# Doktorantūros metinė ataskaita

**Laikotarpis**
**2018 spalio 1d. - 2019 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 2018/2019

- Kurso „Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika“  išklausymas ir egzamino išlaikymas.
- Apžvelgti esamus blokų grandinių protokolus, atsižvelgiant į jų greitaveiką.

# Atlikti darbai 2018/2019

- Išklausytas kursas „Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika“ ir išlaikytas egzaminas. Įvertinimas: 8.

**Viršplaniniai darbai:**

- Parengta publikacija teikti į žurnalą, turintį cituojamumo rodiklį Clarivate Analytics Web of Science duomenų bazėje:

  A Decade of Blockchain: Review of the Current Status, Challenges, and Future Directions

- Parengtas ir dėstomas kursas „Blokų grandinių technologijos“.
- Išklausyti bendrųjų gebėjimų mokymai „LaTeX įvadas“ ir „R įvadas“.

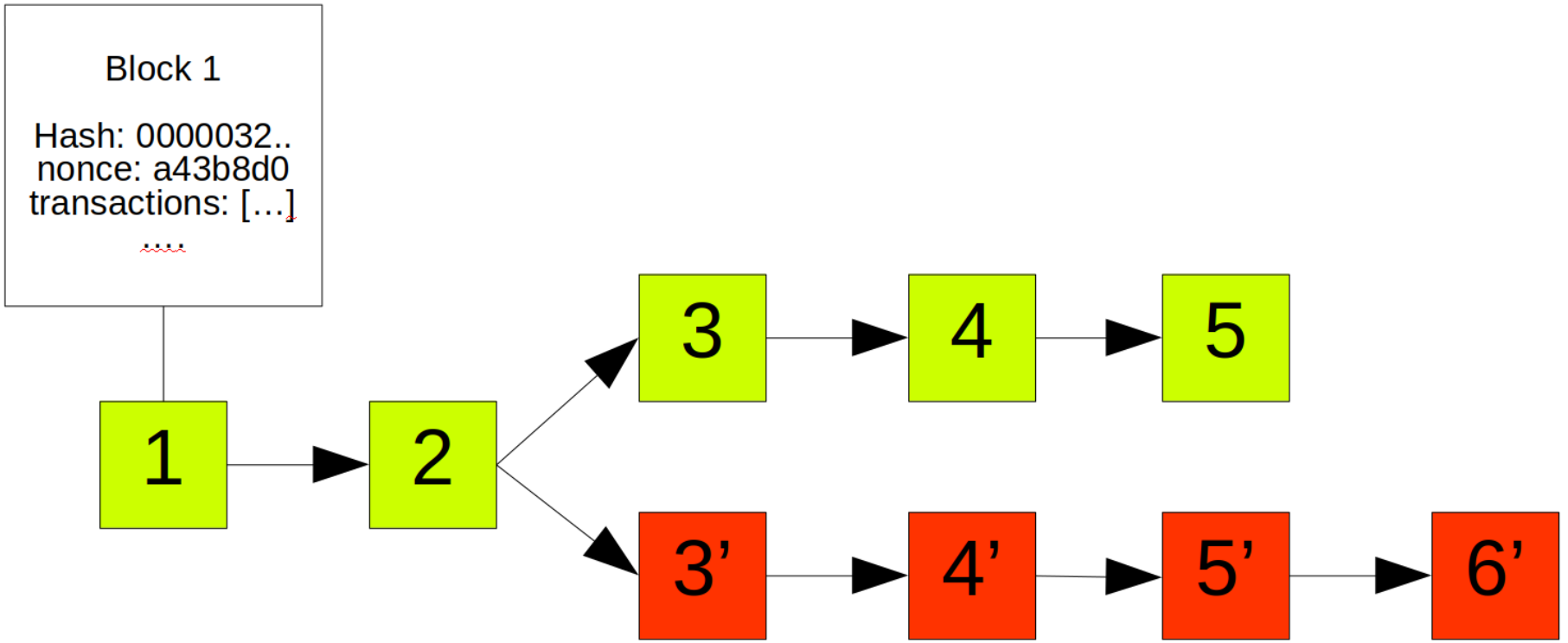
# Planas 2019/2020

- Ištirti šiuo metu dar tik kuriamus patobulinimus naujausiuose blokų grandinių protokoluose, tokiuose kaip Ethereum 2.0 versija, kurioje transakcijų pralaidumą bandoma didinti panaudojant susietas lygiagrečias blokų grandines.
- Eksperimentiškai patikrinti šių protokolų transakcijų pralaidumą ir palyginti su kitais jau apžvelgtais protokolais.
- Pasiūlyti protokolo patobulinimus siekiant dar padidinti transakcijų pralaidumą.
- Kursai „Fundamentalieji informatikos ir informatikos inžinerijos metodai“ ir “Mašininis mokymasis”
- Tyrimo rezultatų pristatymas nacionalinėje mokslinėje konferencijoje

