, kde velký počet uzlů vlastnících většinu aktiva sítě může potenciálně manipulovat s pravidly a transakcemi ve svůj prospěch. Koluzní útoky jsou významnou hrozbou pro decentralizované systémy a mohou narušit jejich důvěryhodnost a bezpečnost. Obranou proti těmto útokům může být rozptýlení moci

mezi větší počet uzlů, náhodný výběr tvůrců bloku, různé typy ekonomických sankcí pro uzly, které se o koluzní útok pokusí, nebo systémy detekce a prevence. [117]

4.1.2 Centralizace

Centralizace je jedním z hlavních rizik v kontextu konsensních mechanismů, jelikož je v rozporu s hlavním cílem decentralizace, což je nezávislost (autonomie), transparentnost, bezpečnost a spravedlnost. Centralizace může všechny tyto vlastnosti sítě negativně ovlivnit a způsobit:

- Zneužití moci – koncentrace moci mezi malou skupinou uživatelů může vést ke střetu zájmů a zneužití v podobě změny pravidel, cenzury, vlastnímu obohacení a jinému zvýhodnění
- Nedůvěryhodnost – nedostatek důvěry ze strany ostatních uživatelů sítě v dosažení konsensu nezávislým způsobem, což může mít za následek odliv uživatelů
- Snížení bezpečnosti – vlivem centralizace může dojít k výskytu slabin, které lze zneužít k útoku na síť (51 % útok, cenzura, double-spending)
- Snížení odolnosti – závislost na malé skupině uživatelů snižuje odolnost proti případným chybám nebo neetickému chování

Je důležité se tímto rizikem zabývat a zvážit jeho možné dopady při volbě či návrhu konsensního mechanismu pro distribuovanou síť. Eliminace centralizace lze dosáhnout prostřednictvím podpory principů decentralizace, transparentnosti a spravedlnosti jako mohou být:

- Zvýšení počtu účastníků konsensu – odstraněním případných bariér pro vstup nebo větší motivací uživatelů (spravedlivé ekonomické pobídky)
- Rovnoměrné rozdělení zdrojů – možná opatření omezující sdružování výpočetního výkonu nebo hlasovací síly (pools)
- Omezení vzniku vlivných účastníků – pravidla pro dynamické úpravy odměn (úměrně menší odměny se zvyšujícím se podílem v síti)
- Více vrstev konsensu – vícevrstvá konsensní architektura, kde jsou jednotlivé vrstvy optimalizovány ke svým účelům

- Demokratický způsob rozhodování o vývoji – aktivně zapojit účastníky konsensu do rozhodování o vývoji sítě a umožnit demokratické hlasování v případě přijetí navrhovaných změn
- Transparentnost – umožnit účastníkům sítě auditovatelnost konsensního mechanismu a celého procesu dosažení shody

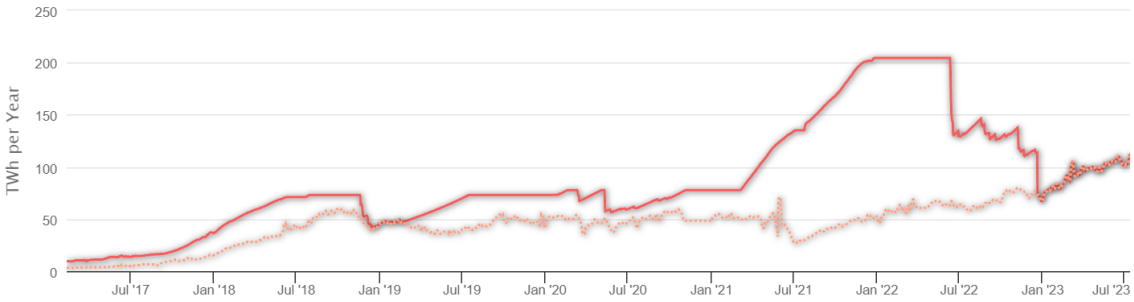
4.1.3 Energetická náročnost a dopad na životní prostředí

Energetická náročnost a dopad na životní prostředí jsou rizika spojená zejména s tradičními mechanismy založenými na Proof of Work jako důsledek způsobu, jakým účastníci konsensu docházejí ke shodě. Tato rizika mohou mít dopad na volbu konsensního mechanismu nejen z hlediska technického, ale i právě ekologického. Spotřeba velkého množství elektrické energie v procesu dosažení konsensu má negativní dopady na životní prostředí v podobě vyšších emisí skleníkových plynů v případě, že je získávána z neobnovitelných zdrojů, což je v rozporu s globální snahou o snížení emisí. Samozřejmě také samotná cena elektrické energie může vést k centralizaci těžebního výkonu na jednom místě či státě, kde potom těžaři podléhají místní legislativě.

Je tedy důležité zvážit, zda je energetická náročnost Proof of Work mechanismů oprávněná výměnou za vysokou míru decentralizace a bezpečnosti. Toto je právě jedním z důvodů, proč vznikly a vznikají další alternativní způsoby dosažení konsensu, které se zaměřují na to, aby zanechávaly co nejmenší uhlíkovou stopu, ovšem za cenu kompromisních řešení v již zmíněných oblastech bezpečnosti a decentralizace.

Způsoby řešení energetické náročnosti mohou být:

- Využití obnovitelných zdrojů energie – motivace těžařů v Proof of Work sítích využívat obnovitelné zdroje
- Lepší energetická efektivita těžebního hardwaru – výpočetní hardware se stává čím dál tím více energeticky efektivnějším
- Volba energeticky nenáročného konsensního mechanismu



Obrázek 21 – Minimální a průměrná spotřeba energie Bitcoinu (PoW) v období 2017-2023 [118]

4.1.4 Škálovatelnost a výkonnost

Škálovatelnost a výkonnost jsou klíčovými faktory, které ovlivňují schopnost konsensních mechanismů zvládat rostoucí počet uživatelů a transakcí v síti, aniž by docházelo k degradaci výkonu. Pokud síť není dostatečně výkonná a škálovatelná, může to vést k následujícím problémům:

- Zpožďování transakcí – pokud mechanismus nedokáže zpracovat velký počet transakcí, bude docházet k jejich zpožďování
- Vyšší transakční poplatky – s nárůstem nezpracovaných transakcí v síti může docházet k tomu, že uživatelé budou navyšovat poplatky za to, aby jejich transakce byla prioritně zpracována
- Omezení využitelnosti a rozvoje – jestli mechanismus není schopen zpracovávat narůstající počet transakcí, může to vést k omezení využitelnosti sítě a budoucímu rozvoji například v oblasti dApps nebo smart kontraktů
- Snížení bezpečnosti – s maximálním vytížením sítě může docházet k útokům a snížení bezpečnosti například zahlcením nelegitimními transakcemi

S adopcí technologie blockchainu je čím dál tím důležitější, aby byly sítě schopné transakce efektivně zpracovávat. Klasickým případem nedostatečné škálovatelnosti je Proof of Work a Bitcoin, který dokáže zpracovávat pouze velmi omezený počet transakcí za sekundu, což při vyšší síťové aktivitě reálně vede ke zpožďování transakcí, vysokým poplatkům a omezení v určitých oblastech a aplikacích.

Mechanismy založené na Proof of Stake řeší problém škálovatelnosti eliminací nutnosti využívat výpočetní výkon, což umožňuje rychlejší potvrzování transakcí, nicméně za cenu nižší bezpečnosti a decentralizace. V ideálním případě by totiž měl mechanismus být schopen zpracovávat velké množství transakcí, aniž by právě docházelo ke kompromisu v jiných oblastech, jako je zmíněná decentralizace a bezpečnost.

Z technického hlediska závisí faktory škálovatelnosti a výkonnosti blockchainových konsensních mechanismů na:

- Kapacita bloku – velikost bloku omezuje počet transakcí, které do něj lze zahrnout, což ovlivňuje maximální počet transakcí za vteřinu
- Čas vytvoření bloku – doba potřebná pro vytvoření nového bloku je rovněž faktorem, který omezuje počet zpracovaných transakcí za vteřinu
- Komunikace mezi účastníky – při vyšším počtu uzlů v síti je potřeba informace šířit mezi více účastníků, způsob komunikace tedy hraje roli v oblasti škálovatelnosti

V posledních letech se objevují nové technologie a způsoby řešení, které se snaží problémy škálovatelnosti zlepšit. Patří mezi ně:

- Implementace více vrstev – jedná se o implementaci další vrstvy v síti nad stávající, která zahrnuje protokoly a technologie, jako je například Lightning Network u Bitcoinu, což umožňuje provádět transakce mimo hlavní řetězec blockchainu, které jsou poté po nějakém časovém úseku do hlavního blockchainu jednotně zaznamenány [119]
- Sharding – technologie shardingu, kterou využívá například již zmiňovaný MultiversX se svým Secure Proof of Stake mechanismem, umožňuje rozdělení sítě na menší segmenty, které zpracovávají transakce paralelně, což znatelně zvyšuje škálovatelnost

4.1.5 Ekonomická rizika

Ekonomická rizika jsou další důležitou součástí konsensních mechanismů v kontextu kryptoměn, protože hrají roli v udržitelnosti a spravedlnosti celé systému. Konsensní mechanismy musejí být navrženy tak, aby jeho účastníci byli ekonomicky

motivováni se jej účastnit, čímž zajišťují stabilitu a bezpečnost sítě. Při volbě nebo návrhu konsensního mechanismu je důležité brát tyto rizika v potaz a snažit se je minimalizovat. Rizika mohou být následující:

- Nerovnoměrné rozdělení odměn – může způsobit nerovnováhu mezi účastníky a následnou centralizaci
- Slabá ekonomická motivace – může dojít k tomu, že menší skupina účastníků konsensu bude kontrolovat většinu sítě, riziko úspěšného útoku je potom vysoké
- Inflace / deflace – nestabilita hodnoty aktiva sítě
- Vysoké náklady na provoz – mechanismy vyžadující vysoké provozní náklady mohou vést k centralizaci zdrojů a stát se pro ostatní bariérou pro účast na konsensu
- Volatilita cen aktiv – prudké výkyvy hodnot (zejména pokles) aktiva sítě mohou vést ke ztrátě motivace se konsensu účastnit

4.2 Kritéria hodnocení

Bezpečnost (Security, SEC)

Bezpečnost je zásadní kritérium hodnocení mechanismů konsensu, které se vztahuje na úroveň odolnosti mechanismu proti útokům, škodlivému chování a dalším bezpečnostním hrozbám. Bezpečnost mechanismu je nanejvýš důležitá, jelikož úspěšný útok může vést ke dvojímu utrácení, ztrátě prostředků a dalším nežádoucím aktivitám.

K zajištění bezpečnosti je nezbytné, aby mechanismus používal silné kryptografické algoritmy a zabezpečené hashovací funkce. Mimo to také silně závisí na velikosti sítě a počtu validátorů / těžařů, kteří se konsensu účastní. Čím větší je velikost sítě, tím těžší pro útočníka je ji ovládnout. Stejné je to s validátory / těžaři, s jejich rostoucím počtem se síť stává více decentralizovanou a tím odolnější proti útokům.

Celkově je bezpečnost kritickým kritériem při hodnocení mechanismů konsensu, jelikož vysoká úroveň zabezpečení s sebou mimo jiné přináší důvěru uživatelů a zaručuje širší přijetí.

Klasifikace	Hodnocení (rozsah bodů)	Deskripce
Nízká	1 - 4	Mechanismus s nízkou úrovní bezpečnosti je obecně považován za zranitelný vůči široké škále potencionálních útoků, což zvyšuje pravděpodobnost úspěšných zlomyslných akcí. Tyto mechanismy mají často nedostatečnou redundancí nebo slabá bezpečnostní opatření.
Střední	5 - 7	Mechanismus se střední úrovní zabezpečení má zavedena určitá bezpečnostní opatření, ale stále existují zranitelná místa, která by mohla být potencionálně zneužita sofistikovanějším nebo koordinovaným útokem. Riziko úspěšného útoku je nízké, ale nezanedbatelné. Síť je schopna odolat útokům omezeného počtu uzlů (zdrojů) ovládaných jednou entitou nebo skupinou.
Vysoká	8 - 10	Mechanismus s vysokou úrovní zabezpečení má implementována přísná bezpečnostní opatření, je navržen tak, aby byl vysoce odolný proti jakémukoliv potencionálnímu útoku. Riziko úspěšného útoku je velmi nízké a síť je schopna odolat širokému spektru zlomyslných akcí. Síť je decentralizovaná, žádná entita nebo skupina nekontroluje její významnou část.

Tabulka 3 – Klasifikace úrovní bezpečnosti konsensních mechanismů

Decentralizace (Decentralization, DEC)

Úroveň decentralizace je měřítko distribuce moci a kontroly mezi jednotlivé účastníky sítě. Vysoká míra decentralizace je žádoucí v tom, aby zabránila jedinému subjektu nebo malé skupince činit rozhodnutí, která by ovlivnila celou síť.

Jednou z možností určení míry decentralizace je analýza počtu uzlů účastnících se konsensu, vyšší počet ukazuje na decentralizovanější síť. Dalším způsobem je rozložení podílu nebo těžební síly mezi uzly, rovnoměrné rozložení naznačuje větší decentralizaci.

Decentralizace je ve mechanismu konsensu důležitá, jelikož zajišťuje, že síť není řízená jednou entitou, čímž se stává odolnější proti útokům či selhání. Vyšší úrovni decentralizace lze dosáhnout spravedlivým rozdělením moci a odměn mezi uzly a nastavení takových podmínek, které budou jednotlivcům bránit v příliš velkém vlivu na síť.

Klasifikace	Hodnocení (rozsah bodů)	Deskripce
Centralizovaný	1 - 4	Mechanismus je řízen jedním subjektem nebo malou skupinou subjektů, entita má plnou kontrolu nad sítí a může libovolně měnit pravidla.
Semi-centralizovaný	5 - 7	Do procesu konsensu je zapojen větší počet subjektů, ale stále se zde vyskytuje dominantní subjekt nebo malá skupina subjektů, kteří mají nad sítí významnou kontrolu – existuje určitá úroveň centralizace.

Decentralizovaný	8 - 10	Konsensu se účastní velký počet různorodých subjektů, neexistuje žádný jednotlivý subjekt nebo skupina, která by měla významnou kontrolu nad sítí. Změny jakýchkoliv pravidel vyžadují konsensus významné části uzlů sítě.

Tabulka 4 – Klasifikace úrovní decentralizace konsensních mechanismů

Model sítě (Network Model, NM)

Model sítě udává, jak spolu uzly v distribuovaném systému komunikují a synchronizují své stavy, což je klíčové pro dosažení konsensu. Efektivní komunikace je důležitá pro zajištění rychlého a spolehlivého sdílení informací a může ovlivnit celkovou efektivitu, latenci a výkon sítě. Konkrétně se modely sítě zaměřují na zpoždění a doručení zpráv mezi jednotlivými uzly. Model sítě je důležitý faktor, který může ovlivnit, jak dobře se daný konsensní mechanismus vypořádá s různými typy problémů.

Volba modelu závisí na konkrétních požadavcích a potřebách sítě, jako je naléhavost na komunikaci, požadavky na dobu odezvy a povaha komunikace.

Klasifikace	Hodnocení (rozsah bodů)	Deskripce
Synchronní	6	Synchronní model má jasně stanovenou dobu pro doručení zprávy, což může být pro konsensus jednodušší, je zde ovšem riziko selhání v případě, že zpráva ve stanoveném čase nedorazí.
Asynchronní	8	Asynchronní model nemá žádná specifická omezení pro doručení zprávy, zvládne jakékoliv zpoždění, což jej činí odolný vůči chybám, ovšem jedná se o velmi složitý model na implementaci.
Částečně synchronní	10	Částečně synchronní model je kombinací výhod synchronního a asynchronního modelu, má stanovenou dobu pro doručení zpráv, ale je navržen tak, aby zvládal situace, kdy tato časová omezení nejsou dodržena.

Tabulka 5 – Klasifikace typů modelu sítě

Škálovatelnost (Scalability, SCA)

Škálovatelnost je schopnost konkrétního konsensního mechanismu zpracovat rostoucí počet transakcí nebo uživatelů, aniž by došlo ke snížení celkové výkonnosti sítě. Škálovatelný mechanismus by měl být schopen zvládnout rostoucí zátěž bez ztráty výkonu, decentralizace a bezpečnosti. Tato schopnost je zásadní, jelikož přímo ovlivňuje počet transakcí, které lze v určitém časovém rámci zpracovat. Nízká

škálovatelnost může vést k zahlcení sítě a pomalému zpracování transakcí a celkovému výkonu sítě.

Škálovatelnost je ovlivněna různými faktory, včetně samotného návrhu mechanismu konsensu, topologie sítě, komunikace a základní architektury. K hodnocení škálovatelnosti dochází z hlediska schopnosti zvládnout rostoucí objemy transakcí nebo uzlů při zachování výkonnosti, zabezpečení a decentralizace.

Klasifikace	Hodnocení (rozsah bodů)	Deskripce
Nízká	1 - 4	Mechanismus s nízkou škálovatelností není schopen efektivně řídit nárůst počtu transakcí nebo uzlů, v období vysoké síťové aktivity je síť neefektivní, dochází k výraznému zpožďování transakcí a vysokým poplatkům za jejich zpracování.
Střední	5 - 7	Mechanismus se střední škálovatelností je schopen efektivně bez problému řídit určitou míru nárůstu počtu transakcí nebo uzlů bez ztráty výkonnosti, ale v období vysoké síťové aktivity stále může docházet ke zpožďování zpracování transakcí a zvýšení poplatků.
Vysoká	8 - 10	Mechanismus s vysokou škálovatelností dokáže bez problému zpracovat nárůst velkého počtu transakcí nebo uzlů bez výrazného snížení výkonnosti sítě. Síť zůstává při výrazném zatížení efektivní bez zpožďování transakcí či zvyšování poplatků

Tabulka 6 – Klasifikace úrovní škálovatelnosti konsensních mechanismů

Transakční propustnost (Transaction Per Second, TPS)

Transakční propustnost je schopnost konsensního mechanismu zpracovávat transakce nebo operace v daném časovém rámci (obvykle počet transakcí za vteřinu – TPS), určuje rychlost, jakou lze transakce přidávat do účetní knihy.

Existuje několik faktorů, které mohou propustnost konsensního mechanismu ovlivnit, včetně šířky pásma sítě, výpočetního výkonu nebo velikosti každé transakce. Mechanismy vyžadující provádění rozsáhlých výpočtů nebo ověřování každé jedné transakce mohou mít nižší propustnost než mechanismy s jednoduššími ověřovacími způsoby.

Propustnost je důležitým kritériem hodnocení konsensních mechanismů, jelikož poskytuje pohled na to, jak dobře mechanismus zvládne vyšší objemy transakcí či operací v různých scénářích. Tato informace je kriticky důležitá pro aplikace jako jsou například platební systémy nebo obchodní platformy, které vyžadují zpracovávání vysokého počtu transakcí za vteřinu.

Klasifikace	Hodnocení (rozsah bodů)	Deskripce
Nízká	1 - 4	Mechanismus je schopen zpracovat malý počet transakcí za vteřinu (<100 TPS), to může mít za následek delší dobu potvrzení, vysoké poplatky a nižší výkon sítě. Mechanismy s nízkou propustností nejsou vhodné pro vysokofrekvenční aplikace.
Střední	5 - 7	Mechanismus je schopen zpracovat střední počet transakcí (100-1000 TPS), je schopen zvládnout vyšší síťový provoz, stále ovšem může docházet k přetížení ve vysoké síťové aktivitě.
Vysoká	8 - 10	Mechanismus dokáže zpracovat vysoký počet transakcí (>1000 TPS), je navržen tak, aby zvládal vysokou úroveň síťového provozu bez zahlcení nebo snížení výkonnosti sítě.

