Jihočeská univerzita v Českých Budějovicích
Ekonomická fakulta
Katedra aplikované matematiky a informatiky

Teze diplomové práce

Komparativní hodnocení mechanismů konsensu v kryptoměnách

Vypracoval: Bc. Tadeáš Pekárek

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

České Budějovice

Rok 2023

Klíčová slova: kryptoměny, konsensní mechanismy, analýza, komparativní hodnocení
Anotace: Tato diplomová práce poskytuje komplexní analýzu různých mechanismů konsensu, které jsou nezbytné pro distribuované účetní technologie jako blockchain, sidechain, DAG a další. Celkem 22 konsensních mechanismů včetně tradičních a alternativních algoritmů založených na důkazech, algoritmů odolných vůči chybám a algoritmů založených na DAG, bylo vyhodnoceno pomocí osmi kritérií, jako jsou bezpečnost, decentralizace, škálovatelnost a energetická účinnost.
Tato práce zahrnuje metodologicky navrženou sadu testovacích scénářů pro tyto mechanismy a na základě analýzy jednotlivých mechanismů jsou dána doporučení, která zdůrazňují důležitost výběru mechanismů vhodných pro specifické požadavky systému. Výzkum významně přispívá do oblasti tím, že poskytuje podrobné pochopení mechanismů konsensu, komparativní analýzu zdůrazňující jejich silné a slabé stránky a cenné testovací scénáře pro budoucí studie.

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.

Cíl 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.

Metodika

Celkové komparativní analýze nejprve předcházela literární rešerše technologie distribuované účetní knihy, jako je blockchain, sidechain, DAG a další pro celkové pochopení kontextu. Následně se rešerše přesunula k problematice a detailnímu popisu 22 vybraných konsensních mechanismů (tab. 1), které jsou implementovány v úspěšnějších projektech a nejedná se tedy pouze o návrhy. Mechanismy jsou rozděleny do několika charakteristických skupin.

Dále následovala komparativní analýza, kde byly nejdříve detailně popsány rizika spojená s konsensními mechanismy a detailně nadefinována kritéria hodnocení bezpečnost, decentralizace, model sítě, škálovatelnost, transakční propustnost, finalita, energetická účinnost a model protivníka. Ve vybraných kritériích byly všechny mechanismy hodnoceny, a to jak slovně, tak bodově a váhově. Byly popsány výhody a nevýhody jednotlivých mechanismů spolu s přehledem zranitelnosti proti kybernetickým útokům.

Poté jsem se zaměřil na rešerši dostupných open-source simulátorů pro možné simulace konsensních mechanismů. Tento proces byl zdlouhavý, jelikož většina simulátorů neměla dostatečnou dokumentaci, nebo nebyly dokončeny či nesprávně implementovány. Je důležité zdůraznit, že není dostupný simulátor, který by podporoval všechny konsensní algoritmy, což byl jeden z hlavních problémů, se kterými jsem se během výzkumu setkal. Nakonec jsem identifikoval dva plně funkční simulátory, které jsem mohl použít pro své testy.

V závěrečné části jsem metodicky navrhl sadu testovacích scénářů pro konsensní mechanismy v různých situacích. Některé scénáře byly dostupnými simulátory otestovány a ostatní jsou připraveny pro další výzkum a testování. Tato část mi umožnila ověřit chování vybraných mechanismů v různých situacích.

Celkově jsem v rámci této metodiky provedl rozsáhlý výzkum a testování s cílem lépe porozumět problematice a konsensních mechanismů, což poskytne základní cenné informace pro další výzkum v této oblasti.

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 1 - Přehled vybraných konsensních mechanismů

Výsledky

Z vypracované komparativní analýzy konsensních mechanismů vyplývají data interpretována v tabulce 2, která porovnávají jednotlivé mechanismy za využití vah, které jsou mechanismům přiděleny v závislosti na tom, jak jsou pro ně relevantní, tzn., že rozdělení odpovídá specifickému účelu a zaměření každého mechanismu. Výsledkem jsou i tabulky se slovním popisem a výhodami/nevýhodami pro každý mechanismus.

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 2 – Bodové a vážené hodnocení mechanismů konsensu dle stanovených kritérií

Dále je v práci navrhnuto 20 testovacích scénářů, které jsou buď společné pro blockchainové konsensní mechanismy, nebo jsou navrženy pro konkrétní mechanismus a specifický účel.

Následující navržený testovací scénář byl simulován pomocí dostupného BlockSim blockchainového simulátoru a výsledná data byla interpretována pomocí tabulek a grafů.