# Protokolai

- Įrodymas darbų (ang. “Proof of Work”)
- Įrodymas turtu (ang. “Proof of Stake”)
- Deleguotas įrodymas turtu (angl. “Delegated Proof of Stake”)
- Įrodymas autoritetu (angl. “Proof of Authority”)
- Įrodymas ...

# Įrodymas darbu




Atakuotojo šaka

# Įrodymas darbu

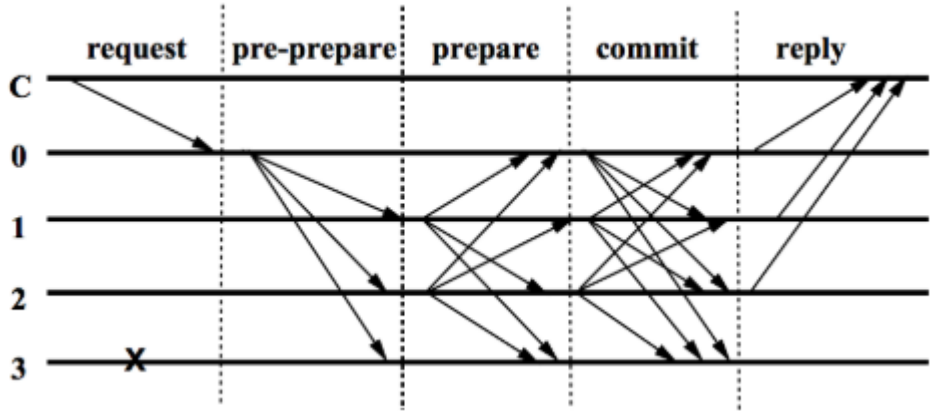
- Lėtas (Bitcoin ~7 transakcijos/s, Ethereum ~15 )
- Saugumas proporcingas energijos kiekiui iššvaistytam skaičiavimo resursams;
- Tikimybinis blokų finalizavimas;
- Sąlyginai pigios atakos;
- Atakuotojas rizikuoja tik sąlyginai mažais kaštais;
- Maža ekonominė paskata mazgams elgtis sąžiningai;
- Skatina centralizaciją (sunku atrasti bloką turint mažai resursų);

# Įrodymas turtu

- Užstatas suteikia balso teisę - nešvaistoma energija;
- Didesnės finalizavimo garantijos (pvz. ekonominis finalizavimas arba absoliutus finalizavimas BFT tipo protokoluose);
- Brangi atakos kaina (pvz. 1/3 viso užstatyto kriptovaliutos kieko);
- Atakuotojas yra dalininkas ir rizikuoja savo užstatu;
- Didelė ekonominė paskata elgtis sąžiningai;
- Kol kas nematoma priežasčių centralizacijos skatinimui.

# BFT tipo įrodymas turtu

- PBFT (Castro ir Liskov 1999) įkvėpti algoritmai;
- Garantuotas finalizavimas sulaukus bent 2/3 balsų (pagal svorį) esant ne daugiau 1/3 mazgų su bet kokio tipo klaidomis;
- Protokolas sustoja jeigu nesulaukiama 2/3 balsų;
- Dažnai sutinkamas privačiuose tinkluose.