Tabulka 7 – Klasifikace úrovní propustnosti konsensních mechanismů

Finalita (Finality, FIN)

Finalita (konečnost) zajišťuje, že jakmile jsou transakce nebo blok potvrzeny, nelze je žádným způsobem zrušit nebo pozměnit bez opětovného konsensu sítě. Finalita poskytuje uživatelům i vývojářům jistotu, že transakce jsou trvale zaznamenány v účetní knize a jsou sítí považovány za potvrzené. Jedná se o důležitý aspekt konsensních mechanismů, protože zajišťuje integritu, důvěryhodnost a neměnnost dat.

Klasifikace	Hodnocení (rozsah bodů)	Deskripce
Probabilistická	8	Existuje malá pravděpodobnost, že by potvrzená transakce nebo blok mohly být zrušeny nebo pozměněny. Pravděpodobnost, že transakce nebo blok budou považovány za konečné se v čase zvyšuje.
Deterministická	10	Jakmile jsou transakce nebo blok potvrzeny, nelze je vrátit zpět ani žádným způsobem pozměnit, jsou považovány za konečné.

Tabulka 8 – Klasifikace typů finality konsensních mechanismů

Energetická účinnost (Energy Efficiency, EE)

Energetická účinnost je kritérium hodnocení na základě množství energie potřebné k udržení bezpečnosti sítě a konsensního mechanismu. Tento aspekt ovlivňuje udržitelnost a dopad celého systému na životní prostředí. Energetická účinnost se měří jako množství energie potřebné k potvrzení transakce nebo k provozu sítě za jednotku času. Energeticky účinnější mechanismy vyžadují k provozování sítě menší množství energie, což vede k nízkým nákladům a menší uhlíkové stopě.

Klasifikace	Hodnocení (rozsah bodů)	Deskripce
Nízká	1 - 4	Mechanismy k udržení konsensu spotřebovávají vysoké množství energie, to může být ovlivněno faktory, jako jsou požadavky na vysoký výpočetní výkon, ukládání dat nebo vysoká komunikační režie.
Střední	5 - 7	Mechanismy k udržení konsensu spotřebovávají mírné množství energie, mají optimalizované požadavky na výpočetní výkon, ukládání dat nebo komunikační režii tak, aby se spotřeba energie snížila.
Vysoká	8 - 10	Mechanismy k udržení konsensu vyžadují minimální množství energie, jsou navrženy tak, aby spotřeba byla co možná nejnižší.

Tabulka 9 – Klasifikace úrovní energetické účinnosti konsensních mechanismů

Model protivníka (Adversary Model, AM)

Model protivníka určuje úroveň odolnosti konsensního mechanismu proti chybám nebo zlomyslnému chování, které je bezpečně schopen tolerovat bez narušení konsensu, pomáhá určit, jak robustní a bezpečný daný mechanismus je vůči různým typům útoků a celkové snaze o narušení konsensu v síti.

Všeobecně platí, že je model vyjádřen rovnicí $n = k\,f + 1$, kde n vyjadřuje celkový počet uzlů nebo obecně zdrojů sítě (výpočetní výkon, tokeny a další), f je maximální počet zlomyslných uzlů (nebo zdrojů útočníka), které lze tolerovat a k je koeficient určující stupeň redundance v systému (každá hodnota koeficientu k určuje jinou úroveň odolnosti).

Toto kritérium je velmi důležité, protože v decentralizovaných systémech je nutné předpokládat, že budou existovat aktéři, kteří selžou nebo se pokusí proces narušit. Jedná se tedy o klíčovou součást hodnocení a zajišťování bezpečnosti konsensních mechanismů v decentralizovaných systémech.

Klasifikace	Hodnocení (rozsah bodů)	Deskripce
Nízká n = 4f + 1 (< 25 %)	6	Mechanismy s nízkou úrovní odolnosti mohou tolerovat až 25 % zlomyslného chování v síti a stále dosáhnout konsensu. Mechanismy s touto úrovní odolnosti je vhodné využívat v prostředí, kde je nižší pravděpodobnost zlomyslného chování.
Střední n = 3f + 1 (< 33 %)	8	Mechanismy se střední úrovní odolnosti mohou tolerovat až 33 % zlomyslného chování v síti bez narušení konsensu. Tato úroveň poskytuje rovnováhu mezi redundancí a odolností.

Vysoká n = 2f + 1 (< 50 %)	10	Mechanismy s vysokou úrovní odolnosti mohou tolerovat až 50 % zlomyslných akcí v síti bez narušení konsensu. Tato úroveň odolnosti je vhodná pro robustní sítě, které vyžadují vysokou toleranci k chybám nebo zlomyslnému chování.

Tabulka 10 – Klasifikace úrovní odolnosti konsensních mechanismů proti zlomyslnému chování v síti

4.3 Zranitelnost proti kybernetickým útokům

Tabulka 11 níže poskytuje obecný přehled zranitelnosti a náchylnosti vybraných konsensních mechanismů vůči různým typům kybernetických útoků. Kromě těchto specifických zranitelností můžou být všechny mechanismy náchylné vůči Eclipse, Timejacking a dalším typům útoků, které se pokouší manipulovat s časem a způsobovat nekonzistenci mezi uzly.

Žádný konsensní mechanismus není úplně imunní vůči všem typům útoků. Před jeho výběrem a implementací v decentralizované síti je důležité nejdříve provést bezpečnostní analýzu, zvážit specifické zranitelnosti daného mechanismu a přijmout opatření k minimalizaci bezpečnostních rizik.

Algoritmus	Příklady implementace	Typy útoků
PoW	Bitcoin Ethereum (pre-PoS) Litecoin [120]	51 % útok, Selfish mining
DPoW	Komodo	Selfish mining
PoS	Ethereum 2.0 Cardano [121]	Nothing-at-Stake, Long range
DPoS	EOS TRON [122] BitShares	Nothing-at-Stake, Long range, Koluzní útok
LPoS	WAVES	Nothing-at-Stake, Long range, Koluzní útok
SPoS	MultiversX	N/A
PoI	NEM	N/A
PoC	Burstcoin [123]	51 % útok
PoST	Filecoin Chia [124]	51 % útok
PoR	Storj	51 % útok

PoB	Slimcoin	51 % útok
PoAc	Decred	N/A
PoET	Hyperledger Sawtooth	Sybil
PoAu	Kovan VechainThor [125]	Koluzní útok
PBFT	Hyperledger Sawtooth	Sybil, DoS
DBFT	NEO	Koluzní útok
ABFT	Hedera Hashgraph	N/A
FBA	Stellar XRP [126]	N/A
Paxos	Google Chubby	Sybil, DoS a DDoS
FPaxos	-	Sybil, DoS a DDoS
Raft	Quorum Hyperledger Fabric [127]	Sybil, DoS a DDoS
Tangle	IOTA	Parasite Chain Attack [128]

Tabulka 11 – Přehled zranitelnosti mechanismů vůči kybernetickým úrokům

4.4 Hodnocení mechanismů na základě stanovených kritérií

Tato kapitola se zabývá komparativním hodnocením, které je přehledně uvedeno v tabulce 12, vybraných konsensních mechanismů na základě dříve stanovených klíčových kritérií, která jsou zásadní pro úspěšnou implementaci a udržitelnost systému.

Bezpečnost

Vysoce bezpečné mechanismy: PoW, DPoW, PoS, LPoS, SPoS, PoI, PoAc, ABFT, FBA (SCP) a Tangle lze zařadit mezi nejbezpečnější mechanismy. Výhodou těchto mechanismů je jejich robustní odolnost proti široké škále útoků, díky tomu jsou ideální pro využití ve veřejných sítí, kde se potencionálně může vyskytovat vysoký počet zlomyslných aktérů. PoW je zabezpečen tím, že vyžaduje, aby těžaři vykonávali výpočetně náročnou práci, čímž se jakékoliv útoky stávají extrémně nákladné. DPoW přidává k tradičnímu PoW dodatečnou vrstvu zabezpečení v podobě notářského

systému na sekundárním blockchainu, PoS pro zabezpečení využívá tokeny sítě, které slouží jako kolaterál, kterým nahrazují nutnost využívat výpočetní výkon k účasti na konsensu. LPoS je varianta PoS, která zvyšuje úroveň zabezpečení tím, že navíc umožňuje držitelům tokenů pronajmout své tokeny pro těžbu jiným uzlům sítě. SPoS používá sharding a omezuje možnost, aby jednotliví držitelé velkého množství tokenů mohli ovládnout síť, snaží se v podstatě dosáhnout rovnoměrnějšího a spravedlivějšího rozdělení moci. PoI zohledňuje kromě uzamčených tokenů i celkovou aktivitu v síti, to jej činí více bezpečným než tradiční PoS. PoAc kombinuje prvky PoW a PoS s ohledem na energetickou účinnost PoW části konsensu. ABFT je mechanismus odolný vůči byzantským chybám v asynchronním prostředí a využívá sofistikované mechanismy pro řešení konfliktů mezi uzly sítě, čímž je odolný vůči široké škále útoků. FBA (SCP) umožňuje uzlům v síti si vybrat vlastní skupinu důvěryhodných uzlů, se kterými se chce shodnout na aktuálním stavu účetní knihy. Tangle je konsensní mechanismus v alternativní datové struktuře DAG, nevyžaduje výpočetní výkon, místo toho umožňuje paralelní přidávání transakcí, kdy každá nová transakce musí potvrdit dvě předchozí, což tento mechanismus činí vysoce bezpečným. Je nutné dodat, že ABFT, FBA a Tangle jsou poměrně nové mechanismy, které jsou oproti mechanismům založených na důkazech velmi komplexní a náročné na implementaci.

Mechanismy se střední bezpečností: DPoS, PoC, PoST, PoR, DBFT představují mechanismy se střední úrovní bezpečností. Tyto mechanismy mohou nabízet kompromis mezi bezpečností, decentralizací, výkonem/škálovatelností a stále být dostatečně vhodnou volbou pro využití ve veřejných sítích. DPoS se řadí mezi mechanismy se střední bezpečností z toho důvodu, že omezuje počet validátorů na velmi nízký počet, což zvyšuje náchylnost ke koluzním útokům. PoC a mechanismy na něm založené jako jsou PoST a PoR nejsou široce adoptovány, úložný prostor je v dnešní době velmi levný a vzhledem k tomu, že každé zařízení úložiště využívá, by jejich adopce vedla k masivnímu rozšíření malwaru, který by jej zneužil ve prospěch těžby a byl by velmi obtížně detekovatelný (na rozdíl od PoW malwaru). DBFT je ve skupině střední bezpečnosti ze stejného důvodu jako DPoS, rovněž využívá pouze nízký počet delegátů volených na základě vlastnictví tokenů, což s sebou přináší stejná bezpečnostní rizika v podobě koluzních útoků.

Mechanismy s nízkou bezpečností: PoB, PoET, PoAu, PBFT, Paxos, FPaxos a Raft představují mechanismy s nižší bezpečností. Tyto mechanismy jsou obvykle vhodné pro privátní nebo konsorciální sítě, kde jsou účastníci sítě důvěryhodní. PoB je

jediným mechanismem ze skupiny algoritmů založených na důkazech využívaným ve veřejných sítích, který je řazen ve skupině s nízkou bezpečností. Je to z ekonomických důvodů, protože uživatel není dostatečně motivován kryptoměnu pálit, jelikož spálení velkého množství kryptoměny jej uvede do vysoké počáteční ztráty bez jakékoliv jistoty, že v budoucnu bude v zisku, to způsobuje, že je síť nedostatečně agilní a náchylná k 51 % útoku. PoET se musí spoléhat na specializovanou výpočetní techniku pro spravedlivé losování, což by jej při nasazení v nedůvěryhodném prostředí silně vystavovalo Sybil útokům. PoAu je závislý na předem vybrané skupince validátorů, která síť řídí, čímž je centralizovaný a automaticky se stává zranitelný proti koluzním útokům. PBFT, Paxos, Fast Paxos a Raft jsou všechno mechanismy určené pro nasazení v důvěryhodném prostředí malých sítí, kde dokážou efektivně fungovat i v případě selhání, ovšem pro využití ve veřejných sítích jsou silně nevhodné z důvodů zranitelnosti proti široké škále kybernetických útoků.

Decentralizace

Decentralizované mechanismy: PoW, DPoW, PoS, SPoS, PoI, PoC, PoST, PoR, PoAc, PoET, ABFT, FBA (SCP) lze zařadit do skupiny decentralizovaných mechanismů. Tato skupina obecně nevyžaduje centrální autoritu a využívá různé mechanismy a metody pro motivaci účastníků na udržování sítě. Decentralizované mechanismy jsou většinou využívány ve veřejných sítích a obecně v nedůvěryhodném prostředí. Výjimkou je PoET, který využívá decentralizovaný způsob výběru validátora (hardware pro náhodný časový interval) v privátním nebo konsorciálním blockchainu. PoW a DPoW jsou decentralizované, jelikož umožňují libovolnému uzlu s výpočetním výkonem se účastnit konsensu. Podobně je na tom PoS s uzamčením tokenů, varianty PoS jako jsou SPoS, PoI navíc ještě zohledňují reputaci uzlů v síti. PoC a mechanismy na něm založené, jako jsou PoST a PoR, jsou svou povahou rovněž decentralizované, jelikož umožňují širokému spektru uživatelů s kapacitním prostorem se účastnit konsensu. Uzly v ABFT jsou autonomní a rozhodují se na základě informací, které přijímají od ostatních uzlů, je zajištěno, že žádná skupina nebo jednotlivec nemůže ovlivnit stav účetní knihy. FBA (SCP) umožňuje vytvářet na základě více faktorů skupiny důvěryhodných kvór, které náhodně ověřují transakce a spolupracují na dosažení konsensu plně decentralizovaným způsobem.

Částečně centralizované mechanismy: DPoS, LPoS, PoB, DBFT a Tangle spadají do skupiny částečně centralizovaných mechanismů, jelikož vykazují jistý stupeň centralizace. Jak již bylo zmíněno, DPoS společně s DBFT dosahují konsensu v malém počtu delegátů, což je sice činí výkonnými, ale dají se považovat za částečně centralizované vzhledem k nízkému počtu účastníků konsensu. LPoS umožňuje pronajímat tokeny ve prospěch jiných uzlů sítě, což částečně umožňuje se účastnit konsensu menším držitelům tokenů, nicméně tento způsob může vést k centralizaci moci do rukou velkých validátorů. PoB lze označit jako částečně centralizovaný vzhledem ke svému návrhu a nedostatečným ekonomickým pobídkám. Tangle by svojí podstatou měl být decentralizovaný, ale aktuálně stále využívá koordinátora, což je centralizovaný mechanismus pro potvrzování transakcí v případě nízké síťové aktivity.

Centralizované mechanismy: PBFT, Paxos, Fast Paxos, Raft a PoAu jsou centralizované mechanismy využívané v privátních a konsorciálních sítích, kde jsou uzly důvěryhodné. Tyto mechanismy jsou schopny efektivně dosáhnout konsensu v omezeném počtu uzlů na úkor decentralizace.

Škálovatelnost a transakční propustnost

Vysoce škálovatelné mechanismy: DPoS, SPoS, PoAu, DBFT, ABFT, FBA (SCP) a Tangle je možné zařadit do skupiny vysoce výkonných mechanismů v oblasti škálovatelnosti a transakční propustnosti. DPoS, PoAu, DBFT zvyšují svoji škálovatelnost a propustnost snížením počtu účastníků konsensu na malý počet validátorů, to snižuje blocktime ovšem za cenu nižší úrovně decentralizace. SPoS implementuje sharding, což umožňuje efektivní paralelní zpracování transakcí. ABFT je škálovatelný vzhledem k povaze asynchronní komunikace a gossip protokolů, které informace sítí šíří velmi rychle. FBA (SCP) je vysoce škálovatelný díky způsobu komunikace, kdy snižuje počet potřebných zpráv k dosažení konsensu a dynamicky se měnícím kvórům, které transakce zpracovávají. Tangle z podstaty toho, že v případě nové transakce je nutné potvrdit dvě předchozí, se v případě vysoké síťové aktivity stává masivně škálovatelným.

Mechanismy se střední úrovní škálovatelnosti: PoS, LPoS, PoI lze považovat za mechanismy se střední úrovní výkonnosti eliminující výpočetně náročné operace. Vzhledem k návrhu PoS mechanismů, kdy jsou validátoři vybíráni na základě vsazené

kryptoměny (nebo dalších atributů) je škálovatelnost omezena procesem výběru. U PoET je výkonnost omezena potřebou čekat na uplynutí náhodných časových intervalů.

Mechanismy s nízkou škálovatelností: PoW, DPoW, PoC, PoST, PoR, PoB, PoAc, PBFT, Paxos, Fast Paxos, Raft patří do skupiny mechanismů s nízkou škálovatelností a transakční propustností. PoW a DPoW vyžadují v dosažení konsensu výpočetní výkon, to omezuje rychlost, s kterou lze transakce zpracovávat, to činí tyto mechanismy jedny z vůbec nejméně škálovatelných. Mechanismy využívající kapacitní prostor, jako jsou PoC, PoST a PoR mají také velmi omezenou rychlost zpracování transakcí vzhledem k potřebě číst a zapisovat data na disk. PoB se ve škálovatelnosti a propustnosti od PoW neliší, tento mechanismus vznikl pouze jen jako jeho ekologická alternativa. PoAc je sice o trochu více škálovatelný než například tradiční PoW, nicméně vzhledem k tomu, že je to hybridní mechanismus, tak ho jeho komplexnost stále řadí mezi ty méně škálovatelné. PBFT, Paxos, Fast Paxos a Raft jsou mechanismy založeny na koordinaci a komunikaci mezi uzly v síti, s nárůstem požadavků se zvyšuje i náročnost komunikace, což zabraňuje škálovatelnosti systému.

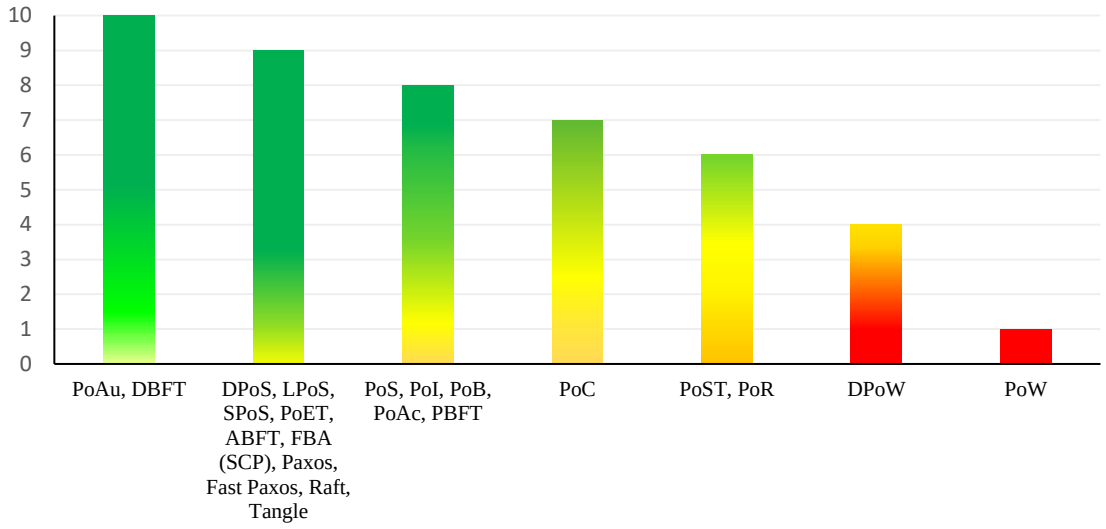
Energetická účinnost

Mechanismy s vysokou energetickou účinností: PoS, DPoS, LPoS, SPoS, PoI, PoB, PoAc, PoET, PoAu, PBFT, DBFT,ABFT, FBA (SCP), Paxos, Fast Paxos, Raft a Tangle jsou mechanismy vysoce energeticky účinné, jelikož místo výpočetního výkonu k dosažení shody využívají jiné způsoby, ať už se jedná o energeticky nenáročné formy důkazů (sázka, kapacitní prostor, pálení), shoda prostřednictvím komunikace, hlasováním, omezením počtu účastníků konsensu nebo využitím nových datových struktur jako například Tangle a Hashgraph.

