Doktorantūros ataskaita

Doktorantas: Saulius Grigaitis

Prelimenarus disertacijos pavadinimas: Blokų grandinių spartinimas naudojant negrandinines transakcijas

Numatomas studijų laikas: 2018 - 2022

Vadovas: dr. Remigijus Paulavičius

Konsultantas: dr. Ernestas Filatovas

Tyrimo objektas:

Blokų grandinių protokolai orientuoti į spartesnį transakcijų vykdymą.

Tyrimo tikslas:

Tobulinti ir modifikuoti esamus blokų grandinių protokolus, siekiant didinti transakcijų pralaidumą.

Planuojami rezultatai

- Atlikti blokų grandinių protokolų analitinę apžvalgą
- Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su transakcijų pralaidumo didinimu blokų grandinių protokoluose
- Pasiūlyti patobulinimus egzistuojantiems blokų grandinių protokolams siekiant padidinti transakcijų pralaidumą
- Pasiūlytų patobulinimų pagrindu realizuoti prototipą
- Eksperimentiškai ištirti patobulintas protokolų versijas ir jų savybes palyginti su pradiniais protokolais

Plano vykdymo suvestinė

Studijų metai	Egzaminai		Dalyvavimas konferencijose		Publikacijos		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta	Būklė
I (2018/2019)	1	1					
II (2019/2020)	2	3			1	1	Publikuota
III (2020/2021)	**1**		**1**	**Priimta**	**1**	**1**	**Publikuota**
IV (2021/2022)			1				

Atlikti darbai 2020/2021

Egzaminai		Dalyvavimas konferencijose		Publikacijos	
Planas	**Įvykdyta**	**Planas**	**Įvykdyta**	**Planas**	**Įvykdyta**
Mašininis mokymasis	Išlaikytas (jau praėjusį semestrą): Mašininis mokymasis	Tyrimo rezultatų pristatymas tarptautinėje mokslinėje konferencijoje	Priimta į 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)	Žurnalas, turintis cituojamumo rodiklį *Clarivate Analytics Web of Science* duomenų bazėje.	„A Systematic Review and Empirical Analysis of Blockchain Simulators“ žurnale IEEE Access (Volume 9)

Viršplaniniai darbai:

- Parengtas ir dėstomas kursas „Blokų grandinių technologijos“
- Vadovavimas bakalauro ir magistro studentų darbams

Mokslinių tyrymų etapai

Darbo pavadinimas		Atlikimo terminai	Pastabos
1.	Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje): 1.1. Atlikti blokų grandinių tinklų analitinę apžvalgą. 1.2 Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su blokų grandinių spartinimu naudojant negrandinines (angl. *off-chain*) transakcijas.	2018 m. spalio mėn. – 2019 m. spalio mėn.	Atspausdinta apžvalginė publikacija šios dalies pagrindu.
2.	Mokslinio tyrimo vykdymas:		Fokusuojamasi į simuliatorių tyrimus, kurie leistų įvertinti protokolų patobulinimus našumo atžvilgiu. Nustatyta, kad tinkamų simuliatorių naujos kartos PoS protokolams nėra.
	2.1. Tyrimo metodikos sudarymas: 2.1.1. Tyrimo metodikos išsikeltam uždaviniui spręsti parinkimas; 2.1.2. Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką.	2019 m. lapkričio mėn. - 2020 m. sausio mėn.	
	2.2. Teorinis tyrimas: 2.2.1. Sričių, kuriose tikslinga spartinti blokų grandines negrandininėmis transakcijomis identifikavimas; 2.2.2. Blokų grandinių spartinimo naudojant negrandinines transakcijas tyrimas; 2.2.3. Blokų grandinių spartinimo naudojant negrandinines transakcijas modelio sukūrimas ar testavimas.	2020 m. vasario mėn. – 2020 m. spalio mėn.	

