Doktorantūros ataskaita

Doktorantas: Saulius Grigaitis

Prelimenarus disertacijos pavadinimas: Blokų grandinių spartinimas naudojant negrandinines transakcijas

Numatomas studijų laikas: 2018 – 2023 (akademinės atostogos 2021-2022)

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 [4]
I (2018/2019)	1	1					
II (2019/2020)	2	3			1	1	Publikuota
III (2020/2021)	**1**		**1**	**1**	**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 ankstesnį semestrą): Mašininis mokymasis	Tyrimo rezultatų pristatymas tarptautinėje mokslinėje konferencijoje	An overview and current status of blockchain simulators, 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2021 gegužės 3 – 6 d., Sidnėjus, Australija	Žurnalas, turintis cituojamumo rodiklį *Clarivate Analytics Web of Science* duomenų bazėje	R. Paulavičius, S.Grigaitis, E.Filatovas, „A Systematic Review and Empirical Analysis of Blockchain Simulators“, IEEE Access Volume 9, 38010 – 38028, 2021, 10.1109/ICBC51069.2021.9461114. Publikuota, *impact factor* 3.367 (2020)

Viršplaniniai darbai:

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

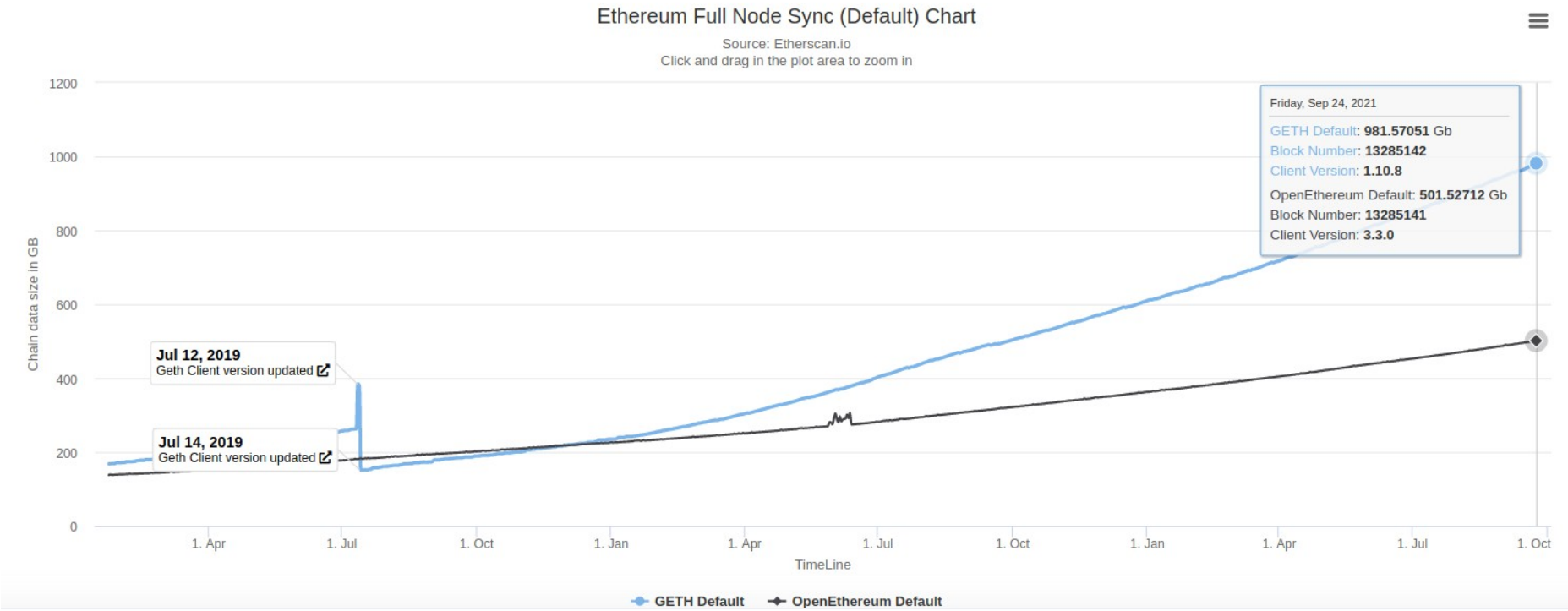
Mokslinių tyrymų etapai

	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 tyrimai fokusuojasi į optimizavimą kriptografijos algoritmų (KZG10 ir kt.), kurie įgalina didinti transakcijų našumą duomenų *shardingo* pagalba
	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.	
3.	Atskirų daktaro disertacijos dalių (tyrimo metodikos, rezultatų, ginamų teiginių, išvadų ir kt.) parengimas: 3.1. Tikslų, uždavinių, tyrimo metodikos, ginamųjų teiginių patikslinimas;	2021 m. lapkričio mėn. – 2022 m. gegužės mėn.	Planas nusikelia metams dėl akademinių atostogų 2021-

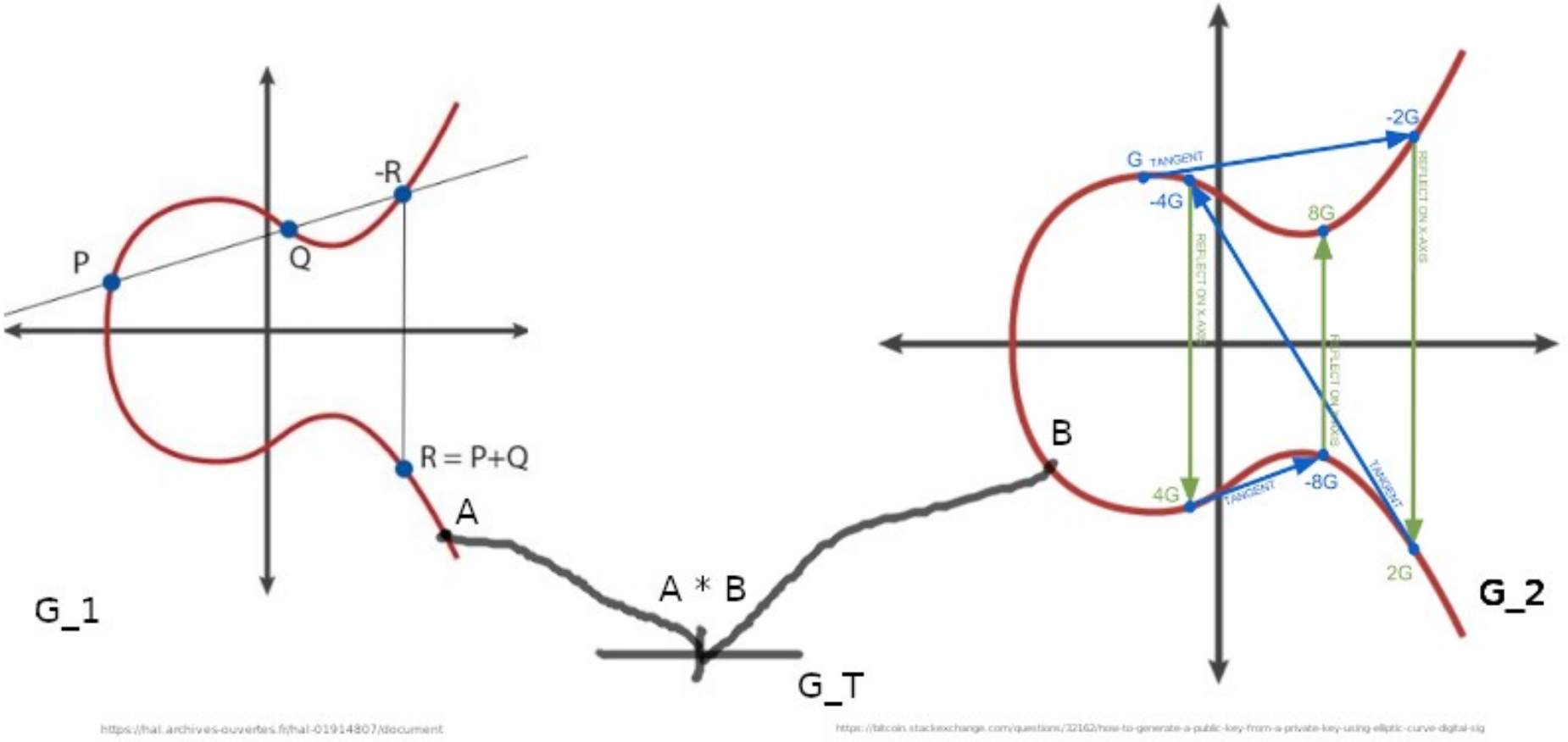
Problema: blokų grandinės būsenos augimas