Mechanismy se střední energetickou účinností: PoC, PoST a PoR jsou mechanismy s energetickou účinností na úrovni mezi PoW a PoS. U těchto mechanismů je těžba založena na množství dostupného místa na disku těžaře než na výpočetním výkonu. Proces dosažení konsensu sám o sobě není až tak energeticky náročný, ovšem samotný plotting může trvat i několik týdnů v závislosti na dostupné kapacitě a stále je potřeba energie k udržení a provozu pevných disků.

Mechanismy s nízkou energetickou účinností: PoW, DPoW jsou extrémně energeticky náročné konsensní mechanismy, jelikož k dosažení shody v síti využívají výpočetní výkon, který vyžaduje vysokou spotřebu elektrické energie. DPoW jakožto

modifikace PoW může snižovat potřebu výpočetního výkonu v primárním blockchainu, ovšem stále využívá sekundární PoW blockchain, čímž jej lze zařadit mezi málo energeticky účinné mechanismy.



Graf 2 – Srovnání konsensních mechanismů v energetické účinnosti

Algoritmus	SEC	DEC	NM	SCA	TPS	FIN	EE	AM
PoW	Vysoká	Decentr.	Částečně synchr.	Nízká	Nízká	Probab.	Nízká	n = 2f + 1
DPoW	Vysoká	Decentr.	Částečně synchr.	Nízká	Nízká	Probab.	Nízká	n = 2f + 1
PoS	Vysoká	Decentr.	Částečně synchr.	Střední	Střední	Probab.	Vysoká	n = 2f + 1
DPoS	Střední	Semi-centr.	Částečně synchr.	Vysoká	Vysoká	Probab.	Vysoká	n = 2f + 1
LPoS	Vysoká	Semi-centr.	Částečně synchr.	Střední	Střední	Probab.	Vysoká	n = 2f + 1
SPoS	Vysoká	Decentr.	Částečně synchr.	Vysoká	Vysoká	Determ.	Vysoká	n = 3f + 1
PoI	Vysoká	Decentr.	Částečně synchr.	Střední	Střední	Probab.	Vysoká	n = 2f + 1
PoC	Střední	Decentr.	Částečně synchr.	Nízká	Nízká	Probab.	Střední	n = 2f + 1
PoST	Střední	Decentr.	Částečně synchr.	Nízká	Nízká	Probab.	Střední	n = 2f + 1
PoR	Střední	Decentr.	Částečně synchr.	Nízká	Nízká	Probab.	Střední	n = 2f + 1
PoB	Nízká	Semi-centr.	Částečně synchr.	Nízká	Nízká	Probab.	Vysoká	n = 2f + 1
PoAc	Vysoká	Decentr.	Částečně synchr.	Nízká	Nízká	Probab.	Vysoká	n = 2f + 1

PoET	Střední	Decentr.	Částečně synchr.	Nízká	Střední	Probab.	Vysoká	n = 2f + 1
PoAu	Nízká	Centr.	Částečně synchr.	Vysoká	Vysoká	Determ.	Vysoká	n = 2f + 1
PBFT	Nízká	Centr.	Asynchr.	Nízká	Střední	Determ.	Vysoká	n = 3f + 1
DBFT	Střední	Semi-centr.	Částečně synchr.	Vysoká	Vysoká	Determ.	Vysoká	n = 3f + 1
ABFT	Vysoká	Vysoká	Asynchr.	Vysoká	Vysoká	Determ.	Vysoká	n = 3f + 1
FBA (SCP)	Vysoká	Decentr.	Asynchr.	Vysoká	Vysoká	Determ.	Vysoká	n = 3f + 1
Paxos	Nízká	Centr.	Asynchr.	Nízká	Nízká	Determ.	Vysoká	n = 2f + 1
FPaxos	Nízká	Centr.	Asynchr.	Nízká	Střední	Determ.	Vysoká	n = 3f + 1
Raft	Nízká	Centr.	Asynchr.	Nízká	Střední	Determ.	Vysoká	n = 2f + 1
Tangle	Vysoká	Semi-centr.	Asynchr.	Vysoká	Vysoká	Probab.	Vysoká	n = 3f + 1

Tabulka 12 – Porovnání mechanismů na základě stanovených kritérií

4.4.1 Bodové a vážené hodnocení

Kapitola Bodové a vážené hodnocení plynule navazuje na předchozí, mechanismy jsou v kontextu stanovených kritériích bodově hodnoceny (viz. kapitola 4.2 Kritéria hodnocení) na škále 1-10 s váženým hodnocením na základě relevance pro daný mechanismus (tab. 13). Tímto přístupem je možné získat ucelený obraz o výkonnosti jednotlivých konsensních mechanismů s ohledem na jejich silné i slabé stránky. Celkové skóre v tabulce je agregovaný ukazatel, který hodnotí výkonnost daného mechanismu v závislosti na stanovených kritériích. Mechanismus s vysokým celkovým skóre bude pravděpodobně dobře vyvažovat kritéria a dosahovat solidního výkonu v různých oblastech. Na druhou stranu mechanismus s nízkým celkovým skóre může mít slabiny ve více kritériích, nebo může být specificky zaměřen pouze na jedno nebo několik málo kritérií na úkor ostatních.

Váhy jsou poté přiděleny jednotlivým kritériím v závislosti na tom, jak jsou pro daný mechanismus relevantní, to znamená, že rozdělení vah odpovídá specifickému účelu a zaměření daného mechanismu.

Při rozdělování vah byly brány v úvahu následující faktory:

- Charakteristika daného mechanismu – Každý mechanismus má svojí unikátní charakteristiku, jejíž pochopení je důležitým aspektem při hodnocení. Například PoW je obecně považován za velmi bezpečný mechanismus, ale rovněž velmi energeticky náročný, proto byla bezpečnosti přidělena vyšší váha než energetické účinnosti, která naopak má váhu nejnižší.
- Prioritizace kritérií – Některá kritéria mohou být pro daný mechanismus důležitější než ostatní. Například kritérium decentralizace je důležitější pro PoS, zatímco vysoká transakční propustnost pro DPoS.
- Kompenzace slabých stránek – V některých případech mohou být váhy přizpůsobeny tak, aby kompenzovaly slabosti daného mechanismu, pokud má nízkou energetickou účinnost, může být přidělena vyšší váha jinému kritériu, aby tento nedostatek kompenzovala.

Výsledek bodového a váženého hodnocení ukazuje širokou rozmanitost konsensních mechanismů a může poskytnout užitečný přehled a sloužit jako orientační bod například při výběru nejvhodnějšího mechanismu pro danou implementaci. I přes to je ale vždy potřeba zvážit specifické potřeby a brát v úvahu jednotlivá kritéria, jelikož v některých případech může prioritní bezpečnost, zatímco v jiných škálovatelnost.

Algoritmus	SEC	DEC	NM	SCA	TPS	FIN	EE	AM	Celkové skóre
PoW	9	9	10	1	1	8	1	10	**7,23**
	0,2	0,175	0,1	0,1	0,1	0,075	0,05	0,2	
DPoW	10	8	10	2	2	8	4	10	**7,5**
	0,225	0,15	0,1	0,1	0,1	0,075	0,075	0,175	
PoS	8	8	10	5	5	8	8	10	**7,85**
	0,175	0,15	0,1	0,1	0,1	0,075	0,175	0,125	
DPoS	7	5	10	8	8	8	9	10	**8,03**
	0,175	0,1	0,1	0,175	0,175	0,075	0,1	0,1	
LPoS	8	7	10	7	6	8	9	10	**8,05**
	0,175	0,15	0,1	0,125	0,125	0,075	0,125	0,125	
SPoS	8	8	10	9	9	10	9	8	**8,75**
	0,175	0,125	0,1	0,15	0,15	0,075	0,1	0,125	
PoI	8	8	10	7	7	8	8	10	**8,2**
	0,175	0,15	0,1	0,125	0,125	0,075	0,125	0,125	

PoC	7	8	10	1	1	8	7	10	**6,76**
	0,175	0,15	0,1	0,1	0,1	0,075	0,15	0,15	
PoST	7	8	10	1	1	8	6	10	**6,68**
	0,175	0,175	0,1	0,1	0,1	0,075	0,125	0,15	
PoR	7	8	10	1	1	8	6	10	**6,68**
	0,175	0,175	0,1	0,1	0,1	0,075	0,125	0,15	
PoB	4	6	10	1	1	8	8	10	**6,1**
	0,175	0,15	0,1	0,1	0,1	0,075	0,15	0,15	
PoAc	9	8	10	2	2	8	8	10	**7,08**
	0,175	0,15	0,1	0,125	0,125	0,075	0,15	0,1	
PoET	6	8	10	3	5	8	9	10	**7,18**
	0,15	0,15	0,1	0,125	0,15	0,075	0,15	0,1	
PoAu	4	2	10	8	8	10	10	10	**7,7**
	0,15	0,1	0,1	0,15	0,15	0,1	0,15	0,1	
PBFT	4	4	8	1	5	10	8	8	**6,05**
	0,15	0,1	0,125	0,1	0,15	0,1	0,125	0,15	
DBFT	7	5	10	9	10	10	10	8	**8,63**
	0,175	0,1	0,1	0,15	0,15	0,075	0,15	0,1	
ABFT	9	8	8	10	10	10	9	8	**9,03**
	0,15	0,125	0,1	0,15	0,15	0,075	0,125	0,125	
FBA (SCP)	8	8	8	10	10	10	9	8	**8,88**
	0,15	0,125	0,1	0,15	0,15	0,075	0,125	0,125	
Paxos	4	3	8	1	3	10	9	10	**6,23**
	0,15	0,1	0,125	0,1	0,125	0,1	0,15	0,15	
FPaxos	4	3	8	3	5	10	9	8	**6,38**
	0,15	0,1	0,125	0,1	0,125	0,1	0,15	0,15	
Raft	4	3	8	4	5	10	9	10	**6,78**
	0,15	0,1	0,125	0,1	0,125	0,1	0,15	0,15	
Tangle	8	7	8	10	10	8	9	8	**8,6**
	0,15	0,125	0,1	0,15	0,15	0,1	0,125	0,1	

Tabulka 13 – Bodové a vážené hodnocení mechanismů konsensu dle stanovených kritérií

4.5 Přehled výhod a nevýhod konsensních mechanismů

Algoritmus	Výhody	Nevýhody
PoW	• Vysoká míra decentralizace a zabezpečení vzhledem k využití výpočetního výkonu pro dosažení konsensu • Vysoká adopce • Jednoduchý mechanismus	• Vysoká pořizovací cena těžebního hardwaru (ASIC, GPU, CPU) • Náročný na výpočetní výkon • Sdružování výpočetního výkonu v těžebních poolech může mít potencionální vliv na úroveň decentralizace • Extrémní spotřeba energie a negativní dopad na životní prostředí • Nízká škálovatelnost a transakční propustnost • Zranitelný vůči 51 % útoku • Rozšíření malwarů zneužívajících výpočetní výkon zařízení k těžbě • Nákladné transakce
DPoW	• K zabezpečení vlastní sítě využívá navíc k Proof of Work ještě sekundární blockchain jako druhou vrstvu zabezpečení • Téměř imunní vůči 51 % útoku • Menší spotřeba elektrické energie než tradiční PoW	• Závislý na sekundárním blockchainu • Limitovaný pouze na PoW a PoS sekundární blockchainy • Nižší energetická účinnost oproti PoS • Komplexnější než tradiční PoW • Nízká adopce
PoS	• Ekologická varianta k PoW • Vyšší transakční propustnost a škálovatelnost než u PoW • Bezpečnost – potencionální ztráta vsazených tokenů v případě zlomyslného chování • Nižší bariéry pro účast na konsensu • Vysoká adopce • Jednoduchý mechanismus	• Decentralizace je závislá na distribuci tokenů • Počáteční problémy s distribucí tokenů vzhledem k absenci těžby - centralizovaná distribuční metoda • Nothing-at-Stake problém • Koncentrace moci u bohatých uzlů
DPoS	• Vysoká energetická účinnost • Velmi efektivní v oblasti škálovatelnosti a transakční propustnosti	• Sklon k centralizaci, jelikož síť ovládá pouze malý počet delegátů • Většina držitelů tokenů se konsensu neúčastní • Zranitelnost vůči koluzním útokům
LPoS	• Vysoká energetická účinnost • Malí držitelé tokenů mohou získávat podíl z konsensu formou pronájmu svých tokenů – pasivní příjem	• Podobně jako u DPoS, síť se spoléhá na malý počet validátorů, kteří se účastní konsensu – sklon k centralizaci • Pronajímatel musí důvěřovat nájemci, že bude jednat čestně • Zranitelnost proti koluzním útokům • Komplexnější než tradiční PoS
SPoS	• Vysoká energetická účinnost a bezpečnost • Velmi vysoká transakční propustnost a škálovatelnost (implementace shardingu) • Vysoká fluktuace validátorů, kteří jsou vybíráni nejen na základě sázky, ale i reputace • Snaha o spravedlivé rozdělení moci	• Velmi komplexní mechanismus • Nízká adopce a standardizace • Závislost na konkrétní implementaci • Vzhledem k faktu, že se jedná o nový a nerozšířený mechanismus, který se stále vyvíjí, nemusejí být známa všechna potencionální rizika
PoI	• Vyšší škálovatelnost, transakční propustnost • Energetická účinnost • Výběr validátorů na základě sady atributů (skóre důležitosti) • Validátoři jsou z ekonomických důvodů motivováni k síťové aktivitě • Snaha o rovnoměrnější rozdělení moci než tradiční PoS	• Komplexnější než tradiční PoS • Noví uživatelé jsou v nevýhodě vzhledem k nízkému skóre důležitosti • Počáteční problémy s distribucí tokenů

PoC	• Méně nákladný těžební hardware v porovnání s PoW = menší bariéra pro účast na konsensu • Možnost využití široké škály zařízení • Kapacitní prostor je možné zpětně využít ke svému původnímu účelu • Nižší spotřeba energie než u PoW	• Mechanismus není široce přijat • Velmi omezená škálovatelnost a propustnost • Neustálé čtení a zápis na úložiště může znatelně zkrátit jeho životnost (zejména SSD) • Potencionální rozšíření malwarů zneužívajících kapacitní prostor pro těžbu • Velmi časově náročný počáteční plotting úložiště • Méně bezpečný než PoW
PoST	• Stejné výhody jako tradiční PoC • Spravedlnost – PoST vyžaduje kromě úložného prostoru i čas	• Dědí stejné nevýhody od PoC • Vzhledem k nízké adopci nemusí být známa všechna rizika • Složitější mechanismus než PoC, což částečně omezuje jeho širší přijetí
PoR	• Dědí výhody od PoC a PoST • Efektivní pravidelná kontrola integrity dat v síti	• Stejné nevýhody jako PoC a PoST • Limitovaná použitelnost pouze pro decentralizované úložné služby
PoB	• Energetická účinnost • Jednoduchý mechanismus • Dlouhodobější závazek síti spálením tokenů	• Tokeny se pálením stávají navždy neutratitelné, což se dá považovat jako zbytečné plýtvání zdroji • Nedostatečná ekonomická motivace se konsensu účastnit vzhledem k nejistému výnosu • Nízká škálovatelnost a propustnost
PoAc	• Hybridní model PoW a PoS, který dědí jejich výhody – rovnováha mezi bezpečností a energetickou účinností • Odolný proti kybernetickým útokům	• Složitější mechanismus na implementaci • Potencionální koncentrace moci v PoW i PoS části konsensu • Nenabízí o mnoho vyšší škálovatelnost než tradiční PoW, PoS
PoET	• Energetická účinnost • Spravedlivý a decentralizovaný výběr validátora na základě náhodného časového intervalu • Jednoduchý mechanismus	• Závislost na specializovaném hardwaru pro náhodné časování, což může představovat kritický bod selhání • Špatně nastavené časování může vést k manipulaci výběru validátorů • Nevhodný mechanismus pro použití ve veřejných sítích – náchylný k Sybil útokům • Problematická škálovatelnost vzhledem k závislosti na náhodném časování
PoAu	• Velmi efektivní mechanismus v oblasti škálovatelnosti • Energeticky nenáročný • Snadná implementace a správa • Možnost využití v privátních i veřejných sítích	• Proces dosažení konsensu je centralizovaný, jelikož síť řídí pouze malý počet vybraných validátorů • Uživatelé sítě musí validátorům plně důvěřovat • Náchylnost ke koluzním útokům
PBFT	• Energetická účinnost • Rychlé potvrzování transakcí a deterministická finalita	• Velmi nízká škálovatelnost vzhledem k povaze komunikace • Složitější na implementaci • Zranitelnost proti Sybil útokům • Nevhodný mechanismus pro využití ve velkých otevřených sítích
DBFT	• Vysoká energetická účinnost • Vysoká škálovatelnost a transakční propustnost • Deterministická finalita • Vhodné pro dApps, smart kontrakty	• Podobně jako DPoS, závislost na malé skupině delegátů, kteří se účastní procesu konsensu – centralizace • Uživatelé musí důvěřovat delegátům • Nižší adopce než u tradičních konsensních mechanismů
ABFT	• Vysoká energetická účinnost, škálovatelnost a transakční propustnost • Deterministická finalita • Dosažení shody asynchronní komunikací • Extrémně rychlé šíření zpráv za pomoci gossip protokolů	• Nová a unikátní datová struktura • Velmi nízká adopce, všechna potencionální rizika stále nemusejí být známa • Velmi komplexní mechanismus složitý na implementaci

FBA (SCP)	• Vysoká energetická účinnost, škálovatelnost a transakční propustnost • Spravedlivější rozdělení moci • Rychlé a nenákladné transakce, svou podstatou vhodný právě pro mikrotransakce, dApps a smart kontrakty	• Nízká adopce • Komplexní mechanismus • Závislost na distribuci tokenů, může vést ke koncentraci moci a ovlivňování výběru kvór
Paxos	• Vysoká odolnost proti selhání • Energetická účinnost	• Vhodný pro menší a uzavřené sítě • Velmi nízká škálovatelnost • Celkově nízká efektivita • Složitý mechanismus • Náročná komunikace při dosahování konsensu
FPaxos	• Lepší škálovatelnost snížením počtu komunikačních kol než u Paxos • Efektivnější než původní Paxos	• I když se jedná o zjednodušenější a optimalizovanější variantu Paxos, stále se jedná o složitý mechanismus s náročnou komunikací
Raft	• Navržen pro snadnou implementaci a pochopení • Oproti Paxos obsahuje mechanismus pro volbu vůdce, což snižuje komunikační zátěž a zvyšuje škálovatelnost • Vysoká odolnost proti selhání	• Nevhodný pro velké sítě, škálovatelnost se vzhledem k povaze komunikace a závislosti na vůdci rapidně snižuje • V případě selhání vůdce musí být zvolen nový, což může způsobit dočasné přerušení
Tangle	• Velmi vysoká škálovatelnost a transakční propustnost • Energeticky účinný mechanismus • Nevyžaduje transakční poplatky • Potencionálně vhodný mechanismus pro využití v IoT a pro mikrotransakce	• Nízká adopce, všechna rizika stále nemusejí být známa • V období nízké síťové aktivity využívá centralizovaný prvek pro potvrzování transakcí • Zabezpečení a výkonnost sítě závisí na její velikosti

Tabulka 14 – Přehled výhod a nevýhod konsensních mechanismů

5 Použité simulátory konsensních mechanismů

V této práci bylo komplexně popsáno a porovnáno 22 různých konsensních mechanismů, kdy každý z nich představuje vlastní soubor výzev. I když by bylo ideální provést detailní testování každého z těchto mechanismů, vyžadovalo by to jejich technickou implementaci, která by v takovémto rozsahu byla nad rámec této práce. Vzhledem k tomuto omezení se následující kapitola zabývá využitím dvou open-source simulátorů BlockSim a TangleSimulator dostupných z GitHub.