Mokslinių tyrymų etapai

	2.3. Empirinis tyrimas: 2.3.1. Blokų grandinių spartinimo naudojant negrandinines transakcijas pritaikymas 2.2.1 uždavinyje identifikuotoms praktinėms sritims. 2.3.2. El. komercijai pritaikyto blokų grandinių sprendimo, naudojančio negrandinines transakcijas, tyrimas ir tobulinimas.	2020 m. lapkričio mėn. – 2021 m. gegužės mėn.	Atspausdinta publikacija šios dalies pagrindu. Tolesni darbai fokusuosis į simuliavimo metodus, kurie leistų tirti naujos kartos PoS protokolų našumą
	2.4. Gautų rezultatų analizė, apibendrinimas, išvadų parengimas: 2.4.1. Gautų rezultatų analizė; 2.4.2. Rezultatų apibendrinimas, esminių rezultatų išskyrimas; 2.4.3. Išvadų parengimas.	2021 m. birželio mėn. – 2021 m. spalio mėn.	

Blokų grandinių eksperimentinių tyrymų problematika

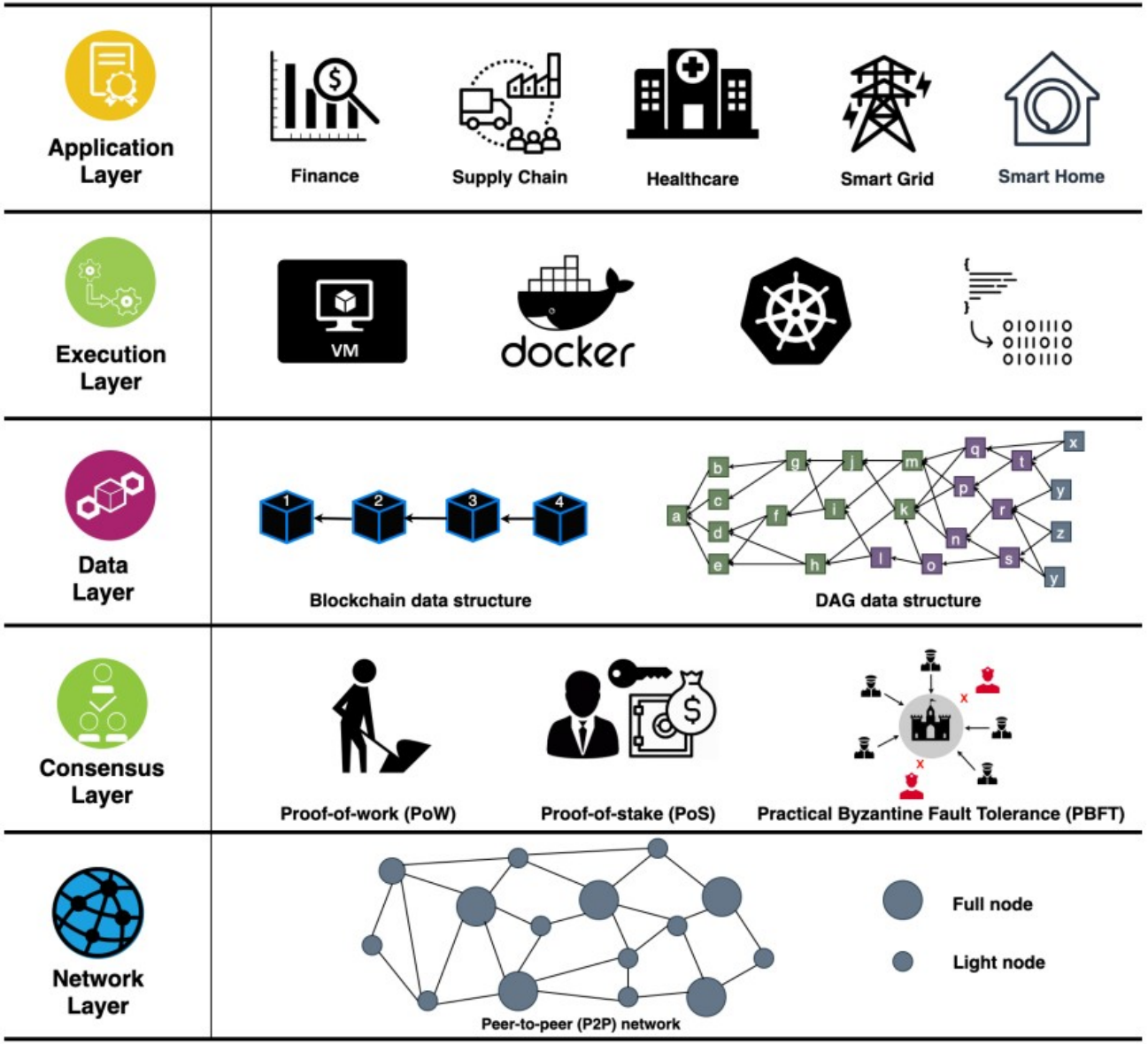
- Blokų grandinių tinklai yra globaliai išskirstytos labai daug resursų naudojančios sistemos, pvz. Bitcoin:

  ~75 Twh sunaudojamos elektros per metus

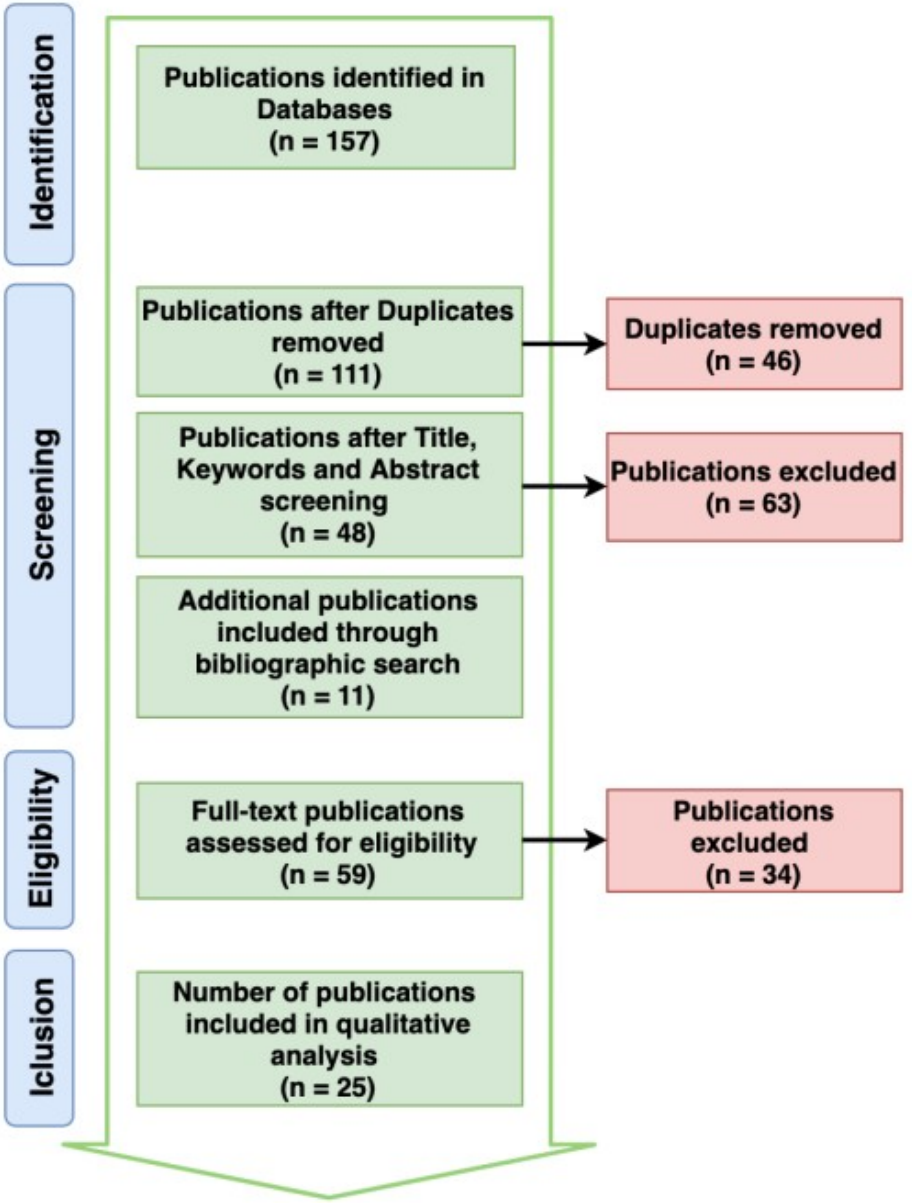
  ~ 50000 mazgų geografiškai paskirstytų visame pasaulyje

