



**Vilniaus
universitetas**

Blokų grandinės technologija grindžiamo taikomojo modelio decentralizuotam elektros energijos skirstymui sukūrimas

Metinė darbo ataskaita už 2019-2020 metus

Doktorantas:

Paulius Danielius

Vadovas:

doc. dr. Saulius Masteika

Doktorantūros laikotarpis:

2018 – 2022 m.

Tyrimo objektas ir tikslas

Vilniaus
universitetas

Tyrimo objektas:

Decentralizuotas elektros energijos mainų validavimas blokų grandinėje.

Tyrimo tikslas:

Pasiūlyti technologiškai ir programiškai efektyvų modelį, įgalinantį smulkiuosius elektros gamintojus-vartotojus vykdyti elektros mainus decentralizuotoje aplinkoje.

- Decentralizuotų energijos sistemų (DES), naudojančių blokų grandinių technologiją, atvejų analizė;
- Kriptografinių valiutų ar žetonų naudojimo DES įvertinimas;
- Techninės įrangos specifikavimas;
- P2P prekybinių arba dalinimosi platformų funkcijų specifikavimas;
- Bendro modelio sudėties sukūrimas;
- Pasiūlyto modelio technologinio ir programinio efektyvumo įvertinimas.

Planuojami rezultatai

Vilniaus
universitetas

Sukurtas unikalus modelis P2P elektros energijos mainams tarp smulkiųjų elektros gamintojų-vartotojų blokų grandinių technologija paremtoje aplinkoje.

2019/2020 m. m. darbo planas

Vilniaus
universitetas

- **Išlaikyti egzaminus:**
 - ✓ Fundamentalieji informatikos ir informatikos inžinerijos metodai, 8 kreditai;
 - ✓ Blokų grandinių technologijos, 7 kreditai.
- **Moksliniai tyrimai:**
 - ✓ detaliau išanalizuoti P2P energijos mainų mechanizmus ir išmaniųjų kontraktų panaudojimą decentralizuotose energijos sistemose, naudojančiose blokų grandinių technologiją;
 - ✓ sudaryti mokslinio tyrimo metodiką;
 - ✓ atlikti teorinį tyrimą.
- **Sudalyvauti tarptautinėje mokslinėje konferencijoje**
- **Sudalyvauti mokslinėje stažuotėje užsienio aukštojoje mokykloje**
- **Sudalyvauti mokslinėje stažuotėje užsienio verslo sektoriuje**
- **Parengti mokslinę publikaciją *ISI web of Science* žurnale**

2019/2020 m. m. atlikti darbai

Išlaikytas egzaminas:

- ✓ Fundamentalieji informatikos ir informatikos inžinerijos metodai, 8 kreditai.
2020.01.29 d., įvertinimas 8 (gerai);
- ✓ *Blokų grandinių technologijos dalyko egzaminas numatytas išlaikyti 2020 m. gruodžio mėn. pirmųjų dviejų savaitių laikotarpyje.*

Atlikti moksliniai tyrimai:

- ✓ Tyrimo metodų parinkimas;
- ✓ Atlikti pirmieji teorijos ir praktinio taikymo tyrimai.

Parengtos disertacijos dalys:

- ✓ Nuosekliai rengiamos ir pildomos dalys: tyrimo metodika, teorinis tyrimas, empirinis tyrimas.

Dalyvauta konferencijose:

- ✓ Pristatytas stendinis pranešimas tarptautinėje konferencijoje „Data Analysis Methods for Software Systems” (DAMSS), 2019 m. lapkričio 28-30 d. Druskininkuose;
- ✓ Skaitytas pranešimas „*Vulnerabilities and Excess Gas Consumption Analysis within Ethereum-based Smart Contracts for Electricity Market*“ tarptautinėje konferencijoje „Business Informations Systems“ (3rd Blockchain and Smart Contract Technologies Workshop), 2020 m. liepos 8-10 d. University of Colorado, Colorado Springs, JAV (*konferencija vyko online*).

Parengtos/publikuotos/įteiktos publikacijos:

- ✓ P. Danielius, P. Stolarski and S. Masteika. *Vulnerabilities and Excess Gas Consumption Analysis within Ethereum-based Smart Contracts for Electricity Market*. **Priimta publikavimui**: ISI proceedings, Lecture Notes in Business Information Processing, Springer 2020.