5.1 BlockSim

BlockSim je open-source simulátor blockchainu implementován v programovacím jazyce Python, který umožňuje provádět simulace blockchainových systémů, získávat užitečné poznatky a provádět analýzy různých konfigurací. Součástí BlockSimu je základní model Bitcoin a Ethereum blockchainu, který obsahuje funkční bloky, jako jsou uzly, transakce, bloky, konsensus a další prvky, které jsou obecně přítomné ve většině blockchainů. Tyto bloky lze dále konfigurovat. Po dokončení simulace jsou výsledky uloženy do Excelovské tabulky, která obsahuje informace, jako jsou celkový počet vytěžených bloků, detailní seznam bloků včetně časů a transakcí, počet uncle/stale bloků, dobu propagace bloku, informace o těžařích.

BlockSim je jednoduchý nástroj pro reprezentaci složitého chování blockchainových systémů a umožňuje poskytnout užitečná statistická data pro lepší porozumění. [129]

BlockSim model umožňuje konfiguraci následujícího:

- Průměrný čas vytvoření nového bloku
- Velikost bloku
- Průměrný čas propagace bloku v síti
- Odměna pro těžaře
- Povolit/vypnout transakce v simulaci
- Nastavit způsob modelování transakcí
- Počet vytvořených transakcí za vteřinu

- Průměrný čas propagace transakcí v síti
- Poplatek za transakci
- Velikost transakce
- Počet uzlů v síti
- Nastavení počtu těžařů včetně rozdělení moci
- Čas simulace
- Počet běhů simulace

```
if model == 1:
    ''' Block Parameters '''
    Binterval = 600  # Average time (in seconds)for creating a block in the blockchain
    Bsize = 1  # The block size in MB
    Bdelay = 10  # Average block propogation delay in seconds
    Breward = 6.25  # Reward for mining a block

    ''' Transaction Parameters '''
    hasTrans = True  # True/False to enable/disable transactions in the simulator
    Ttechnique = "Light"  # Full/Light to specify the way of modelling transactions
    Tn = 20  # The rate of the number of transactions to be created per second
    Tdelay = 10 # The average transaction propagation delay in seconds (Only if Full technique is used)
    Tfee = 0.000150  # The average transaction fee
    Tsize = 0.000550  # The average transaction size  in MB

    ''' Node Parameters '''
    Nn = 100  # The total number of nodes in the network
    NODES = []
    from Models.Bitcoin.Node import Node
    # Nodes ID + % of power
    NODES = [Node(id=0, hashPower=30), Node(id=1, hashPower=23), Node(id=2, hashPower=12.5),
             Node(id=3, hashPower=10),Node(id=4, hashPower=7.5),Node(id=5, hashPower=6),
             Node(id=6, hashPower=6),Node(id=7, hashPower=5)]

    ''' Simulation Parameters '''
    simTime = 2419200  # The simulation length (in seconds)
    Runs = 2  # Number of simulation runs
```

Obrázek 22 – Nastavení konfigurace modelu v BlockSim

5.1.1 TS: Vliv doby propagace bloku na výskyt zastaralých bloků a transakční propustnost

Cíle:

Cílem testu je vyhodnotit, jak změny průměrné doby těžby bloku a doby propagace bloku ovlivňují výskyt zastaralých bloků (stale blocks) a celkovou transakční propustnost.

Předpoklady / počáteční nastavení:

- Připravte testovací prostředí pro běh simulace
- Nastavte konfiguraci, která bude během každého testu konstantní:

TPS = maximální možný počet transakcí v bloku

Velikost bloku = 1 MB

Velikost transakce = 550 Bytů

Průměrný čas propagace transakce = 15 sekund

Počet uzlů v síti = 100

Počet opakování simulace = 2

Testovací kroky:

1. Nastavte průměrnou dobu těžby bloku na hodnotu 600 sekund a průměrnou dobou propagace bloku na 0,5 sekundy. Spusťte simulaci po dobu nezbytně dlouhou pro vytěžení 4000 bloků a zaznamenejte z výstupu data o produkci zastaralých bloků společně s transakční propustností.
2. Opakujte test s průměrnou dobou těžby bloku 600 sekund pro hodnoty průměrné doby propagace bloku 1/3/5/10/15 sekund a zaznamenávejte data o produkci zastaralých bloků a transakční propustnosti.
3. Nastavte průměrnou dobu těžby bloku z 600 sekund na 480/300/180/120/60/30/10/1 sekundy a pro každý čas proveďte testy s nastavením doby propagace bloku na 0,5/1/3/5/10/15 sekund a opět zaznamenejte výsledky jednotlivých testů.

   Čas simulace nastavte pro průměrné doby těžby bloku tak, aby počet vytěžených bloků byl ve všech testech srovnatelný.

Očekávané výsledky:

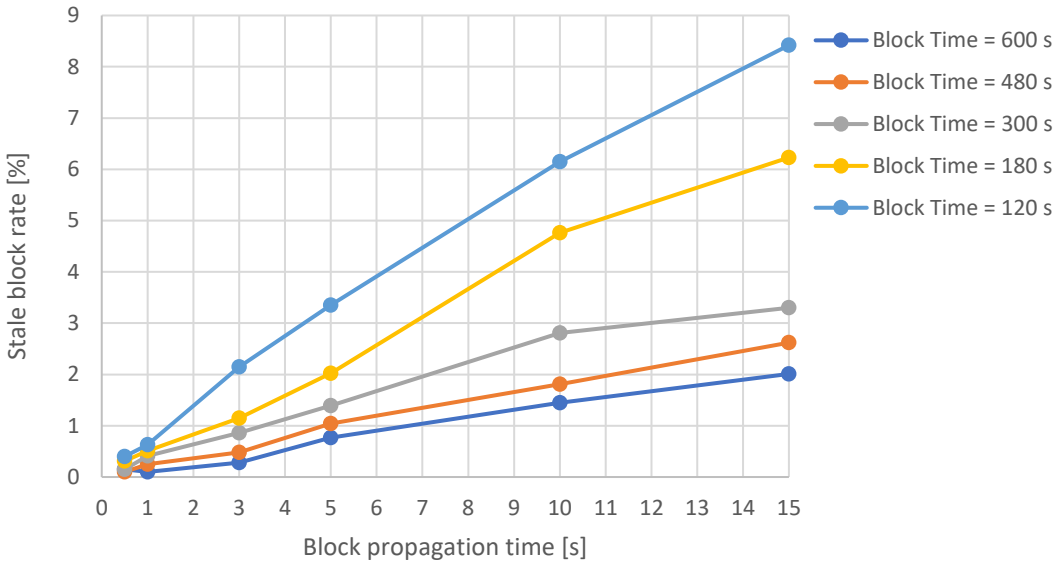
Nejvyšší stanovená průměrná doba těžby bloku by měla produkovat nejmenší podíl zastaralých bloků, který se procentuálně s dobou propagace bloku zvyšuje. Zároveň čím vyšší je průměrná doba vytěžení nového bloku, tím nižší je transakční propustnost. Snižováním průměrné doby těžby bloku by mělo docházet k vyšší transakční propustnosti, ale zároveň také k rapidnímu nárůstu zastaralých bloků.

Aktuální výsledky:

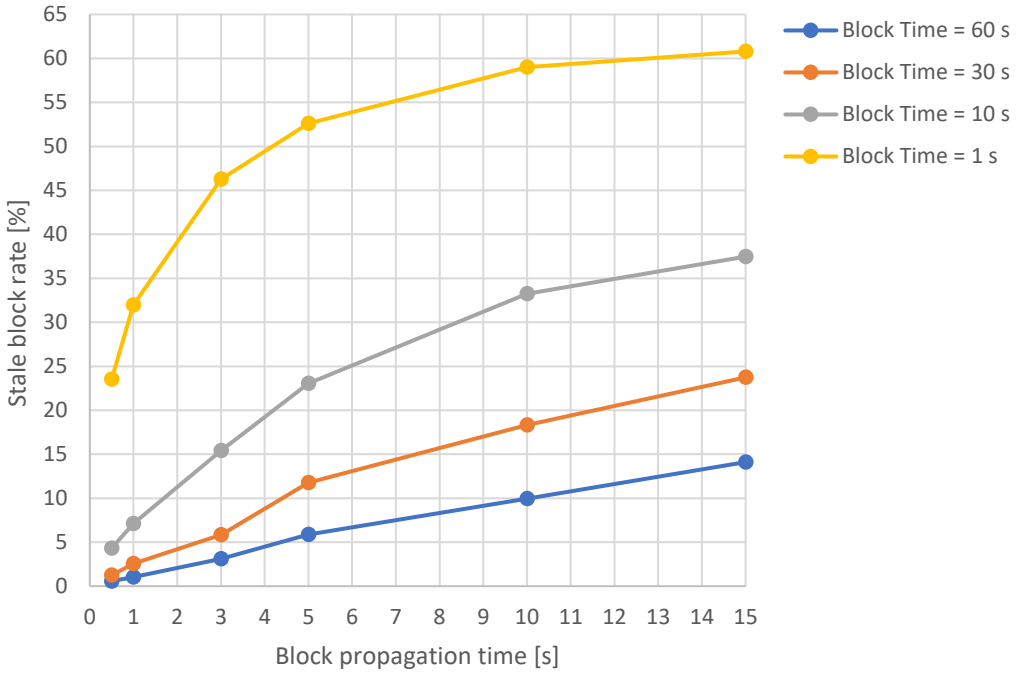
Block Time [s]	Block propagation delay [s]	Mined blocks	Stale blocks	Stale rate [%]	TPS
600	0,5	3884	6	0,15	2,93
600	1	4035	4	0,1	3,05
600	3	3940	11	0,28	2,98
600	5	3977	31	0,77	3,00
600	10	3954	58	1,45	2,99
600	15	3810	78	2,01	2,88
480	0,5	3934	4	0,1	3,72
480	1	4070	10	0,25	3,85
480	3	3955	19	0,48	3,74
480	5	4100	43	1,04	3,88
480	10	3916	72	1,81	3,70
480	15	3937	106	2,62	3,72
300	0,5	3928	6	0,15	5,94
300	1	4124	17	0,41	6,24
300	3	4020	35	0,86	6,08
300	5	3985	56	1,39	6,02
300	10	3838	111	2,81	5,80
300	15	3930	134	3,3	5,94
180	0,5	4119	13	0,31	10,38
180	1	4090	21	0,51	10,30
180	3	3961	46	1,15	9,98
180	5	3879	80	2,02	9,78
180	10	3783	189	4,76	9,53
180	15	3717	247	6,23	9,37
120	0,5	3948	16	0,4	14,92
120	1	3915	25	0,63	14,79
120	3	4009	88	2,15	15,15
120	5	3924	136	3,35	14,84
120	10	3873	254	6,15	14,63
120	15	3719	342	8,42	14,05
60	0,5	3961	23	0,58	29,95
60	1	4051	43	1,05	30,60
60	3	3901	126	3,13	29,49
60	5	3785	236	5,87	28,60
60	10	3578	395	9,94	27,03
60	15	3444	566	14,11	26,03
30	0,5	4063	51	1,24	61,41
30	1	3894	103	2,58	58,85
30	3	3794	235	5,83	57,34
30	5	3606	481	11,77	54,49
30	10	3311	742	18,31	50,02
30	15	3096	964	23,74	46,78
10	0,5	3996	181	4,33	180,99
10	1	3729	286	7,12	168,89
10	3	3340	608	15,4	151,29
10	5	3185	955	23,07	144,27
10	10	2692	1340	33,23	121,91
10	15	2478	1485	37,47	112,20
1	0,5	3144	967	23,52	1423,04
1	1	2770	1301	31,96	1254,05
1	3	2149	1851	46,27	972,93
1	5	1900	2110	52,62	860,09

1	10	1699	2447	59,02	770,12
1	15	1581	2451	60,79	715,65

Tabulka 15 – Data ze simulace vlivu doby propagace bloku na výskyt zastaralých bloků a transakční propustnost sítě



Graf 3 – Vliv doby propagace bloku na produkci zastaral (600/480/300/180 s)



Graf 4 – Vliv doby propagace bloku na produkci zastaral (60/30/10/1 s)

Komentář:

Ze simulace je patrné, že se snižující se průměrnou dobou nalezení bloku se zvyšuje transakční propustnost, ovšem rovněž narůstá podíl zastaralých bloků dle dob propagace bloku v síti (graf 3 a 4), což je vysoce nežádoucí. Výsledná data ukazují, že nejlépe je na tom s podílem zastaralých bloků s dobou propagace 0,5 až 15 sekund (0,15 % - 2,01 %) varianta času těžby 600 sekund. Pokud by se provedla optimalizace, při které by se našla nová minima a maxima doby propagace bloku, bylo by možné snížit průměrnou dobu těžby a dosáhnout vyšší transakční propustnosti bez markantního nárůstu podílu zastaralých bloků.

5.1.2 TS: Vliv rozložení moci na spravedlivou distribuci odměn

Cíl:

Cílem testu je zjistit, jak různé rozložení moci mezi těžaři ovlivňuje férovost distribuce odměn v síti (tj. rozložení vytěžených bloků mezi těžaře)

Předpoklady / počáteční nastavení:

- Připravené testovací prostředí pro běh simulace
- Nastavené konfigurace jsou během každého testu konstantní:

  TPS = maximální možný počet transakcí v bloku
  Velikost bloku = 1 MB
  Průměrná doba vytěžení bloku = 300 sekund
  Průměrná doba propagace bloku = 0,5 sekundy
  Velikost transakce = 550 Bytů
  Počet uzlů v síti = 100
  Počet opakování simulace = 2

Testovací kroky:

1. Rozložte rovnoměrně výpočetní výkon/moc mezi 10 těžebních uzlů a spusťte simulaci po dobu 14 dnů a zaznamenejte distribuci vytěžených bloků mezi těžebními uzly.

2. Změňte rozložení moci mezi 10 těžebními uzly nerovnoměrně v poměru například 30/12/10/9/9/8/6/6/5/5 % a spusťte simulaci po dobu 14 dnů. Data o distribuci vytěžených bloků rovněž zaznamenejte.
3. V dalším testu přidělte jednomu z uzlů nadpoloviční většinu moci v síti například v následujícím poměru 60/8/4/4/4/4/4/4/4/4 % spusťte test na stejnou dobu 14 dnů a zaznamenejte data.

Očekávané výsledky:

Při rovnoměrném rozdělení moci mezi uzly v síti by měl každý uzel vytěžit zhruba stejný podíl z bloků. Rozdělení moci mezi těžaři by mělo s menšími odchylkami korelovat s distribucí vytěžených bloků. Těžaři s větším podílem moci v síti by měli mít větší šanci na vytěžení nového bloku v porovnání s těžaři, kteří mají v síti menší podíl moci.

Aktuální výsledky:

Těžař ID	Výkon [%]	Vytěžených bloků	Podíl [%]
0	10	405	10,12
1	10	425	10,62
2	10	423	10,57
3	10	347	8,67
4	10	392	9,8
5	10	426	10,65
6	10	398	9,95
7	10	383	9,57
8	10	411	10,27
9	10	391	9,77

Tabulka 16 – Distribuce odměn při rovnoměrném rozložení moci

Těžař ID	Výkon [%]	Vytěžených bloků	Podíl [%]
0	30	1231	30,87
1	12	453	11,36
2	10	414	10,38
3	9	342	8,58
4	9	372	9,33
5	8	296	7,42
6	6	229	5,74
7	6	259	6,49
8	5	200	5,02
9	5	192	4,81

Tabulka 17 – Distribuce odměn při nerovnoměrném rozložení moci

Těžař ID	Výkon [%]	Vytěžených bloků	Podíl [%]
0	60	2415	59,97
1	8	360	8,94
2	4	171	4,25
3	4	150	3,72
4	4	159	3,95
5	4	152	3,77
6	4	153	3,8
7	4	159	3,95
8	4	149	3,7
9	4	159	3,95

Tabulka 18 – Distribuce odměn s dominantním těžebním uzlem

Komentář:

Výsledek simulace ukazuje, že distribuce vytěžených bloků s odchylkami odpovídá procentuálnímu podílu moci v síti (tabulka 16 a 17) a to i v případě, že se v síti nachází dominantní těžební uzel (tabulka 18).

5.2 TangleSimulator

TangleSimulator je open-source nástroj implementovaný v Jupyteru, který umožňuje modelovat a vizualizovat síť Tangle, které je základem kryptoměny IOTA. Simulátor umožňuje provádět simulace s různými možnostmi výběru tipů (tip selection) a parametry ovlivňujícími potvrzování a šíření transakcí v síti. Výsledky jsou poté vykreslovány pomocí vizualizací a grafů.

V rámci simulátoru lze konfigurovat následující parametry:

- **λ (lambda, rate)** – tento parametr ovlivňuje frekvenci, s jakou jsou vytvářeny nové transakce, jedná se o průměrný počet nových transakcí za jednotku času (vyšší hodnota = vyšší frekvence transakcí)
- **tip selection** (výběr tipů) – tento parametr určuje, jaký algoritmus se použije pro výběr tipů (tip = nepotvrzená transakce) – URTS slouží pro rovnoměrný náhodný výběr tipů, MCMC pro vážený náhodný výběr tipů
- **α (alfa)** – alfa ovlivňuje chování algoritmu MCMC při výběru tipů, vyšší hodnota znamená vyšší preferenci tipů s vyšší kumulativní váhou (cumulative weight)
- **Počet transakcí**

V simulátoru jsou implementovány hlavní experimenty, které umožňují vizualizaci DAG transakcí s využitím algoritmu URTS/MCMC, sledování kumulativní váhy transakcí a počtu tipů v čase. Dále je možné provádět experimenty s různými hodnotami parametrů alfa a lambda. [130]

5.2.1 TS: Vliv rychlosti generování transakcí na počet tipů v síti s využitím algoritmu URTS

Cíl:

Cílem tohoto testu je analyzovat, jak úprava parametru lambda představující rychlost generování transakcí za jednotku času má vliv na počet tipů s využitím algoritmu URTS za předpokladu, že počet transakcí je neměnný.