- Nėra galimybės keisti veikiančių populiarių tinklų protokolus siekiant išbandyti juos realioje aplinkoje
- Nėra galimybės sukurti ekperimentines aplinkas analogiškas realioms
- Simuliatoriai – realiausias kandidatas eksperimentams

Blokų grandinių technologijų sluoksniai



Simuliatorių publikacijų atranka



Simuliatoriai I

Simulator name	Source)	Title	Platform(s)	Layer(s)	Year	# Citations
"Bitcoin privacy simulator"[a]	Androulaki et al. [34]	Evaluating User Privacy in Bitcoin	Bitcoin	data, network	2013	563
Bitcoin protocol simulator	Eyal & Sirer [35]	Majority Is Not Enough: Bitcoin Mining Is Vulnerable	Bitcoin	data, network	2014	1599
Shadow-Bitcoin	Miller & Jansen [36]	Shadow-bitcoin: Scalable simulation via direct execution of multi-threaded applications	Bitcoin	network	2015	39
Bitcoin simulator	Gervais et al. [37]	On the Security and Performance of Proof of Work Blockchains	PoW blockchains	data, network	2016	775
Bitcoin mining simulator	Carlsten et al. [38]	On the instability of Bitcoin without the block reward	Bitcoin	network	2016	216
VIBES	Stoykov et al. [39]	VIBES: fast blockchain simulations for large-scale peer-to-peer networks	PoW blockchains	data, network	2017	28
VIBES "attack" (based on [39])	Schüssler et al. [40]	Attack and Vulnerability Simulation Framework for Bitcoin-like Blockchain Technologies	Bitcoin	network	2018	2
eVIBES	Deshpande et al. [41]	eVIBES: Configurable and Interactive Ethereum Blockchain Simulation Framework	Ethereum	data, network	2018	1
CLoTH	Conoscenti et al. [42]	The cloth simulator for HTLC payment networks with introductory lightning network performance results	Bitcoin	network	2018	9
BlockSim (Hao)	Hao et al. [43]	BlockP2P: Enabling Fast Blockchain Broadcast with Scalable Peer-to-Peer Network Topology	PoW blockchains	network	2019	3
BlockSim (Faria)	Faria & Correia [44]	BlockSim: Blockchain simulator	Bitcoin, Ethereum	data, network	2019	9
BlockSim (Alharby)	Alharby & Moorsel [45]	BlockSim: A Simulation Framework for Blockchain Systems	PoW blockchains	data, network	2019	18
SimBlock	Aoki et al. [46]	SimBlock: A Blockchain Network Simulator	Bitcoin	network	2019	32