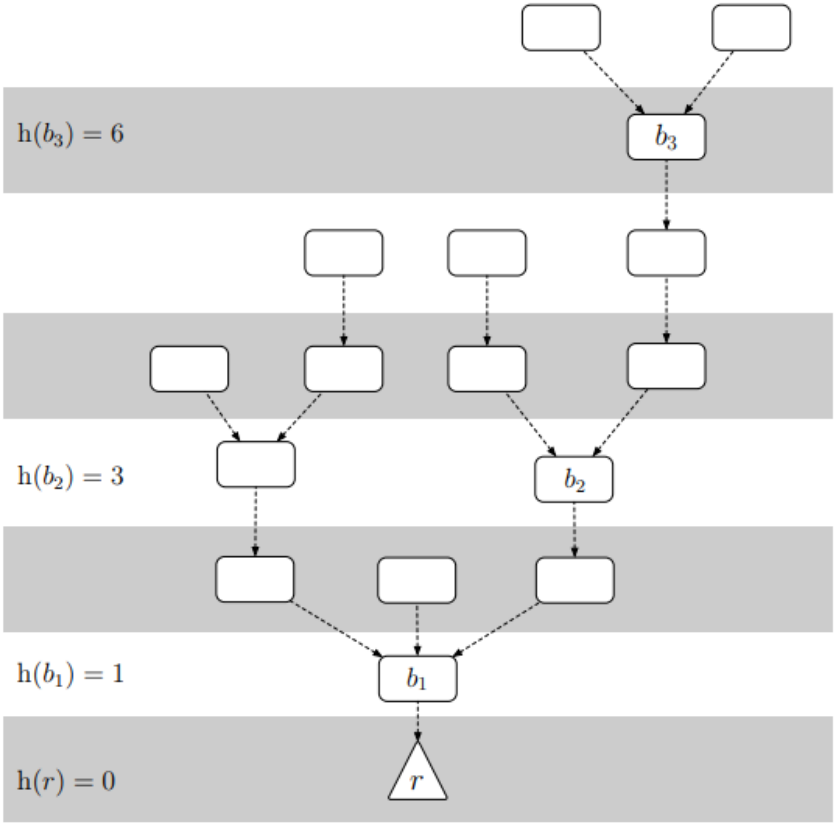


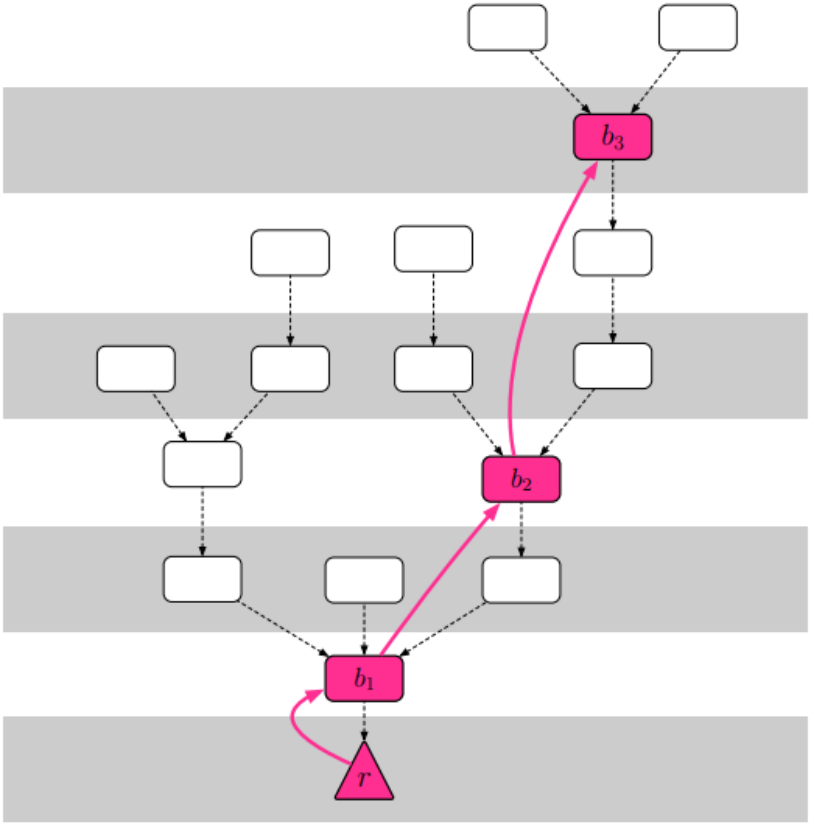

http://pmg.csail.mit.edu/papers/osdi99.pdf

# Grandinės tipo įrodymas turtu

- Įrodymo darbu įkvėpti protokolai;
- Didesnės finalizavimo garantijos (bet ne absoliutus finalizavimas), pvz. ekonominis finalizavimas;
- Protokolai orientuoti į pasiekiamumą paaukojant vientisumą;
- Dažniau sutinkamas viešuose tinkluose.