Předpoklady / počáteční nastavení:

- Připravte testovací prostředí pro běh simulace
- Nastavte algoritmus pro výběr typů na URTS
- V jednotlivých simulacích lze upravovat hodnotu lambda

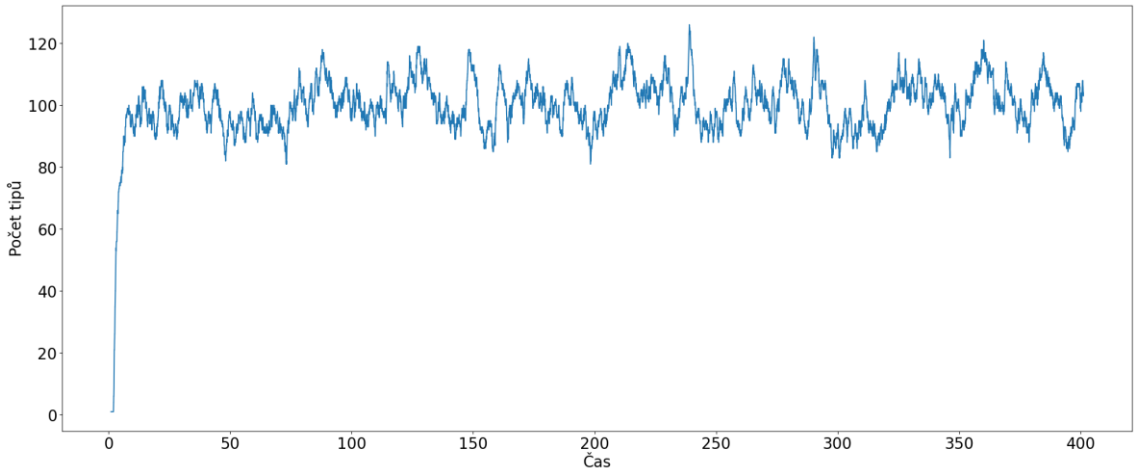
Testovací kroky:

1. Nastavte počáteční hodnotu lambda na 50 a počet transakcí na 20000
2. Proveďte simulaci a monitorujte chování sítě.
3. Změňte hodnotu lambda na 100 při zachování konstantního počtu transakcí 20000 a monitorujte chování sítě.
4. Nastavte hodnotu lambda na 150 při stejném počtu transakcí, zaznamenejte data a porovnejte je s výsledky z předchozích kroků.

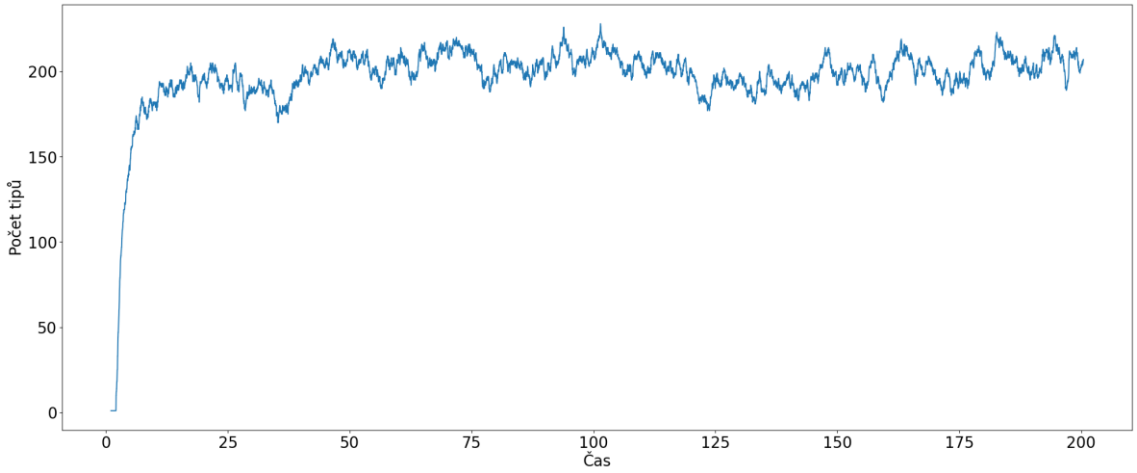
Očekávané výsledky:

S rostoucí rychlostí generování transakcí se očekává, že se zvýší i počet tipů v síti vzhledem k faktu, že nové transakce, které ještě nejsou potvrzeny jsou generovány rychleji.

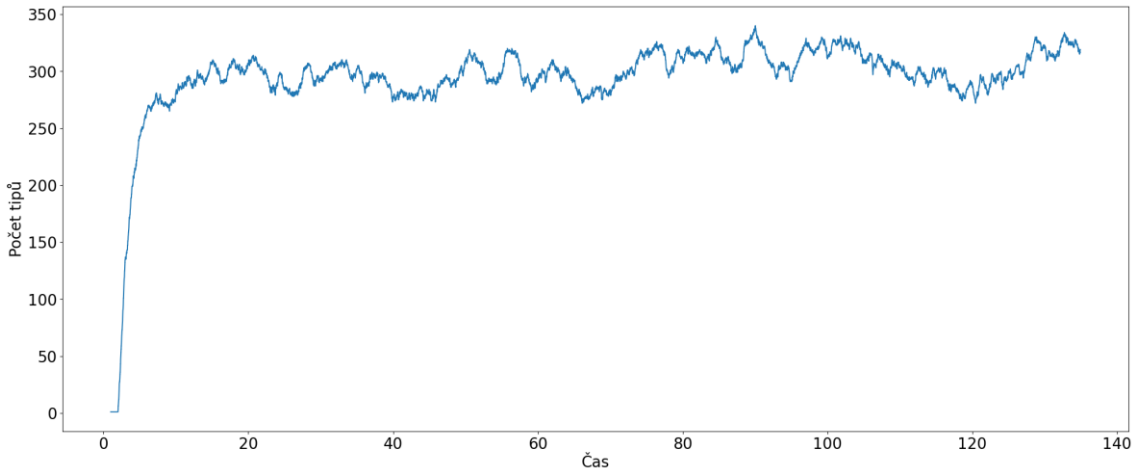
Aktuální výsledky:



Graf 5 – Vliv λ = 50 na počet tipů v síti (URTS)



Graf 6 – Vliv λ = 100 na počet tipů v síti (URTS)



Graf 7 – Vliv λ = 150 na počet tipů v síti (URTS)

Komentář:

Tento scénář umožňuje pochopit, jak rychlost generování transakcí ovlivňuje chování sítě. Výsledek simulace ukazuje, že počet tipů se s využitím algoritmu URTS úměrně zvyšuje při zvyšování hodnoty lambda (graf 5, 6, 7), i když celkový počet transakcí zůstává stejný.

5.2.2 TS: Vliv zvyšování hodnoty preferencí tipů s kumulativní váhou na jejich výskyt v síti s využitím algoritmu MCMC

Cíl:

Cílem tohoto testu je analyzovat, jaký vliv má zvyšování hodnoty preferencí tipů s kumulativní váhou alfa na celkový výskyt tipů v síti s využitím algoritmu MCMC za předpokladu, že hodnota lambda a počet transakcí je konstantní.

Předpoklady / počáteční nastavení:

- Připravte testovací prostředí pro běh simulace
- Nastavte algoritmus pro výběr typů na MCMC
- V jednotlivých simulacích lze upravovat hodnoty alfa

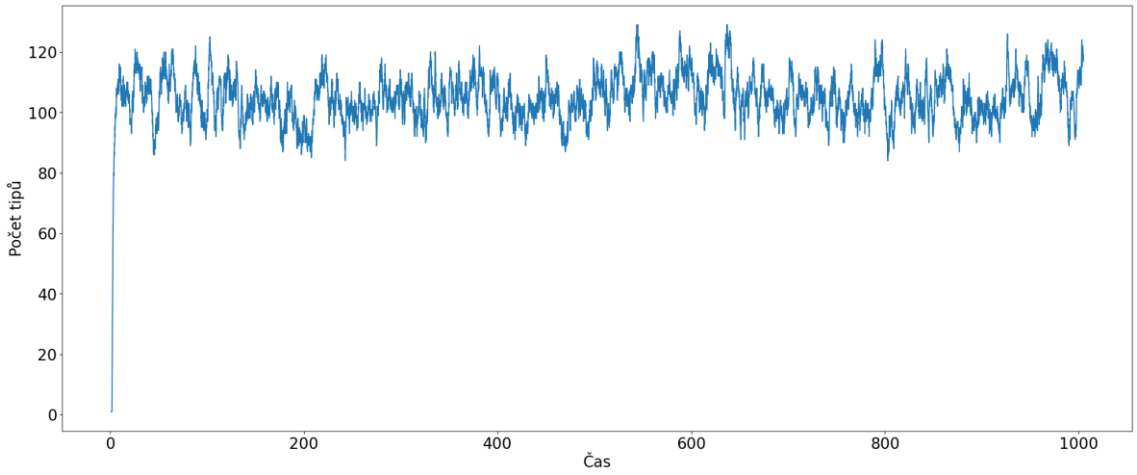
Testovací kroky:

1. Nastavte počáteční hodnotu lambda na 50, počet transakcí 50000 a prvotní hodnotu preferencí tipů s kumulativní váhou alfa na 0,01. Hodnota lambda a počet transakcí je ve všech krocích konstantní.
2. Proveďte simulaci, monitorujte a zaznamenejte výskyt tipů v čase.
3. Zvyšte hodnotu alfa na 0,1 a proveďte další simulaci. Monitorujte a zaznamenejte výskyt tipů
4. Proveďte třetí simulaci tentokrát s nastavenou hodnotou alfa na 1, zaznamenejte výsledky a porovnejte s těmi z předchozích kroků.

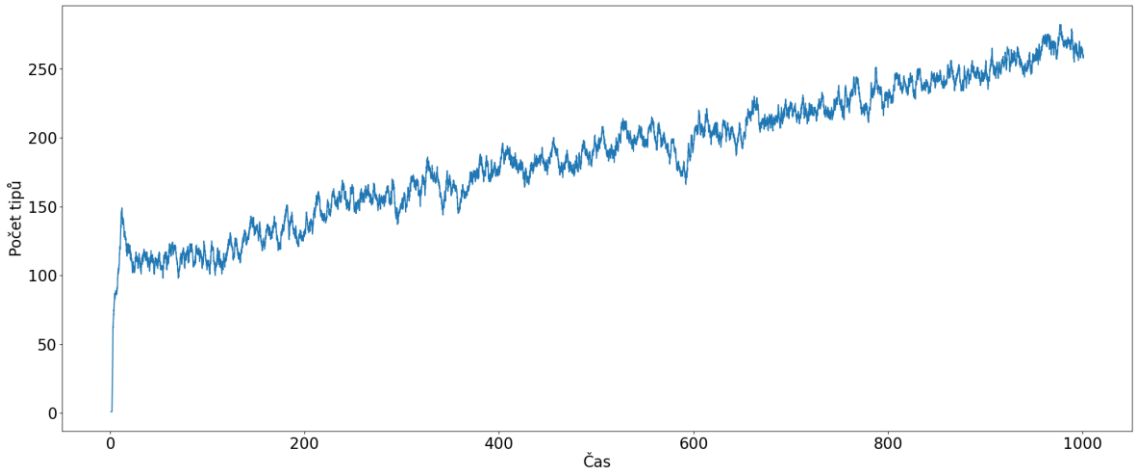
Očekávané výsledky:

Zvyšování hodnoty alfa by mělo v průběhu času vést k pozorovatelným změnám v počtu tipů v síti. V závislosti na zvyšování hodnoty parametru alfa by mělo docházet k jejich nárůstu.

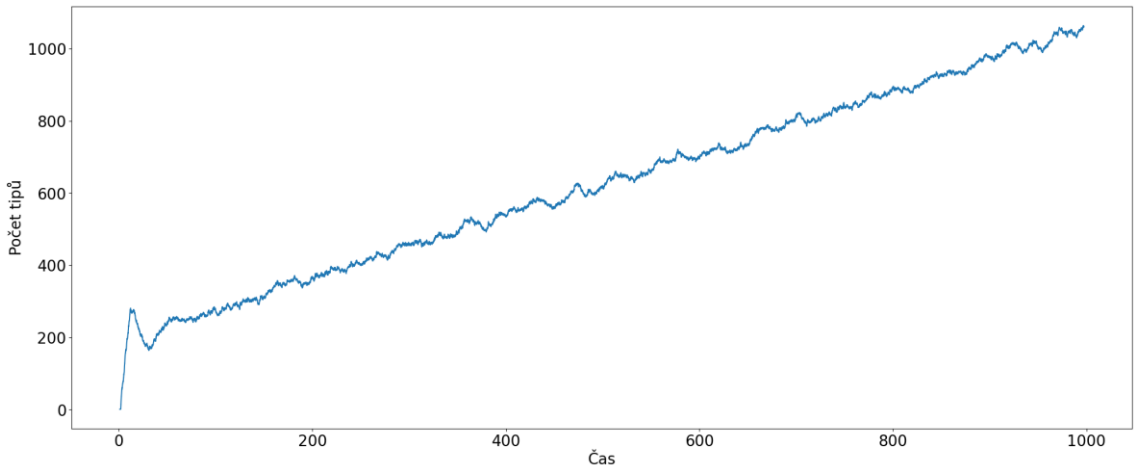
Aktuální výsledky:



Graf 8 – Vliv zvyšování hodnoty α = 0,01 na výskyt tipů v síti



Graf 9 – Vliv zvyšování hodnoty α = 0,1 na výskyt tipů v síti



Graf 10 – Vliv zvyšování hodnoty α = 1 na výskyt tipů v síti

Komentář:

Tento scénář poskytuje informace o vývoji počtu tipů v Tangle síti s využitím algoritmu MCMC při změnách hodnoty preferencí tipů s kumulativní váhou alfa. Zvyšování hodnoty parametru alfa (graf 8, 9, 10) vede k nárůstu tipů v síti vzhledem k tomu, že jsou preferovanější tipy s vyšší kumulativní váhou.

6 Metodologické návrhy testovacích scénářů konsensních mechanismů

Tato kapitola se primárně zaměřuje na návrh a vytvoření promyšlených testovacích scénářů pro vybrané konsensní mechanismy používané v blockchainových sítích. Tyto scénáře byly pečlivě navrženy tak, aby zkoumaly a testovaly různé aspekty a vlastnosti těchto mechanismů, od jejich odolnosti vůči napadení až po jejich schopnost účinně fungovat v různých síťových podmínkách. Scénáře byly navrženy tak, aby bylo možné získat podrobné a přesné výsledky, které by mohly vést k hlubšímu porozumění těchto mechanismů a jejich praktickému využití. Kapitola tedy slouží jako důležitý krok k dalšímu testování a výzkumu v oblasti konsensních mechanismů pro blockchainové sítě.

6.1 Obecné testovací scénáře blockchainových konsensních mechanismů

6.1.1 TS: Škálovatelnost sítě

Cíl:

Cílem tohoto testovacího scénáře je zjistit, jak je blockchainová síť s vybraným konsensním mechanismem schopna zvládat zvyšující se nárůst počtu uzlů a transakcí.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť se zvoleným konsensním mechanismem
- Do sítě je připojených a synchronizovaných na počátku 100 uzlů
- Nastavte generátor transakcí, který bude simulovat mírné zatížení
- V síti se nebudou nacházet žádné nezpracované transakce
- Připravte nástroje pro monitoring klíčových výkonnostních metrik

Testovací kroky:

1. Spusťte testovací síť s počátečním nízkým stavem 100 uzlů.
2. Ujistěte se, že uzly jsou funkční a plně synchronizovány.

3. Spusťte generátor transakcí, který bude simulovat mírnou zátěž
4. Monitorujte a zaznamenejte po omezenou dobu výkonnost sítě, jako je:
    - Čas potvrzení bloku
    - Doba propagace bloku
    - Transakční propustnost
    - Latence v síti
    - Případně spotřeba zdrojů
5. Zvyšujte zátěž sítě připojováním další uzlů (100/200/300 … n). Udržujte pro všechny uzly stejnou míru transakční zátěže.
6. Zvyšujte a monitorujte výkonnost sítě pro každou sadu uzlů, dokud nedosáhnete požadovaného počtu.
7. Poté vraťte počet uzlů v síti na prvotní hodnotu a postupně simulujte větší transakční zatížení sítě.
8. Nechte síť pracovat v zátěži při každé změně dostatečně dlouhou dobu a monitorujte její výkon. Tímto způsobem pokračujte, dokud nedosáhnete požadovaného zatížení.
9. Analyzujte výsledky testování.

Očekávané výsledky:

Předpokládá se, že by síť měla se zvyšující se zátěží nadále bezproblémově fungovat. Časy potvrzení bloků, transakční propustnost by se měla škálovat s velikostí sítě, zatížení a latence by se neměly výrazně zvýšit, stejně tak jako spotřeba zdrojů. To vše do určitého bodu, ve kterém by se měly začít ve výkonnostních metrikách projevovat nedostatky.

6.1.2 TS: Vliv velikosti bloku na dobu jeho propagace a TPS

Cíl:

Cílem testu je analyzovat, jak změna velikosti bloku ovlivňuje dobu jeho šíření a propustnost transakcí v blockchainové síti.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť se zvoleným konsensním mechanismem a předem definovaným počtem uzlů
- Nastavte generátor transakcí, který bude simulovat střední zátěž
- Připravte nástroje pro monitoring klíčových výkonnostních metrik
- K dispozici je možnost upravovat velikost bloku

Testovací kroky:

1. Spusťte blockchainovou testovací síť s vybraným konsensním mechanismem s nastavenou základní velikostí bloku například 1 MB po dostatečně dlouhou dobu.
2. Zaznamenejte průměrnou dobu šíření bloku (čas, za který se nově vytvořený blok rozšíří na většinu uzlů v síti – 50 % a 90 %) a propustnost transakcí
3. Zvyšte velikost bloku o nastavený přírůstek (např. dvojnásobek na 2 MB).
4. Po úpravě velikosti bloku zvyšte odpovídajícím způsobem množství generovaných transakcí, aby byl simulován normální provoz v síti.
5. Zaznamenejte průměrnou dobu šíření bloku, čas, kdy je poprvé blok potvrzen a kdy je přijat ostatními uzly v síti.
6. Vypočítejte zvýšení transakční propustnosti (ujistěte se, že se potencionálně nezvyšuje podíl zastaralých bloků v případě, že to daný mechanismus umožňuje).
7. Opakujte krok 3 a 4 a zaznamenávejte důležité metriky.
8. Po testování konsolidujte všechna data a proveďte jejich analýzu, hledejte body, ve kterých zvýšení velikosti bloku začne negativně ovlivňovat dobu jeho propagace, transakční propustnost nebo celkové dosažení konsensu.

Očekávané výsledky:

S rostoucí velikostí bloku se může prodlužovat i doba jeho propagace kvůli většímu množství dat, které je třeba přenést do každého uzlu. Transakční propustnost se může zpočátku zvýšit s větší velikostí bloku díky možnosti zahrnout do něj více transakcí. Pokud se však časy propagace příliš prodlouží, může to omezit rychlost potvrzování bloků, snížit propustnost (případně zvýšit podíl zastaralých bloků) a mít další negativní dopady na proces konsensu.

Tento testovací scénář může pomoci identifikovat potenciální výhody a nevýhody zvýšení velikosti bloku s daným mechanismem konsensu. Ideální velikost bloku může být rovnováha mezi transakční propustností a dobou propagace bloku.

6.1.3 TS: Vliv latence sítě na celkový výkon

Cíl:

Cílem je vyhodnotit vliv latence sítě na celkový výkon a spolehlivost mechanismu konsensu, dobu šíření bloku, dobu potvrzení transakce a celkovou propustnost sítě.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť se zvoleným konsensním mechanismem a předem definovaným počtem uzlů
- K dispozici je generátor transakcí, který bude simulovat různé úrovně zátěže
- Připravte nástroje pro monitoring klíčových výkonnostních metrik
- K dispozici je funkce, která umožňuje simulovat různé úrovně latence sítě

Testovací kroky:

1. Spusťte blockchainovou testovací síť s vybraným konsensním mechanismem
2. V počátečním stavu s nízkou úrovní latence zaznamenejte standardní výkonnostní metriky, jako je doba potvrzení transakce, doba šíření bloku, celková propustnost sítě. Tento základní test simulujte po dostatečně dlouhou omezenou dobu a vytvořte tak základní bod, se kterým budete porovnávat výsledky v následujících krocích při zvýšené latenci.
3. Zvyšte konzistentně úroveň latence v síti na vyšší hodnotu (např. 50/100/200 … ms).
4. V každé úrovni latence generujte dostatečně významný počet transakcí mezi uzly tak, aby byl simulován normální provoz sítě.
5. Sledujte a zaznamenávejte časy potvrzení každé zahájené transakce - sledování času od odeslání transakce do sítě až do jejího zahrnutí do bloku a potvrzení.
6. Monitorujte dobu propagace bloků v síti a celý proces konsensu.

