



Vilnius  
University

# Mokslinių straipsnių apie blokų grandinių spartinimą naudojant negrandines technologijas apžvalga

Rytis Bieliauskas  
2021 m. kovo 25 d.



**Disertacijos pavadinimas:** „Darbo įrodymu“ pagrįstų blokų grandinių plėtros problemų sprendimas naudojant negrandines technologijas.

**Darbo vadovas:** Dr. Remigijus Paulavičius

**Doktorantūros pradžios ir pabaigos metai:** 2019 – 2023

# Visų studijų planas

Studijų metai	Egzaminai		Dalyvavimas konferencijose		Publikacijos		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta	Būklė
I (2019/2020)	1	1	0	1	0	0	
<b>II (2020/2021)</b>	<b>2</b>	<b>1</b>	<b>1</b>	<b>0 (1)</b>	<b>0</b>	<b>0</b>	
III (2021/2022)	1	0	2	0	1	0	
IV (2022/2023)	0	0	0	0	1	0	

# Einamieji studijų metai

Egzaminai		Dalyvavimas konferencijose		Publikacijos	
Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta
Fundamentalieji informatikos ir informatikos inžinerijos metodai	Išlaikyta: Fundamentalieji informatikos ir informatikos inžinerijos metodai	Tyrimo rezultatų pristatymas nacionalinėje mokslinėje konferencijoje	11 tarptautinė konferencija „Duomenų analizės metodai programų sistemoms“. (DAMSS 2019) [atlikta 2019/2020 metais]		
Blokų grandinių technologijos	Dar nebuvo: Blokų grandinių technologijos				

# Visų mokslinių tyrimų ir disertacijos rengimo etapai

Darbo pavadinimas	Atlikimo terminai	Pastabos
<p>Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):</p> <p>1.1. Atlikti „darbo įrodymu“ (angl. <i>proof of work</i>) pagrįstų blokų grandinių tinklų analitinę apžvalgą.</p> <p>1.2. Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su „darbo įrodymu“ pagrįstų blokų grandinių plėtros (angl. <i>scalability</i>) sprendimais naudojant negrandines (angl. <i>off-chain</i>) technologijas.</p>	2019 m. spalio mėn. – 2020 m. spalio mėn.	
Mokslinio tyrimo vykdymas:		
<p><b>2.1. Tyrimo metodikos sudarymas:</b></p> <p>2.1.1. Tyrimo metodikos išsikeltam uždaviniui spręsti parinkimas;</p> <p>2.1.2. Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką.</p>	2020 m. lapkričio mėn. – 2021 m. sausio mėn.	
<p><b>2.2. Teorinis tyrimas:</b></p> <p>2.2.1. Sričių, kuriose tikslinga plėsti „darbo įrodymu“ pagrįstas blokų grandines naudojant negrandines technologijas identifikavimas;</p> <p>2.2.2. „Darbo įrodymu“ pagrįstų blokų grandinių plėtros naudojant negrandines technologijas tyrimas;</p> <p>2.2.3. „Darbo įrodymu“ pagrįstų blokų grandinių plėtros naudojant negrandines technologijas modelio sukūrimas ar testavimas.</p>	2021 m. vasario mėn. – 2021 m. spalio mėn.	

<p><b>2.3. Empirinis tyrimas:</b></p> <p>2.3.1. „Darbo įrodymu“ pagrįstų blokų grandinių plėtros naudojant negrandines technologijas pritaikymas 2.2.1 uždavinyje identifikuotoms praktinėms sritims.</p> <p>2.3.2. EI. komercijai pritaikyto „darbo įrodymu“ pagrįstų blokų grandinių plėtros sprendimo naudojant negrandines technologijas tyrimas ir tobulinimas.</p>	2021 m. lapkričio mėn. – 2022 m. gegužės mėn.	
<p><b>2.4. Gautų rezultatų analizė, apibendrinimas, išvadų parengimas:</b></p> <p>2.4.1. Gautų rezultatų analizė;</p> <p>2.4.2. Rezultatų apibendrinimas, esminių rezultatų išskyrimas;</p> <p>2.4.3. Išvadų parengimas.</p>	2022 m. birželio mėn. – 2022 m. spalio mėn.	
<p>Atskirų daktaro disertacijos dalių (tyrimo metodikos, rezultatų, ginamų teiginių, išvadų ir kt.) parengimas:</p> <p>3.1. Tikslų, uždavinių, tyrimo metodikos, ginamųjų teiginių patikslinimas;</p> <p>3.2. Analitinės disertacijos dalies parengimas;</p> <p>3.3. Teorinės disertacijos dalies parengimas;</p> <p>3.4. Eksperimentinės disertacijos dalies parengimas;</p> <p>3.5. Bendrųjų išvadų formulavimas.</p>	2022 m. lapkričio mėn. – 2023 m. gegužės mėn.	
Daktaro disertacijos parengimas ir svarstymas padalinyje	2023 m. birželio mėn.	
Daktaro disertacijos gynimas	2023 m. rugsėjo mėn.	

## Tyrimo objektas:

„Darbo įrodymu“ (angl. proof of work) pagrįstų blokų grandinių plėtros (angl. scalability) sprendimai.