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:

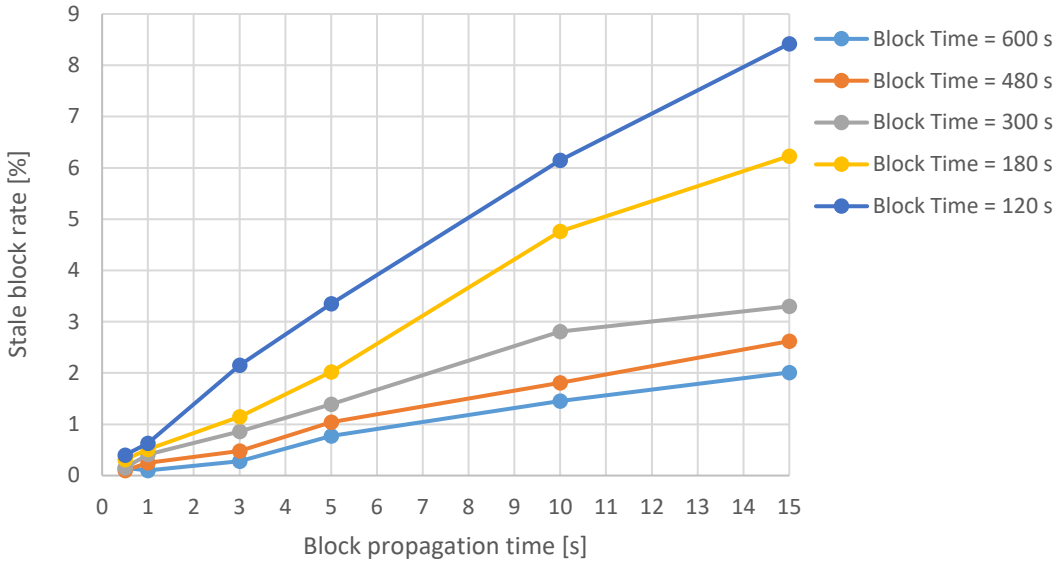
1. Nastavte průměrnou dobu těžby bloku na hodnotu 600 sekund a průměrnou dobou propagace bloku na 0,5 sekundy. Spusťte simulaci po dobu nezbytně dlouhou pro vytěžení 4000 bloků a zaznamenejte z výstupu data o produkci zastaralých bloků společně s transakční propustností.
2. Opakujte test s průměrnou 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.

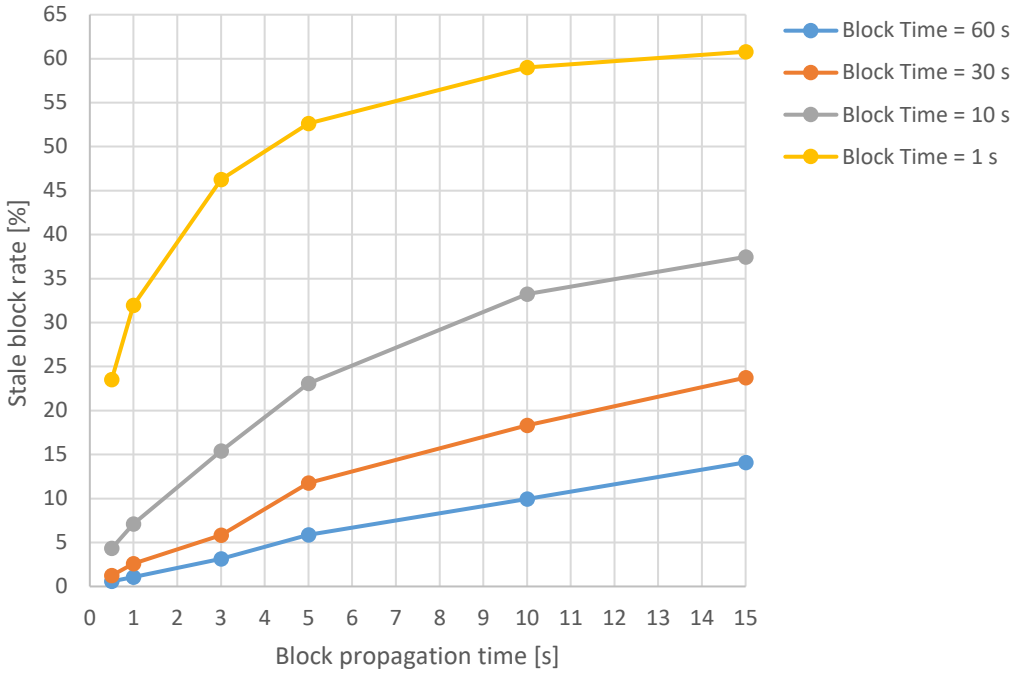
   Čas simulace nastavte pro průměrné doby těžby bloku tak, aby počet vytěžených bloků byl ve všech testech srovnatelný.

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:





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.

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.

Seznam literatury použité v tezích

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

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

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

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.

Další bibliografické údaje

Type of thesis: master

Author: Tadeáš PEKÁREK

Academic Year: 2022/2023

Department: Department of Applied Mathematics and Informatics, Faculty of Economics, University of South Bohemia in Ceske Budejovice, Czech Republic

Thesis supervisor: doc. Ing. Ladislav Beránek, Csc., MBA

Number of pages: 139

Language od thesis: CZ

Title of Thesis: Comparative evaluation of consensus mechanisms in cryptocurrencies

Annotation: 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.

Key words: cryptocurrencies, consensus mechanisms, analysis, comparative evaluation

---

Přílohy volně vložené:

Příloha 1 – Results_BlockSim.zip