7. Sledujte transakční propustnost sítě pro danou úroveň latence.
8. Jakmile zaznamenáte výkonnostní metriky pro danou úroveň latence, zvyšte latenci na další úroveň a opakujte kroky 4 až 7.
9. Analyzujte získaná data z různých úrovní latence v síti.

Očekávané výsledky:

Se zvyšující se latencí sítě se očekává, že se bude prodlužovat doba potvrzování transakcí a propagace bloků, protože trvá déle, než se informace po síti rozšíří. Vzhledem k tomu se může celková propustnost sítě snížit. Konkrétní dopady budou záviset na zvoleném mechanismu konsensu. Některé mechanismy mohou zvládnout latenci sítě lépe než jiné. Při vysoké latenci se síť může stát nestabilní a potencionálně vést až k rozvětvením nebo nekonzistenci v blockchainu.

6.1.4 TS: Odolnost sítě proti 51 % útok

Cíl:

Cíl testovacího scénáře je posoudit zranitelnost daného mechanismu vůči 51 % útoku. V 51 % útoku se jediný subjekt pokusí získat nadpoloviční moc v síti, aby mohl manipulovat s historií transakcí nebo se pokusit o double-spending útok.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť se zvoleným konsensním mechanismem
- Do sítě je připojených a synchronizovaných na počátku alespoň 100 uzlů
- Nastavte generátor transakcí, který bude simulovat běžný provoz v síti
- Připravte nástroje pro monitoring klíčových výkonnostních metrik
- Zvolte samostatný uzel, který bude simulovat roli útočníka a přidělte mu počáteční významnou část zdrojů (30 - 40 %)

Testovací kroky:

1. Spusťte blockchainovou testovací síť s vybraným konsensním mechanismem a simulujte běžný provoz sítě.
2. Monitorujte a zaznamenávejte klíčové výkonnostní metriky sítě.

3. Zvyšujte postupným tempem moc útočníka v síti (+5/10/15 %).
4. S každým přírůstkem pokračujte v simulaci běžného provozu sítě a sledujte výkon sítě včetně aktivit útočníka (počet vytvořených bloků, forky).
5. Jakmile získá útočník nadpoloviční moc v síti, začněte simulovat útok v podobě double-spendingu, cenzury transakcí a další.
6. Pokračujte v monitoringu a sledujte schopnost útočníka manipulovat s blockchainem. Během těchto kroků je důležité zaznamenat veškerá data při změně výkonu nebo porušení zabezpečení k budoucí analýze zranitelnosti a dopadů.
7. Analyzujte útočníkovy dopady na síť při různých úrovních zdrojů, kterými disponuje.

Očekávané výsledky:

Na začátku testu by síť měla být v normálu, všechny transakce by se měly zpracovávat a uzly se spravedlivě účastnit konsensu. Doba potvrzení bloku, transakční propustnost a latence by měly být v normě a počet forků by měl být minimální. Se zvyšující se mocí útočníka v síti může docházet k zvýšení počtu bloků přidaných útočníkem a zvýšení počtu forků. Nemělo by však ale docházet k žádnému významnému narušení celkového výkonu sítě. Při simulaci útoku, jakmile útočník získá nadpoloviční moc, by síť měla odolávala jakýmkoliv pokusům o manipulaci. Konsensní mechanismus by měl mít opatření, která by takovým událostem bránila. V závislosti na mechanismu však může docházet k narušení, například se může zvýšit počet forků, nebo se mohou prodloužit potvrzovací časy.

6.1.5 TS: Řešení forků v síti

Cíl:

Cílem testovacího scénáře je zjistit, zda konsensní mechanismus zvládá správně a efektivně řešit forky (neboli rozvětvení) v blockchainu.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť se zvoleným konsensním mechanismem, který uznává pravidlo nejdelšího řetězce
- Do sítě je připojených a synchronizovaných alespoň 100 uzlů
- Nastavte generátor transakcí, který bude simulovat vysoký provoz v síti
- Připravte nástroje pro monitoring klíčových metrik

Testovací kroky:

1. Spusťte testovací síť s vybraným konsensním mechanismem a simulujte vysoký provoz sítě.
2. Monitorujte síť a sledujte přidávání nových bloků do blockchainu až do doby, kdy je detekován fork (tzn. dva validní bloky ve stejné výšce).
3. Zaznamenejte informace o forku, jako jsou čas, výška, tvůrce bloku, konkrétní transakce v každém bloku.
4. Po vytvoření forku pokračujte v monitorování sítě se zaměřením na jeho stav. Sledujte počet uzlů přijímající každou verzi forku (rozšiřování řetězce), délky řetězců, přidávané bloky a informace o nich.
5. Řešení forku by mělo přijít s přidáním dalšího bloku, který naváže na jednu z větví, čímž se daná větev stane nejdelší a tudíž platnou. Zkontrolujte, zda ostatní uzly opuštěnou větev odstranily a zaznamenejte ty, které se s řešením forku neshodují.

Očekávané výsledky:

Po vytvoření forku by měly uzly udržovat kopii všech řetězců, dokud se konflikt nevyřeší. V síti by mělo dojít ke shodě na jedné verzi blockchainu, čímž se fork vyřeší (většinou nejdelším řetězcem, pokud není nadefinováno jinak). Doba potřebná k vyřešení forku by měla být minimální a všechny uzly by měly opuštěnou větev odstranit.

6.1.6 TS: Čas potřebný pro potvrzení transakce

Cíl:

Cílem testu je změřit dobu potřebnou k potvrzení transakcí, to znamená, kdy se stane nevratnou, při různém vytížení sítě a poskytnout přehled o výkonu škálovatelnosti sítě s využitím daného konsensního mechanismu.

Předpoklady / počáteční nastavení:

- Připravená testovací blockchainová síť s implementovaným konsensním mechanismem
- Nástroje pro simulaci transakcí a jejich monitoring
- Do sítě je připojených a synchronizovaných alespoň 100 uzlů

Testovací kroky:

1. Spusťte testovací síť s vybraným konsensním mechanismem.
2. Generujte a odesílejte transakce do sítě požadovanou rychlostí (nízká/střední/vysoká úroveň provozu).
3. Zaznamenejte časy odeslání transakcí.
4. Sledujte blockchain, a monitorujte časy, kdy jsou dané transakce přidány do bloku a potvrzeny – stanou se nevratné (u konkrétního testovaného mechanismu může být transakce považována za potvrzenou buď pouze přidáním do bloku, nebo může vyžadovat přidání určitého počtu dalších bloků za blok, který transakci zahrnuje).
5. Jakmile jsou transakce potvrzeny, vypočtěte čas, který byl potřebný pro jejich potvrzení.
6. Opakujte kroky 2 až 5 s požadovanou transakční zátěží.
7. Proveďte analýzu časových dat různých úrovní síťového provozu.

Očekávané výsledky:

Doba potvrzení transakce se bude lišit v závislosti na úrovni zatížení sítě a konkrétním implementovaném mechanismu konsensu. Jak se úroveň provozu zvyšuje, lze očekávat prodlužující se dobu potvrzování transakcí, ovšem konkrétně to závisí na škálovatelnosti daného mechanismu. Tento scénář může poskytnout informace o

škálovatelnosti a identifikovat potenciální problematické oblasti související s výkonností.

6.1.7 TS: Vliv transakčního poplatku na zahrnutí do bloku

Cíl:

Cílem je otestovat dopad výše transakčního poplatku, který je buď nižší nebo vyšší než průměrný síťový poplatek, na dobu potřebnou k tomu, aby byla transakce zahrnuta do bloku.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť se zvoleným konsensním mechanismem
- Do sítě je připojených a synchronizovaných na počátku alespoň 100 uzlů
- Nastavte generátor transakcí, který bude simulovat různé úrovně provozu v síti
- Nástroje pro monitoring klíčových metrik
- Je znám průměrný poplatek za transakci
- Ostatní síťové parametry jsou konstantní

Testovací kroky:

1. Spusťte testovací síť s vybraným konsensním mechanismem s nastavenou průměrnou základní hodnotou poplatků a simulujte běžný síťový. Tímto způsobem získejte základní data (průměrná doba zahrnutí transakce do bloku).
2. Vygenerujte skupinu transakcí s nastaveným nižším poplatkem, než je průměr a zaznamenejte časy odeslání do sítě.
3. Zaznamenejte časy, kdy byly tyto jednotlivé transakce zahrnuty do bloku a zjistěte, jak se liší od průměru.
4. Opakujte stejný postup jako v kroku 2 až 3, ale tentokrát vygenerujte skupinu transakcí s vyšším poplatkem, než je průměr a zaznamenejte časy odeslání a zahrnutí transakcí do bloku.
5. Spusťte současně generování transakcí s různými poplatky pro vyhodnocení dopadu smíšených poplatků na zahrnutí transakcí do bloku.
6. Shromážděte a analyzujte data s časy zahrnutí transakcí do bloku.

Očekávané výsledky:

Obecně se očekává, že transakce s vyšším poplatkem budou při zařazování do bloku preferovanější než transakce s průměrným a nižším poplatkem, protože validátoři bloků jsou motivování vyšší odměnou. Transakce s nižšími poplatky mohou být zejména při vyšší síťové zátěži zařazeni až do budoucích bloků. Test poskytuje jasnější pochopení vlivu transakčních poplatků na čas zahrnutí do bloku pro konkrétní konsensní mechanismus, to by mohlo být užitečné při návrhu optimalizací.

6.1.8 TS: Účinnost konsensního mechanismu

Cíl:

Cílem testu je zjistit čas a zdroje potřebné k tomu, aby síť dosáhla konsensu.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť se zvoleným konsensním mechanismem
- Do sítě je připojených a synchronizovaných N uzlů
- Nastavte generátor transakcí, který bude simulovat běžný provoz v síti
- Připravte nástroje pro monitoring sítě a klíčových metrik

Testovací kroky:

1. Spusťte testovací síť s vybraným konsensním mechanismem.
2. Spusťte proces dosažení konsensu bez jakékoliv zátěže a stanovte základní data měření času a zdrojů potřebných pro konsensus (CPU, GPU, paměti, disky, síťový provoz…)
3. Generujte transakce a simulujte průměrnou zátěž sítě.
4. Monitorujte síť a zaznamenávejte data o využití jednotlivých zdrojů.
5. Monitorujte proces konsensu napříč uzly a zaznamenejte čas zahájení jako T1.
6. Určete bod, ve kterém je dosaženo konsensu (přidán nový blok do blockchainu, nebo když je konkrétní transakce ověřena většinou – záleží na mechanismu) a zaznamenejte čas ukončení jako T2.

7. Opakujte kroky 3 až 6 s různými úrovněmi vytíženosti sítě a shromažďujte data o časech (odečtěte T1 od T2) a zdrojích potřebných pro dosažení konsensu.
8. Proveďte analýzu získaných dat.

Očekávané výsledky:

Očekávaným výsledkem je získání dat o době, zdrojích a systémových prostředcích potřebných k dosažení procesu konsensu. Výsledky se budou lišit v závislosti na implementovaném mechanismu, ale obecně by síť měla efektivně dosáhnout konsensu při normální i vysoké zátěži bez nadměrné spotřeby zdrojů a v přijatelném čase.

6.2 Proof of X

6.2.1 TS PoS: Vliv coin-age na úspěšné ověření bloku

Cíl:

Účelem tohoto testu je analyzovat, jak stáří vsazených mincí (coin-age) ovlivňuje pravděpodobnost úspěšného ověření bloku v síti PoS. Ve většině PoS sítích je věk vsazených mincí faktorem v procesu ověřování bloku, který může ovlivnit pravděpodobnost, že se uzel stane validátorem.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť s implementovaným Proof of Stake konsensním mechanismem a předem definovaným počtem N uzlů
- V síti je mechanismus pro kontrolu stáří vsazených mincí
- K dispozici je generátor transakcí, který bude simulovat různé úrovně zátěže

Testovací kroky:

1. Spusťte blockchainovou testovací síť s Proof of Stake konsensním mechanismem se zvolenou sadou validátorů, kteří budou mít vsazený stejný počet mincí a coin-age bude pro všechny stejný s hodnotou X.

2. Nechte síť běžet po omezenou dostatečně dlouhou dobu a zaznamenejte počet bloků vytvořený každým uzlem. Tato data budou sloužit jako základ pro další testovací kroky.
3. Změňte nastavení tak, aby 1/3 validátorů měla coin-age nastavený na 2X, další 1/3 validátorů na 0,5X a zbývající 1/3 na stávající X. Restartujte síť a s tímto nastavením proveďte simulační test jako v předchozím kroku. Na konci testu zaznamenejte data o vytvořených blocích.
4. Proveďte opět změnu coin-age sázek části uzlů. Například u poloviny uzlů coin-age resetujte a u druhé poloviny ponechte nastavení z kroku 3. Znovu proveďte simulační test s aktuálním nastavením a zaznamenejte data o vytvořených blocích.
5. Analyzujte výsledná data ze všech měření.

Očekávané výsledky:

Uzly s vyšším coin-age (déle vsazené mince) by měly mít vyšší pravděpodobnost vytvoření bloku, v kroku 3 by tedy měly uzly, které mají coin-age nastaven na 2X, vytvořit více bloků než ostatní. Naopak uzly v kroku 4, u kterých byl coin-age resetován, měly vytvořit méně bloků.

6.2.2 TS PoI: Snižování skóre důležitosti při neaktivitě v síti

Cíl:

Testovací scénář má za cíl změřit rychlost, s jakou se skóre důležitosti snižuje v čase při neaktivitě uzlu v síti. Výsledek může poskytnout pohled na to, jak rychle může uzel s vysokým skóre důležitosti ztratit vliv v síti, jestliže přestane být aktivní.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť s implementovaným Proof of Importance konsensním mechanismem
- Do sítě je připojených a synchronizovaných N uzlů, které mají rovnoměrně rozdělené zdroje
- Generátor transakcí, který bude simulovat běžný provoz v síti

Testovací kroky:

1. Spusťte blockchainovou testovací síť s Proof of Importance konsensním mechanismem.
2. Simulujte uzel s vysokým zůstatkem kryptoměny a vysokou transakční aktivitou po významnou dobu, aby získal vysoké skóre důležitosti.
3. Monitorujte změny ve skóre důležitosti v pravidelných intervalech.
4. V určitém bodě zastavte veškerou aktivitu uzlu, aby jeho skóre důležitosti začalo klesat, v pravidelných časových intervalech tento pokles monitorujte.
5. Analyzujte data z období růstu i poklesu skóre důležitosti a zjistěte, jak rychle se dokáže vrátit zpět na počáteční hodnotu.

Očekávané výsledky:

Během fáze vysoké síťové aktivity se očekává, že se skóre důležitosti konkrétního uzlu bude zvyšovat, protože PoI zohledňuje transakční aktivitu při výpočtu skóre důležitosti. Po zastavení aktivity bude docházet v čase k pokles skóre důležitosti. Pokud je pozastavení aktivity dlouhodobé, mělo by skóre klesnout až na minimální základní hodnotu. Výsledek testu poskytuje pohled na chování PoI mechanismu na dopad transakční aktivity na skóre důležitosti a rychlost jeho úpadku.

6.2.3 TS PoST: Průměrná doba reakce na výzvu

Cíl:

Cílem tohoto testovacího scénáře je zjistit průměrnou dobu odezvy na výzvu (challenge) v konsensním mechanismu Proof of Space Time. Rychlá reakce na výzvu je v PoST důležitá, protože se jedná o důkaz, že uzel uchovává požadovaná data dostupná po určitý čas.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť s implementovaným Proof of Space Time konsensním mechanismem a předem definovaným počtem N uzlů, kdy část z nich je zapojena do procesu konsensu

- Úložný prostor účastníků konsensu je naplněn daty ze sítě
- Mechanismus pro vytváření výzev a reakcí na ně v náhodných časových intervalech

Testovací kroky:

6. Spusťte blockchainovou testovací síť s Proof of Space Time konsensním mechanismem, v které bude několik uzlů simulujících dokazovatele. Dokazovatelé jsou připraveni přijímat a reagovat na výzvy.
7. V náhodném okamžiku vygenerujte výzvu obsahující požadavek na konkrétní část dat, která by měl mít dokazovatel uložena na svém úložišti. Zaznamenejte přesné časové údaje vytvoření a odeslání výzvy.
8. Dokazovatel obdrží výzvu zaprotokolovanou přesným časovým razítkem a zahájí proces prohledávání dat v jeho úložišti.
9. Jakmile požadovaná data nalezne, vytvoří důkaz, kterým prokazuje, že má stále data v čase uložena. Tento důkaz je poté zpětně zaslán vyzyvateli. Zaznamenejte přesné časy vytvoření a odeslání důkazu.
10. Dle získaných časových údajů vypočítejte dobu odezvy na výzvu odečtením času, kdy byla výzva vytvořena od doby obdržení důkazu.
11. Opakujte kroky 2 až 5 (např. 1000x), abyste získali významnou sadu dat.
12. Analyzujte shromážděná data a vypočítejte průměrnou dobu odezvy. V případě hodnot, které se budou od průměru výrazně lišit, se pokuste identifikovat důvody.

Očekávané výsledky:

Dokazovatel by měl být schopen poskytnout důkaz pro každou vydanou výzvu, aby prokázal, že požadovaná data uchovává nedotčená a dostupná. Ve správně fungující PoST síti by doba odezvy měla být přiměřeně krátká, i když přijatelná hodnota se může lišit v závislosti na konkrétní implementaci a požadavcích. V průběhu testu by nemělo docházet k výraznému prodloužení času odezvy. Pokud ano, může to signalizovat potenciální problémy dokazovatele udržovat data v průběhu času nebo s celkovou škálovatelností sítě.

6.2.4 TS PoET: Spravedlivost volby validátora

Cíl:

Cílem testovacího scénáře je vyhodnotit spravedlivost procesu volby validátora v konsensním mechanismu Proof of Elapsed Time sledováním frekvence výběru každého uzlu.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť s implementovaným Proof of Elapsed Time konsensním mechanismem a předem definovaným počtem N uzlů
- V síti se nenachází škodlivé uzly
- Nástroj, který protokoluje výsledky voleb validátorů
- Generátor transakcí, který bude simulovat běžné vytížení sítě

Testovací kroky:

1. Spusťte blockchainovou testovací síť s Proof of Elapsed Time konsensním mechanismem, ve které bude simulován běžný síťový provoz a transakční aktivita.
2. Nechte síť zpracovávat transakce a vytvářet bloky bez jakéhokoliv zásahu po dostatečně dlouhou stanovenou dobu, dokud nebude do blockchainu přidáno významné množství nových bloků B.
3. Během provádění simulace aktivně monitorujte síť a sbírejte data o validátorech, které vytvářejí nové bloky.
4. Po přidání významného počtu bloků do blockchainu zastavte vytváření nových bloků a analyzujte zaprotokolovaná data o tvůrcích bloků a určete, kolik bloků vytvořil každý uzel.

Očekávané výsledky:

Vzhledem k faktu, že PoET vybírá validátory náhodně pomocí specializovaného hardwaru, by všechny uzly měly mít zhruba stejnou šancí být vybrány, tedy každý uzel by měl být vybrán přibližně B/N krát (počet nově vytvořených bloků během testu děleno počtem uzlů účastnících se konsensu), neměla by existovat žádná významná

odchylka. V případě, že by v síti byla významná odchylka při výběru validátorů, znamenalo by to problém s implementací spravedlnosti v PoET síti.