Didinant bloko dydį didėja tranzakcijų skaičių bloke, tačiau tai greitina būsenos augimo greitį, dėl to mažėja decentralizacija, nes tinkle nustoja korektiškai veikti mažiau resursų turintys mazgai.

Duomenų *šardingas* – paskleisti duomenis tinkle taip, ka visiems mazgams nereiktų apdoroti ir saugoti visos informacijos, tačiau tie duomenys būtų prieinami kai jų prireikia, tam panaudojami įsipareigojimai polinomams ir klaidas taisantys kodai.

Elipsinės kreivės



https://hal.archives-ouvertes.fr/hal-01914807/document

https://bitcoin.stackexchange.com/questions/32162/how-to-generate-a-public-key-from-a-private-key-using-elliptic-curve-digital-sig

KZG10 įsipareigojimai polinomams

Elipsinės kreivės G_1 ir G_2, palaikančios poravima:

$$e : G_1 \times G_2 \to G_T$$

p - G_1 ir G_2 eilė, naudojame notacija:

$$[x]_1 = xG \in G_1$$
$$[x]_2 = xH \in G_2$$
$$x \in F_p$$

$[s^i]_1$ ir $[s^i]_2$ - nežinomo s laipsniai virš G_1 ir G_2.

Isipareigojimas polinomui (tik 48 baitai):

$$C = [p(s)]_1 = [\sum_{i=0}^{n} p_i s^i]_1 = \sum_{i=0}^{n} p_i [s^i]_1$$

Jeigu tikrintojui norime irodyti, kad $p(z) = y$, tai randame:

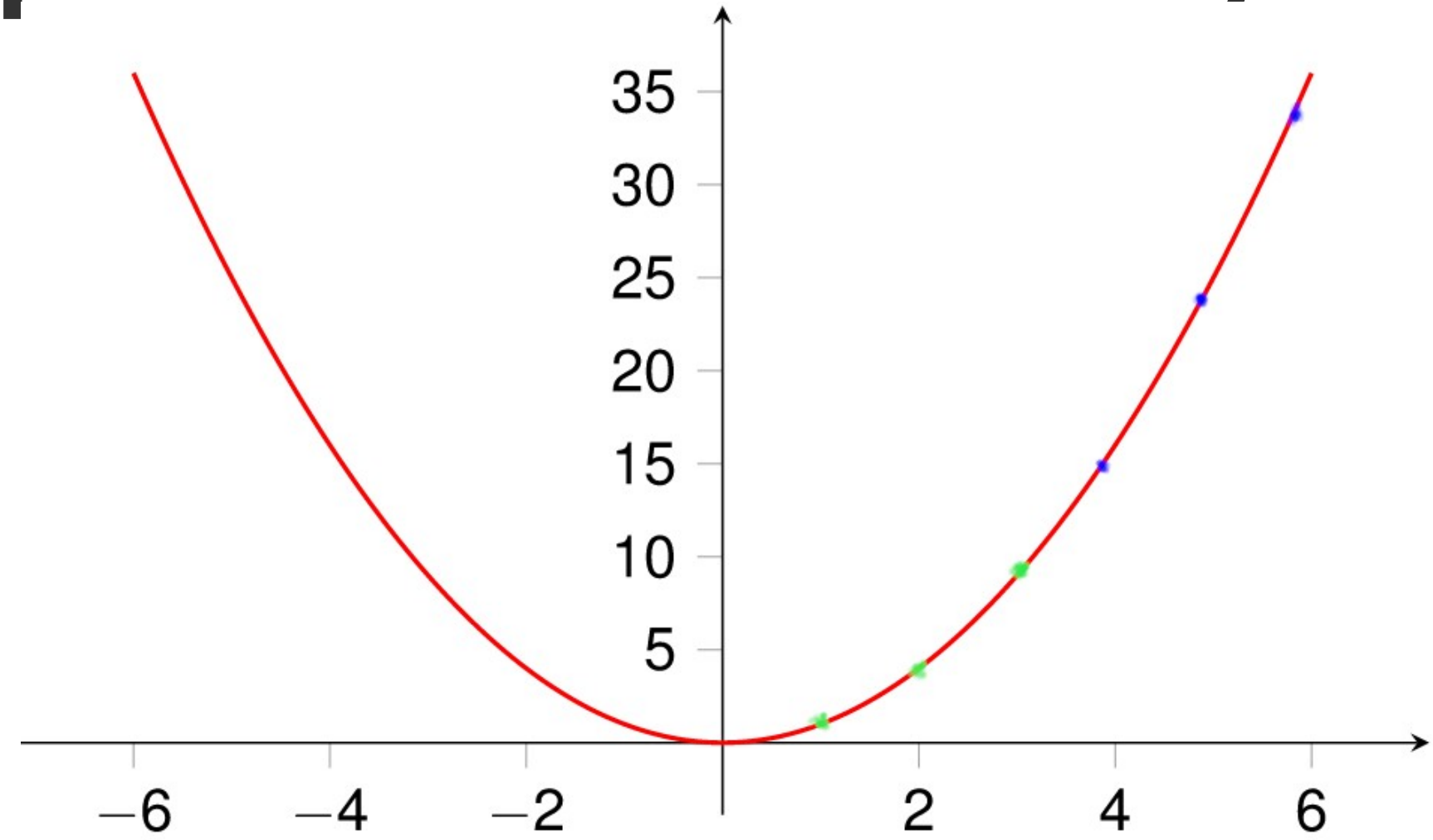
$$q(X) = \frac{p(X) - y}{X - z}$$
$$\pi = [q(s)]_1$$

$q(X)$ egzistuoja, jeigu $p(X) - y = 0$ pozicijoje z, o taip ir yra kadangi $p(z) = y$.

Tikrintojui tereikia paskaičiuoti:

$$e(\pi, [s - z]_2) = e(C - [y]_1, H)$$

Klaidas taisantys kodai: pertekliniai duomenys



Optimizacijos

- Algoritmai teoriniame lygyje jau stipriai optimizuoti (pvz. FK20 schema skaičiuojanti visus įrodymus kartu);
- Tačiau dar yra nemažai erdės optimizuojant realizacijas:

    1) Skirtingų BLS12-381 elipsinių kreivių bibliotekų naudojimas, kadangi jos naudoja skirtingas optimizacijas;

    2) Algoritmų paralelizavimas galėtų atnešti reikšmingą paspartėjimą, nes kai kurios algoritmo dalys yra vienos nuo kitos nepriklausomos;

    3) Greitesnės kalbos naudojimas.

Einamieji rezultatai

Testas	Go Herumi BLS	Go Killic	Rust Herumi BLS (mūsų implementacija)
FFT išplėtimas (4)	0.0056 ms	0.0052 ms	0.0014 ms
FFT išplėtimas (8)	0.156 ms	0.042 ms	0.028 ms
FFT išplėtimas (12)	3.650 ms	0.822 ms	0.705 ms
FFT išplėtimas (15)	36.104 ms	8.505 ms	6.857 ms
FFT FF (4)	0.00996 ms	0.00034 ms	0.00009ms
FFT FF (8)	0.236 ms	0.0069 ms	0.002 ms
FFT FF (12)	4.977 ms	1.423 ms	0.46 ms
FFT FF (15)	45.647 ms	11.073 ms	5.060 ms
FFT G1 (4)	0.00215 s	0.00343 s	0.00085 s
FFT G1 (8)	0.06636 s	0.101 s	0.028 s
FFT G1 (12)	1.578s	2.534 s	0.704 s
FFT G1 (15)	15.709 s	20.944 s	7.513 s

Klausimai