## Tyrimo tikslas:

Mokslinių straipsnių, kuriuose nagrinėjami „darbo įrodymu“ pagrįstų blokų grandinių plėtros sprendimai apžvalga.

## Tyrimo uždaviniai:

Atlikti „darbo įrodymu“ pagrįstų blokų grandinių tinklų analitinę apžvalgą;

Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su „darbo įrodymu“ pagrįstų blokų grandinių plėtros sprendimais naudojant negrandines (angl. off-chain) technologijas.

# Accuracy and completeness of scalability method information in articles:

	Increasing the block size	Reducing the transaction size	Sharding	State channels	Payment channels	Sidechains	DAGs
E. Ademi, "A Comprehensive Study on the Scalability Challenges of the Blockchain Technology"	Good	Low / None	Low / None	Low / None	Low / None	Low / None	Low / None
K. Croman <i>et al.</i> , "On scaling decentralized blockchains (A position paper)"	Low / None	Low / None	Good	Low / None	Low / None	Low / None	Low / None
S. Bano <i>et al.</i> , "The Road to Scalable Blockchain Designs Functional Components of a Blockchain"	Low / None	Low / None	Medium	Low / None	Low / None	Medium	Low / None
A. Singh <i>et al.</i> , "Public blockchains scalability: An examination of sharding and segregated witness"	Good	Excellent	Excellent	Low / None	Low / None	Medium	Low / None
P. McCorry <i>et al.</i> , "You Sank My Battleship! A Case Study to Evaluate State Channels as a Scaling Solution for Cryptocurrencies"	Low / None	Low / None	Low / None	Excellent	Excellent	Low / None	Low / None
J. Herrera-Joancomartí <i>et al.</i> , "Privacy in bitcoin transactions: New challenges from blockchain scalability solutions"	Excellent	Low / None	Low / None	Good	Excellent	Low / None	Low / None

# Accuracy and completeness of scalability method information in articles:

	Increasing the block size	Reducing the transaction size	Sharding	State channels	Payment channels	Sidechains	DAGs
G. Malavolta <i>et al.</i> , "Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability"	Low / None	Low / None	Low / None	Excellent	Excellent	Medium	Medium
S. Kim, Y. Kwon, and S. Cho, "A Survey of Scalability Solutions on Blockchain"	Medium	Medium	Medium	Good	Good	Good	Good
G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains"	Low / None	Low / None	Excellent	Low / None	Low / None	Low / None	Low / None
G. Wang, Z. J. Shi, M. Nixon, and S. Han, "SoK: Sharding on blockchain"	Good	Medium	Excellent	Low / None	Low / None	Low / None	Low / None
Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey"	Medium	Medium	Medium	Excellent	Excellent	Excellent	Excellent
H. Abdelatif <i>et al.</i> , "Scaling Blockchains: A Comprehensive Survey"	Good	Good	Good	Excellent	Excellent	Excellent	Excellent



# Attributes and consequences of different scalability methods:

Scaling method	Scaling solution type	Decentralization	Transactions per second supported	Privacy	Security	Used in
<i>Increasing block size</i>	On-chain	Decreases	Amount of transactions supported increases linearly	Does not change	Decreases because of increased centralization	Bitcoin, Bitcoin Cash, Bitcoin SV
<i>Reducing transaction size</i>	On-chain	Does not change	Increases by % of the amount tx size is reduced	Does not change	Does not change	Bitcoin
<i>Sharding</i>	On-chain	Decreases	Amount of transactions supported increases linearly	Does not change	Decreases because of increased complexity and additional attack vectors	Ethereum (planned)
<i>State channels</i>	Off-chain	Does not change	Virtually no limit to increase	Improved	Does not change	Raiden Network, Perun, Nitro Protocol, PISA, L4, Celer Network
<i>Payment channels</i>	Off-chain	Does not change	Virtually no limit to increase	Improved	Does not change	Lightning Network
<i>Sidechains</i>	On-chain	Does not change	Increases linearly	Can be improved, depending on the sidechain	Does not change	Rootstock, Liquid
<i>DAGs</i>	On-chain	Decreases	Increases exponentially	Does not change	Decreases because of increased centralization	IOTA, Nano

## Išvados:

**Straipsnių apie įvairius blockchain scalability metodus kiekis kiekvienais metais didėja.**

**Pagal bendrą kiekį daugiausiai straipsnių yra apie Sharding bei DAG; pagal augimo tendencijas – apie Lightning Network.**

**Naujausi straipsniai yra pilniausi ir kokybiškiausi.**

**Iš visų tirtų scaling metodų, Lightning Network turi daugiausiai potencialo bei mažiausiai trūkumų lyginant su kitais scaling metodais.**

## 2020/2021 m. m. planuojami darbai:

### Išklausyti modulį ir išlaikyti egzaminą:

- Blokų grandinių technologijos, 7 kreditai.

### Mokslinio straipsnio rengimas:

- “Analysis of Scalability Solutions for Proof-of-work Based Blockchains”.



Vilnius  
University

Ačiū už dėmesį  
Klausimai?