6.2.5 TS PoAc: Rovnováha mezi PoW a PoS částí

Cíl:

Cílem testovacího scénáře je vyhodnotit rovnováhu mezi těžební (PoW) a validační (PoS) částí v konsensním mechanismu Proof of Activity.

Předpoklady / počáteční nastavení:

- Připravená blockchainová testovací síť s implementovaným Proof of Activity konsensním mechanismem a předem definovaným počtem N uzlů
- K dispozici je generátor transakcí, který bude v síti simulovat běžnou zátěž
- Zdroje jsou mezi účastníky rovnoměrně rozděleny – síť je decentralizovaná

Testovací kroky:

1. Spusťte blockchainovou testovací síť s Proof of Activity konsensním mechanismem, ve které bude simulován běžný síťový provoz a transakční aktivita.
2. Zahajte PoW část a monitorujte časy od začátku těžby až po vytěžení nového prázdného bloku.
3. Přesuňte se k PoS části a rovněž zaznamenejte přesný čas od doby, kdy dorazí nový prázdný blok až po přidání transakcí a dokončení procesu validace.
4. Opakujte kroky 2 a 3 (např. 1000krát) a zaznamenejte doby těžby a validace bloků.
5. Vypočítejte ze získaných dat průměrné časy těžby a validace bloku.
6. Porovnejte výsledky, které vám poskytnou představu o rovnováze či nerovnováze mezi jednotlivými částmi konsensu-
7. Pozorujte dopady rovnováhy nebo nerovnováhy na celkovou výkonnost sítě (TPS, latence, bezpečnost).

Očekávané výsledky:

Rovnováha mezi PoW a PoS částí by měla poskytnout zvýšenou bezpečnost a efektivitu ve srovnání s pouze tradičními PoW nebo PoS konsensními mechanismy. Pokud existuje významná nerovnováha, může to značit potenciální neefektivitu v dosahování konsensu. To by mohlo mít vliv na celkovou výkonnost a bezpečnost sítě.

6.3 Byzantine Fault Tolerance

6.3.1 TS PBFT: Odolnost proti byzantským uzlům

Cíl:

Cílem testovacího scénáře je vyhodnotit, jak efektivně dokáže konsensní mechanismu PBFT detekovat a neutralizovat byzantské uzly v síti.

Předpoklady / počáteční nastavení:

- Připravená testovací síť s implementovaným Practical Byzantine Fault Tolerance konsensním mechanismem a předem definovaným počtem N uzlů, které dodržují pravidla konsensu
- Možnost zavést a ovládat chování určitého procenta byzantských uzlů (hlasování proti většině, pokus o double-spending útok, manipulace s historií)
- Nástroje pro monitoring výkonnosti sítě
- K dispozici je generátor transakcí, který bude v síti simulovat běžnou zátěž
- Zdroje jsou mezi účastníky rovnoměrně rozděleny – síť je decentralizovaná

Testovací kroky:

1. Spusťte testovací síť s PBFT mechanismem bez byzantských uzlů a sledujte její výkonnost, tyto data zaznamenejte jako výchozí bod.
2. Zaveďte do sítě určité procento byzantských uzlů (např. 5 %).
3. Monitorujte nepřetržitě výkon sítě a zaznamenávejte změny při dosahování konsensu, počtu zpráv vyměněných během konsensu a počtu kol.
4. Analyzujte a porovnejte výsledky s daty z výchozího bodu.

5. Postupně zvyšujte procento byzantských uzlů v síti a sledujte změny při konsensu s každým přírůstkem.
6. V průběhu času analyzujte chování zbytku sítě vůči byzantským uzlům (např. ignorování jejich zpráv nebo další prostředky mechanismu pro izolaci byzantských uzlů).

Očekávané výsledky:

Mechanismus PBFT je navržen tak, aby zvládl určité procento (většinou 1/3) byzantských uzlů v síti a měl by být schopen nadále efektivně fungovat. Snižování výkonnosti sítě by mělo být procentuálně úměrné zavedeným byzantským uzlům. Síť by měla časem tyto uzly postupně izolovat. V případě, že by síť ovládla podstatná část byzantských uzlů, může docházet k úspěšným útokům a ovládnutí sítě.

6.3.2 TS ABFT: Validace gossip protokolu

Cíl:

Cílem tohoto testovacího scénáře je zhodnotit, jak rychle a efektivně se informace o nové transakci šíří sítí s konsensním mechanismem Asynchronous Byzantine Fault Tolerance a jak rychle může s využitím gossip protokolu dosáhnout konsensu.

Předpoklady / počáteční nastavení:

- Připravená testovací síť s implementovaným ABFT konsensním mechanismem a dostatečným předem definovaným počtem N uzlů (1000), pro správné ověření šíření informací
- Monitorovací nástroje, které jsou schopné sledovat a zaznamenávat jednotlivé kroky komunikace mezi uzly včetně časů a dosažení konsensu
- Generátor transakcí pro sledování šíření informací

Testovací kroky:

1. Spusťte testovací síť s ABFT mechanismem a vytvořte novou transakci v konkrétním uzlu A.

2. Uzel A by měl automaticky zahájit proces gossip, kdy náhodně informuje několik dalších uzlů o nově vytvořené transakci.
3. Sledujte a zaznamenávejte časy šíření transakce v prvním kole, zaznamenejte uzly, které informaci o nové transakci obdržely jako první (od uzlu A).
4. Pokračujte ve sledování a zaznamenávání šíření transakce v dalších kolech (gossip about gossip). Tyto uzly obdržely informaci o transakci od jiných uzlů než A. Sledujte, kdo od koho obdržel informace a jak rychle se šíří.
5. Zaznamenejte časy dosažení konsensu ohledně dané transakce u jednotlivých uzlů – konsensu je dosaženo, když uzel obdrží potvrzení o transakci od více než 2/3 uzlů.
6. Analyzujte získaná data o tom, jak se informace o transakci šířila sítí a jak dlouho trvalo uzlům dosáhnout konsensu. Je důležité, aby čas dosažení konsensu byl pro všechny uzly bez výjimky podobný.
7. Porovnejte časy dosažení konsensu pro uzly, které obdržely informaci přímo od uzlu A a pro uzly, které obdržely info od jiných uzlů. Detekujte případné významné rozdíly.

Očekávané výsledky:

Informace o nové transakcí vy se sítí měla šířit velmi rychle právě díky gossip protokolu. Čas dosažení konsensu by měl pro všechny uzly být podobný bez ohledu na to, kdy informaci o transakci obdržely. Síť by měla velmi efektivně dosáhnout konsensu, což by dokazovalo správnou funkci gossip protokolu.

6.4 Crash Fault Tolerance

6.4.1 TS Raft: Výběr vůdce

Cíl:

Cílem je ověřit a zkontrolovat, že proces výběru vůdce v Raft mechanismu je správně implementován a dojde k němu v případě, že aktuální vůdce není dostupný a uzly od něj nemají po určitou dobu žádnou informaci. Cílem je také zjistit, jak rychle je vůdce nahrazen.

Předpoklady / počáteční nastavení:

- Připravená testovací síť s implementovaným Raft konsensním mechanismem a předem definovaným nižším počtem N uzlů
- Monitorovací nástroje pro sledování a zaznamenávání aktivity v síti (komunikace, volba vůdce)
- Kontrola nad uzly sítě a možnost simulace nedostupnosti vůdce

Testovací kroky:

1. Spusťte testovací síť s Raft mechanismem a identifikujte aktuálního vůdce v síti.
2. Nastavte vůdce do stavu nedostupnosti, kdy neodesílá do sítě informaci o svém stavu.
3. Vyčkejte, až uplyne nakonfigurovaná doba (timeout) a ostatní uzly zahájí proces volby nového vůdce tím, že se prohlásí za kandidáty a odešlou ostatním uzlům volební zprávy. Sledujte komunikaci mezi uzly a ověřte si, že tento proces opravdu nastal.
4. Uzly by měly odpovědět na volební zprávy hlasováním pro vybraného kandidáta (každý uzel má jeden hlas).
5. Kandidát, který získá nejvíce hlasů, se stane novým vůdcem.
6. Monitorujte a zaznamenejte celý proces voleb a výběru vůdce (komunikace, změny stavů), časy, kdy byly volby zahájeny a kdy byl zvolen nový vůdce. Vypočítejte dobu, která mezi těmito událostmi uplynula.
7. Analyzujte výsledky, které by měly ukázat, jak rychle dojde k volbě nového vůdce poté, co selže původní.

Očekávané výsledky:

Po určité době, co se vůdce odmlčí (selže), by měly uzly automaticky zahájit proces voleb, který by měl proběhnout bez problému s uzly hlasujícími pro kandidáty, kdy vítězem se stane ten uzel, který získá nejvíce hlasů. Nově zvolený vůdce by měl odesílat ostatním uzlům informaci o svém stavu a koordinovat síť.

7 Doporučení

Z provedené komparativní analýzy konsensních mechanismů nelze jednoznačně říci, že existuje nejlepší a nejhorší mechanismus, jelikož každý mechanismus byl vytvořen za jiným účelem a zaměřením na konkrétní oblast, ve které se snaží excelovat. Dle bodového hodnocení je ovšem patrné, že mechanismy s vysokým celkovým skóre se snaží ve vybraných kritériích excelovat a ostatní rozumně vyvažovat. Na druhé straně mechanismy s nižším celkovým skóre budou pravděpodobně sloužit pro více specifické použití, což nutně neznamená, že se jedná o horší mechanismy, jen jejich možnosti implementace budou omezenější.

Z hlediska bodového a váženého hodnocení získaly nejvyšší počet bodů mechanismy ABFT, FBA, SPoS a DBFT. Všechny tyto mechanismy vynikají v transakční propustnosti a škálovatelnosti, z hlediska bezpečnosti a decentralizace jsou stále na dobré nebo přijatelné úrovni. Tyto mechanismy jsou vhodné pro využití ve veřejných robustních sítí a různých aplikacích, kde je prioritní požadavek na extrémní škálovatelnost a transakční propustnost. Jedná se ovšem o poměrně nové mechanismy, které jsou na rozdíl od tradičních mechanismů velmi složité na implementaci a nejsou tak prověřené.

Mechanismy, které získaly celkově průměrné hodnocení jsou většinou tradiční mechanismy, jako je PoW, PoS a jejich odvozené varianty. Tyto mechanismy jsou nejvíce rozšířenými a prověřenými mechanismy, jejichž výhody i nedostatky jsou dobře známé. Jejich využití je rovněž vhodné pro veřejné sítě s požadavkem na bezpečnost a decentralizaci. PoS je svojí energetickou účinností vhodnou náhradou za PoW, který je vzhledem ke způsobu dosahování konsensu vhodný pouze pro kryptoměny a platební systémy s nižší propustností. PoS a jeho varianty, které se snaží hledat kompromisní řešení v jiných kritériích, na druhé straně umožňují širší škálu využitelnosti například pro smart kontrakty, De-Fi nebo dApps.

Proof of Capacity a jeho odvozené varianty získaly nižší hodnocení než tradiční PoW a PoS, patří mezi málo škálovatelné a celkově méně efektivní mechanismy, svojí podstatou jsou vhodné pro veřejné sítě a aplikace typu decentralizované úložiště dat, nicméně tento typ mechanismů není příliš adoptován, což se odráží i na stagnujícím vývoji.

Mezi mechanismy, které jsou výborně využitelné v privátních a konsorciálních sítí patří Proof of Authority a Proof of Elapsed Time, což ukázalo i bodové hodnocení. Tyto mechanismy jsou právě určené pro toto více specifické užití, kde je vyšší důvěra mezi účastníky. PoAu nabízí za cenu centralizace vysokou škálovatelnost v distribuovaném systému, PoET naopak zase v privátní síti umožňuje decentralizovaný výběr tvůrce bloku. Ačkoliv tyto mechanismy nejsou ideální pro všechny scénáře, mohou být vynikající volbou pro určité aplikace a užití na podnikové úrovni, což zdůrazňuje skutečnost, že "nejlepší" konsensní mechanismus závisí opravdu na konkrétních požadavcích a omezeních daného systému.

Paxos a Raft jsou typy konsensních mechanismů, které se obvykle používají v distribuovaných systémech. Na rozdíl od blockchainových konsensních mechanismů jsou založeny na koordinaci mezi uzly a navrženy pro běžné distribuované databázové systémy a úložiště dat.

Ve všech případech je důležité si uvědomit, že volba konsensního mechanismu by měla vycházet z konkrétních požadavků dané aplikace nebo sítě. Každý mechanismus má své výhody a nevýhody a neexistuje jedno "nejlepší" řešení pro všechny situace. Místo toho je důležité pečlivě zvážit potřeby dané situace a vybrat nejvhodnější mechanismus na základě těchto požadavků.

8 Závěr

Tato diplomová práce se zabývala hloubkovou analýzou různých mechanismů konsensu, které jsou kritickou součástí distribuovaných systémů založených na technologii účetní knihy.

První část práce byla zaměřena na rešerši technologie distribuované účetní knihy, jako jsou blockchain, sidechain, DAG, BlockDAG, Hashgraph, Holochain a Tempo (Radix DLT). Toto poskytuje čtenáři širší rámec pro pochopení, jak se tyto různé technologie liší a jak mohou být použity. Následně se práce zabývá problematikou konsensních mechanismů. Vzhledem k faktu, že existují až tisíce mechanismů v různých stádiích vývoje a nasazení, jsou vybrány a detailně popsány pouze ty s úspěšnou a reálnou implementací. Mechanismy jsou rozděleny do základních charakteristických skupin, jako jsou tradiční algoritmy založené na důkazech, které zahrnují Proof of Work, Proof of Stake, Proof of Capacity a jejich odvozené varianty, poté alternativní algoritmy založené na důkazech, sem patří mechanismy, které vznikly buď jako hybridy tradičních algoritmů nebo jako úplně nové algoritmy založené na důkazech. Další skupinou jsou Fault Tolerance algoritmy, které se dělí na Byzantine Fault Tolerance a Crash Fault Tolerance, dokonce je zde popsána i skupina algoritmů založených na DAG, která zahrnuje konsensní algoritmus Tangle.

V další části práce byla provedena komparativní analýza a hodnocení popsaných konsensních mechanismů, čemuž nejdříve předcházela obecná identifikace rizik spojených s konsensními mechanismy a stanovení a popsání jednotlivých kritérií hodnocení. Kritéria hodnocení zahrnují celkovou bezpečnost, úroveň decentralizace, typ síťového modelu, škálovatelnost, transakční propustnost, finalitu, energetickou účinnost a model protivníka. Všech 22 vybraných konsensních mechanismů bylo v těchto 8 kritériích hodnoceno jak slovně, tak i bodově a váhově. Zvolená kritéria umožnila provést podrobné hodnocení jednotlivých mechanismů a poukázat na rozdíly mezi nimi.

Dále se práce zabývá metodickým návrhem rozsáhlé sady testovacích scénářů pro vybrané konsensní mechanismy s cílem testovat různé specifické situace. Vzhledem k rozsahu hodnocených mechanismů byly k otestování některých z navržených scénářů využity dostupné open-source simulátory BlockSim a TangleSimulator. Sada testovacích scénářů poskytuje rámec pro další testování a výzkum v tomto směru.

V závěru bylo na základě analýz a hodnocení poskytnuto konkrétní doporučení pro využití jednotlivých mechanismů. Tato doporučení jsou určena jako průvodce pro vývojáře a rozhodovatele, kteří se snaží využít distribuované účetní knihy v různých aplikacích. Práce je důkazem, že neexistuje univerzálně nejlepší konsensní mechanismus pro všechny situace. Naopak analýza ukázala, že každý mechanismus má své silné a slabé stránky a je důležité zvolit vhodný mechanismus na základě specifických požadavků a omezení daného systému.

Diplomová práce několik významných přínosů. Prvním z nich je jednotný a detailní popis jednotlivých konsensních mechanismů, což usnadňuje pochopení a studium této problematiky. Dalším přínosem je komparativní analýza, která umožňuje objektivně porovnat mechanismy a identifikovat jejich silné a slabé stránky. Finálním přínosem jsou testovací scénáře, které nabízejí cenné poznatky pro budoucí experimentování a testování konsensních algoritmů a mohou mimo jiné sloužit i jako výchozí bod pro vytvoření sofistikovanějších simulátorů konsensních mechanismů.

Summary

This Master's thesis provides a comprehensive analysis of various consensus mechanisms essential for distributed ledger technologies like blockchain, sidechain, DAG, and more. A total of 22 consensus mechanisms, including traditional and alternative proof-based algorithms, fault tolerance algorithms, and DAG-based algorithms, were evaluated using eight criteria such as security, decentralization, scalability, and energy efficiency.

The study includes an extensive set of testing scenarios for these mechanisms, and recommendations are given based on the analysis of individual mechanisms, emphasizing the importance of choosing mechanisms suited to specific system requirements. The research contributes significantly to the field by providing a detailed understanding of consensus mechanisms, a comparative analysis highlighting their strengths and weaknesses, and valuable test scenarios for future studies.

Seznam literatury

[1] N. Kannengießer, „Mind the Gap: Trade-Offs Between Distributed Ledger Technology Characteristics (Working Paper),“ 2019. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1906/1906.00861.pdf.

[2] M. Khan, „A Review of Distributed Ledger Technologies in the Machine Economy:,“ 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212827122004103.

[3] A. M. Antonopoulos, Mastering Bitcoin, O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2017.

[4] H. Dai, „An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends,“ 2017. [Online]. Available: https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends.

[5] G. Iredale, „Blockchain Definition: Everything You Need To Know,“ 101blockchains.com, 2020. [Online]. Available: https://101blockchains.com/blockchain-definition/.

[6] W. Yao, „A Survey on Consortium Blockchain ConsensusMechanisms,“ 2021. [Online]. Available: https://www.researchgate.net/publication/349583511_A_Survey_on_Consortium_Blockchain_Consensus_Mechanisms.

[7] K. E. W. E. Wang, „Types of Blockchain: Public, Private, or Something in Between,“ 2021. [Online]. Available: https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between.

[8] „Permissioned blockchain,“ Oracle, 2022. [Online]. Available: https://developer.oracle.com/learn/technical-articles/permissioned-blockchain.

[9] S. SETH, „Public, Private, Permissioned Blockchains Compared,“ Investopedia, 2022. [Online]. Available: https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/.

[10] S. Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System,“ 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[11] H. Anwar, „What Is A Private Blockchain? Beginner’s Guide,“ 101blockchains.com, 2021. [Online]. Available: https://101blockchains.com/what-is-a-private-blockchain/.

[12] H. Anwar, „Federated Blockchain – Blockchain Consortium Simply Explained,“ 101blockchains.com, 2018. [Online]. Available: https://101blockchains.com/federated-blockchain/.

[13] O. Innocent, „Hybrid And Federated Blockchain Networks,“ medium.com, 2020. [Online]. Available: https://medium.com/xord/hybrid-and-federated-blockchain-networks-4508624f10c4.

[14] D. R. Chamria, „Guide to Hybrid Blockchain, Benefits and Use Cases,“ zeeve.io, 2022. [Online]. Available: https://www.zeeve.io/blog/guide-to-hybrid-blockchain-benefits-and-use-cases/.

[15] Grace, „What are sidechains? [2022 Guide],“ limechain.tech, 2022. [Online]. Available: https://limechain.tech/blog/what-are-sidechains/.

[16] U. C. Çabuk, „Sidechains: Highlights and Challenges,“ 2019. [Online]. Available: https://www.researchgate.net/publication/335368901_Sidechains_Highlights_and_Challenges.