Simuliatoriai II

LUNES-Blockchain	Rosa et al. [47]	Agent-based Simulation of Blockchains	Bitcoin	network	2019	4
BlockLite	Wang et al. [48]	Toward Accurate and Efficient Emulation of Public Blockchains in the Cloud	Bitcoin	consensus, data, network	2019	10
Bitcoin simulator "hash power" (based on [37])	Sai et al. [49]	Assessing the security implication of Bitcoin exchange rates	PoW blockchains	network	2019	2
"Algorand simulator"	Conti et al. [42]	Blockchain Trilemma Solver Algorand has Dilemma over Undecidable Messages	Bitcoin	network	2019	5
Bitcoin network simulator	Azimy & Ghorbani [50]	Competitive Selfish Mining	Bitcoin	network	2019	0
DAGsim	Zander et al. [51]	DAGsim: Simulation of DAG-Based Distributed Ledger Protocols	DAG	network	2019	7
"Mining strategy simulator"	Bruschi et al. [52]	Mine with it or sell it: The superhashing power dilemma	Bitcoin	network	2019	1
"Proof of Prestige Simulator"	Król et al. [53]	Proof-of-Prestige: A Useful Work Reward System for Unverifiable Tasks	Proof-of-Prestige	consensus	2019	5
Bitcoin simulator "consensus"(based on [37])	Foytik et al. [54]	A blockchain simulator for evaluating consensus algorithms in diverse networking environments	PoW blockchains	consensus	2020	1
Local Bitcoin Network Simulator	Alsahan et al. [55]	Local Bitcoin Network Simulator for Performance Evaluation using Lightweight Virtualization	Bitcoin	network	2020	3
SIMBA (based on [44])	Fattahi et al. [56]	An Efficient Simulator for Blockchain Applications	Bitcoin	data, network	2020	0

VOLUME 4, 2016 7

Atrinkti simuliatoriai (atvirojo kodo ir gana plačiai naudojami)

Simulator	Platform	Purpose	Model type	Language/ Frame-work	Source code
Bitcoin simu-lator	PoW blockchains	Security and performance analysis	Discrete-event	C++/NS3	https://github.com/arthurgervais/Bitcoin-Simulator
LUNES-Blockchain	PoW blockchains	Security analysis, DoS attack simula-tion	Agent-based	ARTÌS+GAIA	https://pads.cs.unibo.it/doku.php?id=pads:download
VIBES	PoW blockchains	Network performance analysis, se-curity analysis (double-spending and DoS attacks simulation)	Discrete-event	Scala	https://github.com/i13-msrg/vibes
eVIBES	Ethereum	Simulation of Ethereum network be-havior including smart-contracts	Discrete-event	Scala	https://github.com/i13-msrg/evibes
SimBlock	Bitcoin	Simulation of network behavior in Bitcoin-like blockchain	Discrete-event	Java	https://github.com/dsg-titech/simblock
BlockSim (Al-harby)	PoW blockchains	Security and performance analysis	Discrete-event	Python	https://github.com/maher243/BlockSim
BlockSim (Faria)	Bitcoin, Ethereum	Security and performance analysis	Discrete-event	Python/SimPy	https://github.com/carlosfaria94/blocksim

Naujos kartos PoS protokolų tyrimai

- Praktiškai nėra PoS simuliatorių ir artimiausiu metu nėra realu sulaukti kokybiškų versijų
- PoS protokolai daug sudėtingesni už senos kartos PoW
- Perspektyviausi PoS protokolai su numatomu dideliu transakcijų našumu (tokie kaip Ethereum 2.0) dar nėra pilnai sukurti ir ištestuoti realiose sąlygose

PoS Ethereum 2.0 protokolo simuliavimas

Testinių tinklų (Pyrmont, Prater ir kt.) sėkmė leidžia daryti prielaidą, kad PoS tinklų simuliavimą galima atlikti panaudojant testinį tinklą su salyginai mažais resursais (sutelkiant visus validatorius nedideliame skaičiuje mazgų). Šį metodą dar reikės tobulinti:

- Simuliuoti tinklo vėlavimus, nes didelis validatorių validatorių skaičius viename mazge neatspindi tinklo vėlavimų, kurie yra įprasti realiame tinkle esant geografiškai išskirstytiems validatoriams
- Simuliuoti validatorių trikius.

Klausimai