Doktorantūros metinė ataskaita

Laikotarpis
2019 spalio 1d. - 2020 spalio 1d.

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

Planas 2019/2020

- Kurso „Fundamentalieji informatikos ir informatikos inžinerijos metodai“ egzaminas
- Kurso „Blokų grandinių technologijos“ egzaminas
- Kurso “Mašininis mokymasis” egzaminas
- Tyrimo rezultatų pristatymas nacionalinėje mokslinėje konferencijoje
- Blokų grandinių technologijų transakcijų spartinimo teorinis tyrimas

Atlikti darbai 2019/2020

- Kurso „Fundamentalieji informatikos ir informatikos inžinerijos metodai“ egzaminas. Įvertinimas: 9
- Kurso „Blokų grandinių technologijos“ egzaminas. Įvertinimas: 10
- Kurso “Mašininis mokymasis” egzaminas. Įvertinimas: 9
- Pristatytas stendinis pranešimas “BlockLib – The First Library of Blockchains” nacionalinėje konferencijoje “Data Analysis Methods for Software Systems 2019”
- Ištirti simuliatoriai, leidžiantys analizuoti plačiai naudojamų blokų grandinių protokolų našumą
- Vadovauta Ethereum 2.0 kliento, leisiančio tirti naujos kartos PoS protokolo našumą, kūrimui

Viršplaniniai darbai:

- Išleista publikacija žurnale, turinčiame cituojamumo rodiklį Clarivate Analytics Web of Science duomenų bazėje:

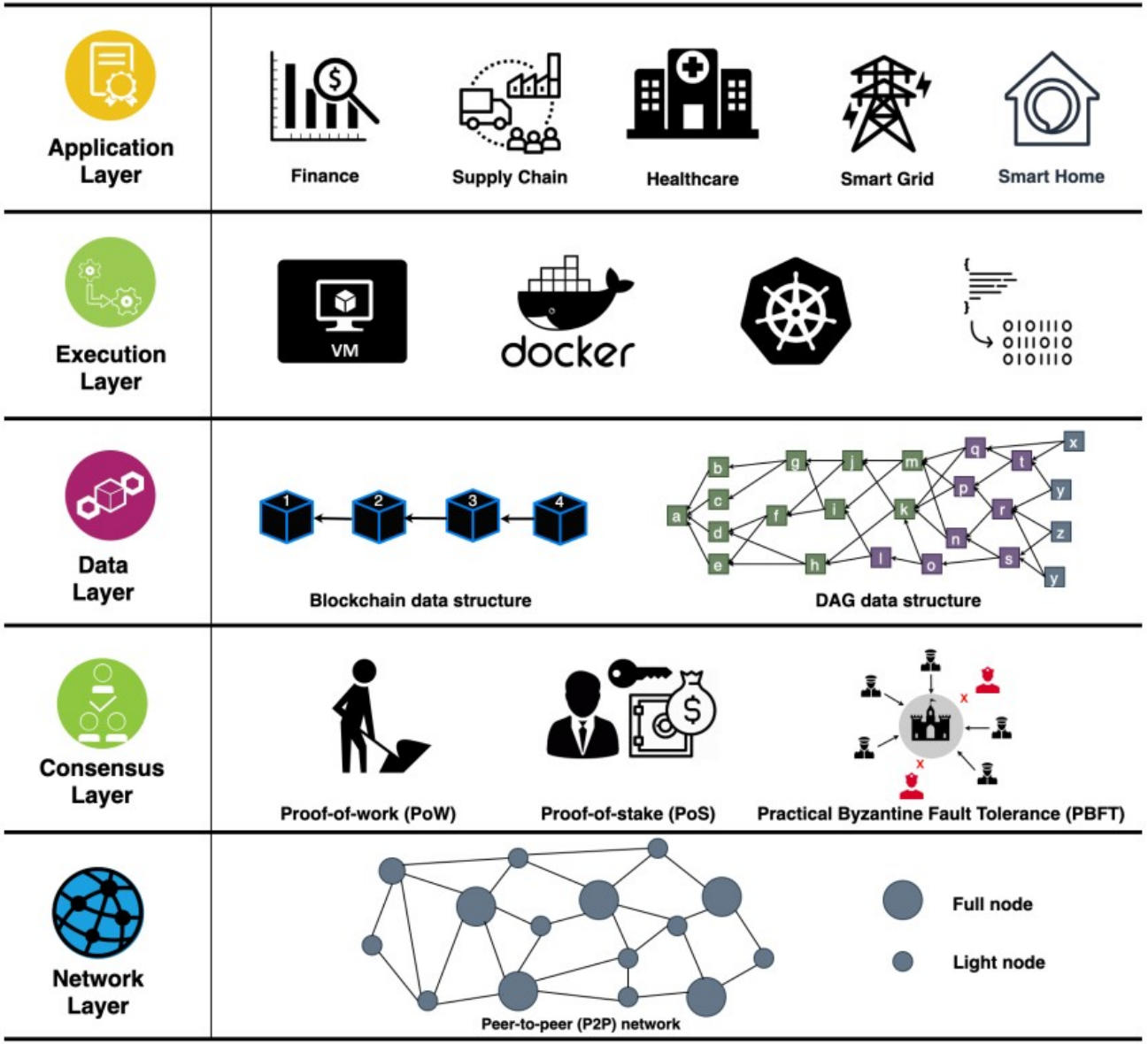
  “A Decade of Blockchain: Review of the Current Status, Challenges, and Future Directions”
- Rengiama publikacija teikti į žurnalą, turintį cituojamumo rodiklį Clarivate Analytics Web of Science duomenų bazėje:

  „A Systematic Review and Empirical Analysis of Blockchain Simulators”
- Parengtas ir dėstomas kursas „Blokų grandinių technologijos“
- Vadovavimas bakalauro ir magistro studentų darbams

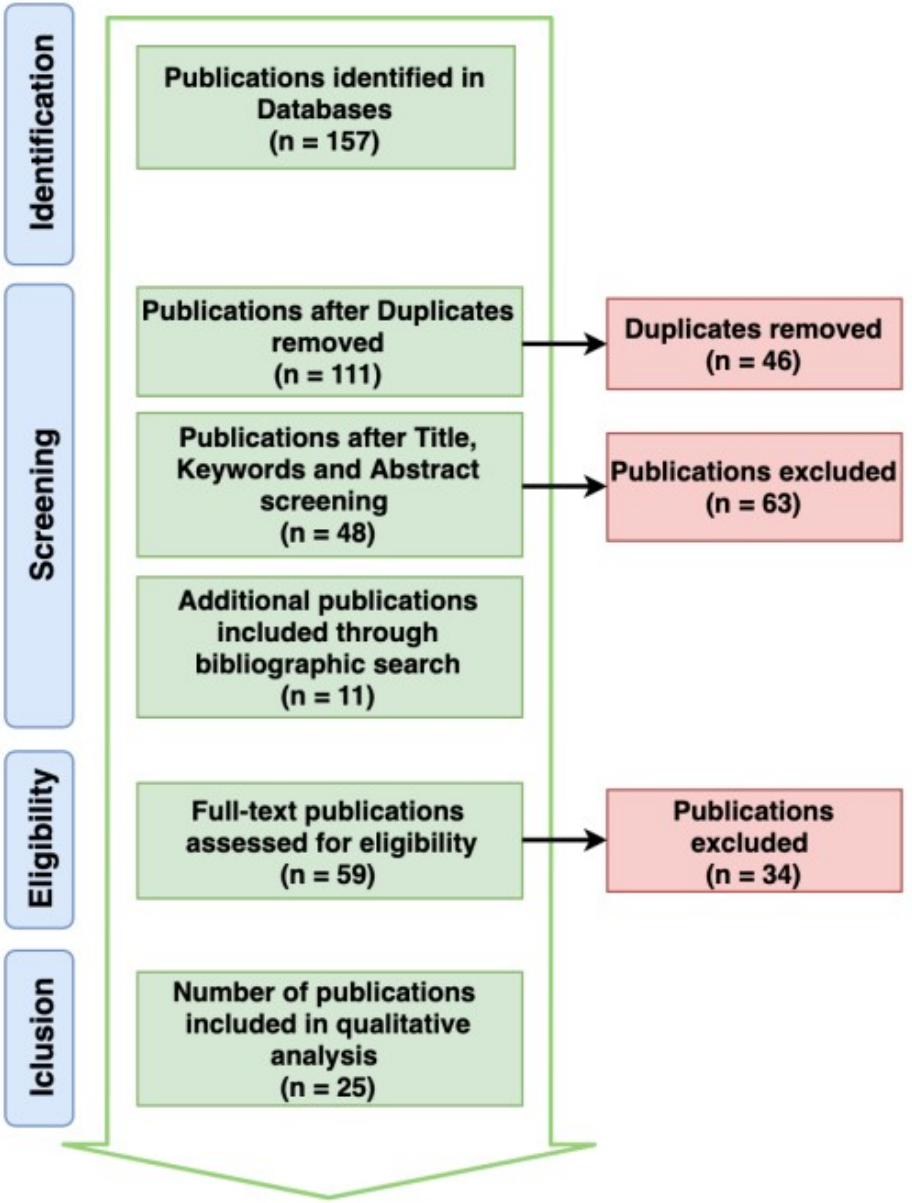
Planas 2020/2021

- Plėsti transakcijų našumo tyrimus apimant sudėtingesnius naujus protokolus, kuriems nėra simuliatorių, pvz. Ethereum 2.0
- Tęsti vadovavimą Ethereum 2.0 kliento kūrimui
- Pasiūlyti protokolų patobulinimus siekiant padidinti transakcijų pralaidumą.
- Išleisti „A Systematic Review and Empirical Analysis of Blockchain Simulators” publikaciją.
- Tyrimo rezultatų pristatymas tarptautinėje mokslinėje konferencijoje

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

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

Naujos kartos PoS Ethereum 2.0 protokolo tyrimai

- Vadovavimas Ethereum 2.0 kliento vystymui, siekiant pakreipti vystymą tokia kryptimi, kuri leistų ne tik implementuoti protokolą, bet ir pasiekti mokslinių rezultatų
- Viešų testinių tinklų (Medalla ir kt.) analizavimas, kol tai yra geriausias būdas, nes tai leidžia nenumatytų, tik realiame tinke iškylančių problemų ir jų įtakos transakcijų našumui analizę. Pvz. leidžia atsižvelgti į žmogiškus faktorius, tokius kaip besikeičiančias mazgų valdytojų nuomones dėl protokolo perspektyvumo ir dalyvavimo jame.

Klausimai