[17] M. Deer, „What is a directed acyclic graph in cryptocurrency? How does DAG work?,“ cointelegraph.com, 2021. [Online]. Available: https://cointelegraph.com/explained/what-is-a-directed-acyclic-graph-in-cryptocurrency-how-does-dag-work.

[18] H. Pervez, „A Comparative Analysis of DAG-Based Blockchain Architectures,“ 2018. [Online]. Available: https://www.researchgate.net/publication/330880551_A_Comparative_Analysis_of_DAG-Based_Blockchain_Architectures.

[19] „DAG the DLT! Directed Acyclic Graph for Enterprise Blockchain!,“ cbcamerica.org, 2019. [Online]. Available: https://www.cbcamerica.org/blockchain-insights/dag-the-dlt-directed-acyclic-graph-for-enterprise-blockchain.

[20] M. Perešíni, „DAG-Oriented Protocols PHANTOM and GHOSTDAG under Incentive Attack via Transaction Selection Strategy,“ 2021. [Online]. Available: https://www.researchgate.net/publication/354329329_DAG-Oriented_Protocols_PHANTOM_and_GHOSTDAG_under_Incentive_Attack_via_Transaction_Selection_Strategy.

[21] „What is a DAG? Directed Acyclic Graphs,“ horizen.io, 2023. [Online]. Available: https://www.horizen.io/blockchain-academy/horizen/advanced/block-dag/ .

[22] A. Carrillo, „An introduction to the blockDAG paradigm,“ ancapalex.medium.com, 2018. [Online]. Available: https://ancapalex.medium.com/an-introduction-to-the-blockdag-paradigm-50027f44facb#.

[23] M. S. Ali, „Applications of Blockchains in theInternet of Things: A Comprehensive Survey,“ 2018. [Online]. Available: https://www.researchgate.net/publication/329763546_Applications_of_Blockchains_in_the_Internet_of_Things_A_Comprehensive_Survey .

[24] P. Muens, „Hashgraph, The better Blockchain?!,“ pmuens.medium.com, 2018. [Online]. Available: https://pmuens.medium.com/hashgraph-b79f901add20.

[25] J. FRANKENFIELD, „Hashgraph Consensus,“ investopedia.com, 2022. [Online]. Available: https://www.investopedia.com/terms/h/hashgraph-consensus-mechanism.asp.

[26] M. H. a. P. M. Dr. Leemon Baird, „Hedera: A Public Hashgraph Network & Governing Council,“ 2020. [Online]. Available: https://hedera.com/hh_whitepaper_v2.1-20200815.pdf.

[27] Y. S. Kıyak, „Holochain: a novel technology without scalability bottlenecks of blockchain for secure data exchange in health professions education,“ 2022. [Online]. Available: https://link.springer.com/article/10.1007/s44217-022-00013-y.

[28] „How the Holochain framework works,“ holochain.org, [Online]. Available: https://www.holochain.org/how-does-it-work/.

[29] 1. Blockchains, „Holochain Ultimate Guide: Better Technology Than Blockchain?,“ 101blockchains.com, 2019. [Online]. Available: https://101blockchains.com/holochain-blockchain-guide/.

[30] L. Lamport, „Time, Clocks, and the Ordering of Events in a Distributed System,“ 1978. [Online]. Available: https://lamport.azurewebsites.net/pubs/time-clocks.pdf.

[31] „Tempo - Consensus Lessons Learned,“ radixdlt.com, 2020. [Online]. Available: https://www.radixdlt.com/blog/tempo-consensus-lessons-learned.

[32] S. Dexter, „Radix DLT: Tempo’s Logical Clocks Explained Simply,“ mangoresearch.co, 2018. [Online]. Available: https://www.mangoresearch.co/radix-dlt-logical-clocks-explained/.

[33] S. Dexter, „RadixDLT Sharding Explained: Scalability Done Right,“ 2018. [Online]. Available: https://www.mangoresearch.co/radixdlt-sharding-scalability/ .

[34] V. Sevan, „Tempo - Radix : Examples Of Consensus Protocols,“ 2019. [Online]. Available: https://medium.com/@vardan.sevan/tempo-radix-examples-of-consensus-protocols-339e14c0abee.

[35] „Czech Republic - Energy,“ trade.gov, 2022. [Online]. Available: https://www.trade.gov/country-commercial-guides/czech-republic-energy.

[36] „Cambridge Bitcoin Electricity Consumption,“ ccaf.io, 2023. [Online]. Available: https://ccaf.io/cbeci/index.

[37] A. Back, „Hashcash - A Denial of Service Counter-Measure,“ 2002. [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf.

[38] A. O. Bada, „Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption,“ 2021. [Online]. Available: https://eprints.bournemouth.ac.uk/36968/1/GREEN_BLOCKCHAIN.pdf.

[39] „The Komodo Solution: Delayed Proof Of Work (dPOW),“ developers.komodoplatform.com, [Online]. Available: https://developers.komodoplatform.com/basic-docs/start-here/core-technology-discussions/delayed-proof-of-work.html#the-komodo-solution-delayed-proof-of-work-dpow.

[40] „Komodo (Advanced Blockchain Technology, Focused On Freedom),“ docs.komodoplatform.com, 2019. [Online]. Available: https://docs.komodoplatform.com/whitepaper/introduction.html#intoduction-to-komodo.

[41] K. Team, „51% Attack Security: Delayed Proof of Work (dPoW),“ komodoplatform.com, 2018. [Online]. Available: https://komodoplatform.com/en/blog/delayed-proof-of-work/.

[42] S. N. Sunny King, „PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,“ 2012. [Online]. Available: https://www.peercoin.net/read/papers/peercoin-paper.pdf .

[43] „Peercoin University,“ [Online]. Available: https://www.peercoin.net/university/#/1-introduction .

[44] M. Ghorbanzadeh, „PROOF-OF-STAKE (POS),“ ethereum.org, 2023. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ .

[45] „Block.one - High Performance Blockchain Solutions,“ [Online]. Available: https://b1.com/ .

[46] I. Grigg, „EOS - An Introduction,“ 2018. [Online]. Available: https://www.allcryptowhitepapers.com/eos-whitepaper/.

[47] block.one, „EOS.IO Technical White Paper v2,“ 2018. [Online]. Available: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md .

[48] K. S. a. T. J. Myles Snider, „Delegated Proof of Stake: Features & Tradeoffs,“ 2018. [Online]. Available: https://holbrook.no/share/papers/DPoS_-Features-and-Tradeoffs.pdf.

[49] Paul, „What Is Leased Proof of Stake (LPoS) and How Does it Work?,“ 2023. [Online]. Available: https://www.gate.io/learn/articles/what-is-leased-proof-of-stake-and-how-does-it-work/374.

[50] w. Docs, „Leasing,“ [Online]. Available: https://docs.waves.tech/en/blockchain/leasing#leasing-benefits-for-waves-holder.

[51] „MultiversX,“ [Online]. Available: https://multiversx.com/ .

[52] M. Docs, „Secure Proof of Stake,“ [Online]. Available: https://docs.multiversx.com/technology/secure-proof-of-stake/.

[53] MultiversX, „MultiversX - A Highly Scalable Public Blockchain via Adaptive State Sharding and Secure Proof of Stake,“ 2019. [Online]. Available: https://files.multiversx.com/multiversx-whitepaper.pdf.

[54] nem, „What is POI,“ [Online]. Available: https://nemproject.github.io/nem-docs/pages/Concepts/what-is-poi/docs.en.html.

[55] n. project, „NEM Technical Reference,“ 2018. [Online]. Available: https://nemproject.github.io/nem-docs/pages/Whitepapers/NEM_techRef.pdf .

[56] „Signum Mining: Introduction,“ [Online]. Available: https://signum.community/signum-mining/.

[57] error_502, „Proof of Capacity,“ geeksforgeeks.org, 2022. [Online]. Available: https://www.geeksforgeeks.org/proof-of-capacity/.

[58] I. O. Tal Moran, „Simple Proofs of Space-Time and Rational Proofs of Storage,“ 2013. [Online]. Available: https://eprint.iacr.org/2016/035.pdf .

[59] „Filecoin: A Decentralized Storage Network,“ 2017. [Online]. Available: https://filecoin.io/filecoin.pdf .

[60] D. D. N. G. Juan Benet, „Proof of Replication,“ 2017. [Online]. Available: https://filecoin.io/proof-of-replication.pdf .

[61] f. docs, „Network performance - Filecoin docs,“ [Online]. Available: https://docs.filecoin.io/networks/mainnet/network-performance/.

[62] A. J. E. S. B. P. J. K. Andrew Miller, „Permacoin: Repurposing Bitcoin Work for Data Preservation,“ 2014. [Online]. Available: https://ieeexplore.ieee.org/document/6956582.

[63] A. J. A. O. Kevin D. Bowers, „Proofs of Retrievability: Theory and Implementation,“ 2008. [Online]. Available: https://www.researchgate.net/publication/220337186_Proofs_of_Retrievability_Theory_and_Implementation.

[64] S. B. S. R. K. S. Binanda Sengupta, „Retricoin: Bitcoin Based on Compact Proofs of Retrievability,“ 2016. [Online]. Available: https://www.isical.ac.in/~binanda_r/publications/ICDCN2016.pdf.

[65] „Globally Distributed Cloud Object Storage,“ [Online]. Available: https://www.storj.io/.

[66] A. K. D. Z. Kostis Karantias, „Proof-of-Burn,“ 2019. [Online]. Available: https://eprint.iacr.org/2019/1096.pdf.

[67] P4Titan, „Slimcoin - A Peer-to-Peer Crypto-Currency with Proof-of-Burn,“ 2014. [Online]. Available: https://slimcoin.info/whitepaperSLM.pdf.

[68] „Proof of Burn - Bitcoin wiki,“ [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_burn.

[69] A. Mackenzie, „MEMCOIN2: A HYBRID PROOF-OF-WORK,PROOF-OF-STAKE CRYPTO-CURRENCY,“ 2013. [Online]. Available: https://decred.org/research/mackenzie2013.pdf.

[70] C. L. A. M. M. R. Iddo Bentov, „Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake,“ 2013. [Online]. Available: https://eprint.iacr.org/2014/452.pdf.

[71] „Decred Documentation,“ [Online]. Available: https://docs.decred.org/.

[72] navk1602, „Proof of Elapsed Time(PoET) in Blockchain,“ 2023. [Online]. Available: https://www.geeksforgeeks.org/proof-of-elapsed-time-poet-in-blockchain/.

[73] „Hyperledger Sawtooth,“ [Online]. Available: https://sawtooth.hyperledger.org/.

[74] D. D. A. M. Mic Bowman, „On Elapsed Time Consensus Protocols,“ 2021. [Online]. Available: https://eprint.iacr.org/2021/086.pdf.

[75] A. CORSO, „PERFORMANCE ANALYSIS OF PROOF-OF-ELAPSED-TIME (POET) CONSENSUS IN THE SAWTOOTH BLOCKCHAIN FRAMEWORK,“ 2019. [Online]. Available: https://www.cs.uoregon.edu/Reports/MS-201906-Corso.pdf .

[76] V. Arasev, „POA Network Whitepaper,“ 2018. [Online]. Available: https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper.

[77] „Kovan Testnet,“ [Online]. Available: https://kovan-testnet.github.io/website/.

[78] R. L. Q. W. S. C. Y. X. Qin Wang, „Exploring Unfairness on Proof of Authority: Order Manipulation Attacks and Remedies,“ 2022. [Online]. Available: https://arxiv.org/pdf/2203.03008.pdf.

[79] P. Szilágyi, „EIP-225: Clique proof-of-authority consensus protocol,“ 2017. [Online]. Available: https://eips.ethereum.org/EIPS/eip-225 .

[80] R. S. M. P. LESLIE LAMPORT, „The Byzantine Generals Problem,“ 1982. [Online]. Available: https://lamport.azurewebsites.net/pubs/byz.pdf .

[81] G. Wang, „SoK: Understanding BFT Consensus in the Age of Blockchains,“ 2021. [Online]. Available: https://eprint.iacr.org/2021/911.pdf.

[82] M. C. a. B. Liskov, „Practical Byzantine Fault Tolerance,“ 1999. [Online]. Available: https://pmg.csail.mit.edu/papers/osdi99.pdf.

[83] P. Hooda, „practical Byzantine Fault Tolerance(pBFT),“ 2022. [Online]. Available: https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/.

[84] M. Z. T. C. Yong Wang, „Research on PBFT consensus algorithm for grouping based on feature trust,“ 2022. [Online]. Available: https://www.nature.com/articles/s41598-022-15282-8.

[85] „Neo Documentation,“ [Online]. Available: https://docs.neo.org/docs/en-us/index.html.

[86] V. N. C. R. P. A. W. Y. Q. B. D. R. Igor M. Coelho, „Challenges of PBFT-Inspired Consensus for Blockchain and Enhancements over Neo dBFT,“ 2020. [Online]. Available: https://www.mdpi.com/1999-5903/12/8/129.

[87] R. L. S. C. Y. X. Qin Wang, „Formal Security Analysis on dBFT Protocol of NEO,“ 2022. [Online]. Available: https://arxiv.org/pdf/2105.07459.pdf.

[88] „Hashgraph Developers,“ [Online]. Available: https://hashgraph.github.io/.

[89] A. L. Leemon Baird, „The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers,“ 2020. [Online]. Available: https://hedera.com/hh-ieee_coins_paper-200516.pdf.

[90] N. Okeke, „Hashgraph: Meaning, Advantages, Disadvantages & More,“ 2023. [Online]. Available: https://targettrend.com/hashgraph/ .

[91] D. MAZIERES, „The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus,“ 2017. [Online]. Available: https://stellar.org/papers/stellar-consensus-protocol .

[92] Y. J. D. S. M. B. Junghun Yoo, „Formal Modeling and Verification of a Federated Byzantine Agreement Algorithm for Blockchain Platforms," 2019. [Online]. Available: https://www.researchgate.net/publication/331750023_Formal_Modeling_and_Verification_of_a_Federated_Byzantine_Agreement_Algorithm_for_Blockchain_Platforms .

[93] Y. K. Y. K. Minjeong Kim, „Is Stellar As Secure As You Think?," 2019. [Online]. Available: https://arxiv.org/pdf/1904.13302.pdf .

[94] „Stellar Network Explorer," [Online]. Available: https://stellarbeat.io/?view=map.

[95] R. CHAMI, „Your Journey To Consensus (Part 1) — Crash Fault Tolerance and Paxos," 2019. [Online]. Available: https://medium.com/@chamirachid/your-journey-to-consensus-part-1-6a88a6f818f6.

[96] M. Burrows, „The Chubby lock service for loosely-coupled distributed systems," 2006. [Online]. Available: https://storage.googleapis.com/pub-tools-public-publication-data/pdf/c64be13661eaea41dcc4fdd569be4858963b0bd3.pdf.

[97] L. Lamport, „The Part-Time Parliament," 1998. [Online]. Available: https://lamport.azurewebsites.net/pubs/lamport-paxos.pdf.

[98] L. Lamport, „Fast Paxos," 2005. [Online]. Available: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/tr-2005-112.pdf .

[99] ,. L. E. B. Gustavo M. D. Vieira, „The Performance of Paxos and Fast Paxos," 2013. [Online]. Available: https://arxiv.org/pdf/1308.1358.pdf.

[100] „GoQuorum,“ [Online]. Available: https://github.com/ConsenSys/quorum.

[101] J. O. Diego Ongaro, „In Search of an Understandable Consensus Algorithm (Extended Version),“ 2014. [Online]. Available: https://raft.github.io/raft.pdf .

[102] J. S. J. S. S. L. H. Peter W. Eklund, „Crash vs Byzantine fault tolerance at scale: the cost of distributing trust in a (trans)national invoicing system,“ 2021. [Online]. Available: https://www.researchgate.net/publication/354616560_Crash_vs_Byzantine_fault_tolerance_at_scale_the_cost_of_distributing_trust_in_a_transnational_invoicing_system.

[103] P. Krzyzanowski, „Raft distributed consensus,“ 2021. [Online]. Available: https://people.cs.rutgers.edu/~pxk/417/notes/raft.html.

[104] „Tangle Vs Blockchain: What’s the Difference?,“ 2022. [Online]. Available: https://shardeum.org/blog/tangle-vs-blockchain/.

[105] „Consensus in the IOTA Tangle — FPC,“ 2019. [Online]. Available: https://blog.iota.org/consensus-in-the-iota-tangle-fpc-b98e0f1e8fa/.

[106] S. Popov, „The Tangle,“ 2018. [Online]. Available: https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.4.2.pdf .

[107] P. M. Moritz Platt, „Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance,“ 2023. [Online]. Available: https://www.mdpi.com/1999-4893/16/1/34.

[108] H. M.-G. Sarwar Sayeed, „Assessing Blockchain Consensus and SecurityMechanisms against the 51% Attack,“ 2019. [Online]. Available: https://www.researchgate.net/publication/332737156_Assessing_Blockchain_Consensus_and_Security_Mechanisms_against_the_51_Attack .

[109] C. Patsakis, „https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8653269,“ 2019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8653269.

[110] M. P. S. S. N. P. Olanrewaju Sanda, „Long-Range attack detection on permissionless blockchains using Deep Learning,“ 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417423001070.

[111] „Eclipse Attacks: Explanations and Preventions,“ 2022. [Online]. Available: https://www.gemini.com/cryptopedia/eclipse-attacks-defense-bitcoin.

[112] H. W. H. H. Q. W. Weijian Zhang, „Selfish Mining and Defending Strategies in the Bitcoin,“ 2022. [Online]. Available: https://techscience.com/iasc/v34n3/47952/html.

[113] „The “Selfish Mining” saga continues,“ [Online]. Available: https://coingeek.com/selfish-mining.

[114] W.-K. H. Choi, „A Survey of Proof of Stake Consensus Algorithm,“ 2020. [Online]. Available: http://dpnm.postech.ac.kr/papers/APNOMS/20/wonseok_apnoms2020.pdf .

[115] G. Sigurdsson, A. Giaretta a N. Dragoni, „Vulnerabilities and Security Breaches in Cryptocurrencies,“ 2020. [Online]. Available: https://backend.orbit.dtu.dk/ws/portalfiles/portal/255563695/main.pdf.

[116] R. CHAGANTI, „A Comprehensive Review of Denial of Service Attacks in Blockchain Ecosystem and Open Challenges,“ 2020. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9881505.

[117] C. Z. Z. L. Z. W. Y. L. Chuyi Yan, „Blockchain abnormal behavior awareness methods: a survey,“ 2022. [Online]. Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00107-4.

[118] „Bitcoin Energy Consumption Index,“ [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption.

[119] „Lightning Network,“ [Online]. Available: https://lightning.network.

[120] „Litecoin,“ [Online]. Available: https://litecoin.com/en/.

[121] „Cardano,“ [Online]. Available: https://cardano.org.

[122] „TRON,“ [Online]. Available: https://tron.network.

[123] „Burstcoin,“ [Online]. Available: https://www.burst-coin.org.

[124] „Chia,“ [Online]. Available: https://www.chia.net.

[125] „VeChain,“ [Online]. Available: https://www.vechain.org/about-vechainthor/.

[126] „XRP,“ [Online]. Available: https://xrpl.org.

[127] „Hyperledger Fabric,“ [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/orderer/ordering_service.html.

[128] A. Penzkofer, „PARASITE CHAIN DETECTION IN THE IOTA PROTOCOL,“ 2020. [Online]. Available: https://arxiv.org/pdf/2004.13409.pdf.

[129] „BlockSim,“ [Online]. Available: https://github.com/maher243/BlockSim.

[130] „TangleSimulator,“ [Online]. Available: https://github.com/minh-nghia/TangleSimulator.

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam příloh

Příloha 1 – Results_BlockSim.zip