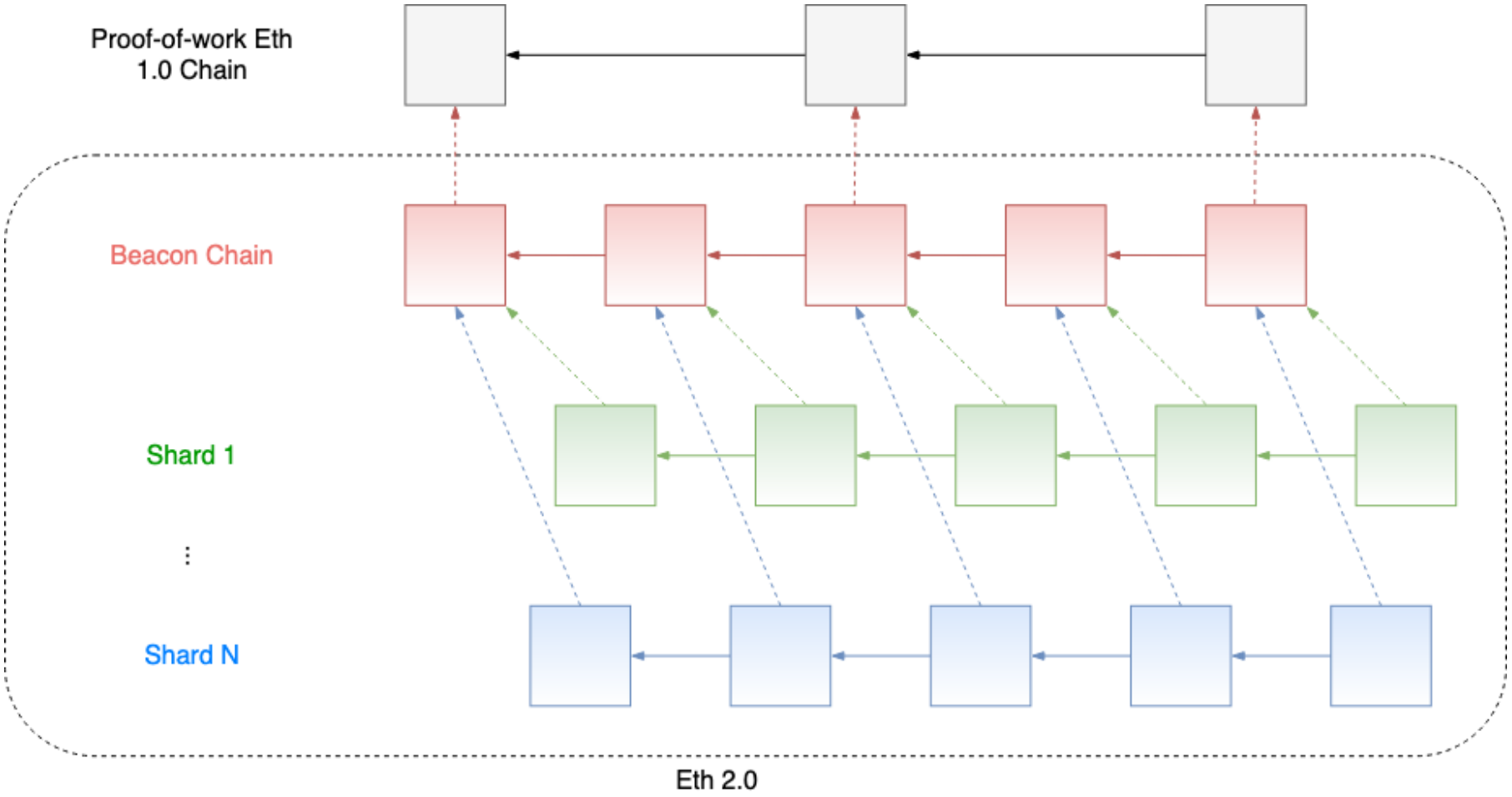
# Ethereum 2.0 Casper FFG grandinės tipo įrodymo turtu protokolo optimizacija - epochų finalizavimas




https://arxiv.org/pdf/1710.09437.pdf

# Lygiagrečios grandinės




https://runtimeverification.com/blog/a-formal-model-in-k-of-the-beacon-chain-ethereum-2-0s-primary-proof-of-stake-blockchain/

# Mokslinės problemos

- Bizantijos generolų problema;
- Pseudoatsitiktinių skaičių generavimas (RANDAO, VDF);
- Maišos funkcijos (Keccak, SHA-2, SHA-3);
- Nulinio atskleidimo kriptografija (zk-SNARK, zk-STARK);
- Greiti agreguoti parašai (Bohen-Lynn-Shacham);
- P2P komunikavimas (Gossip, Kademlia);
- Formalus verifikavimas (K karkasas).

# Klausimai