2019/2020 m. m. papildoma veikla

Vilniaus
universitetas

Pedagoginė veikla:

- ✓ VU Kauno fakultete 2020 m. pavasario semestre Finansų technologijų studijų programos antrosios pakopos studentams dėstytas dalykas „*FinTech taikomieji sprendimai*“.

Dalyvavimas VU KF SMTII projektinėje veikloje:

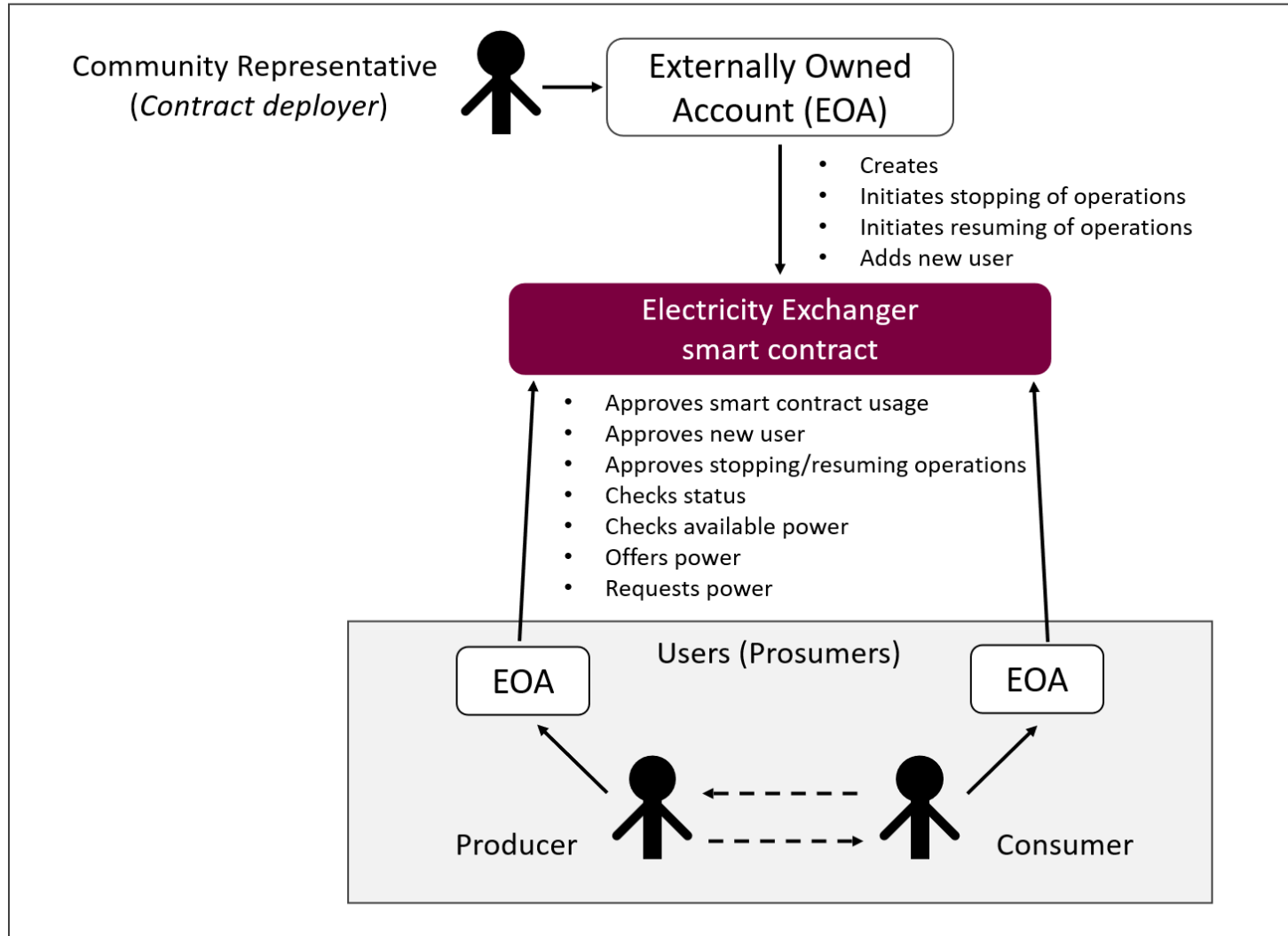
- ✓ Techninis darbuotojas projekte „Fuse IT“ (Marketingo ir IKT ateities kompetencijų gairės).

II kartos blokų grandinių platformų charakteristikos

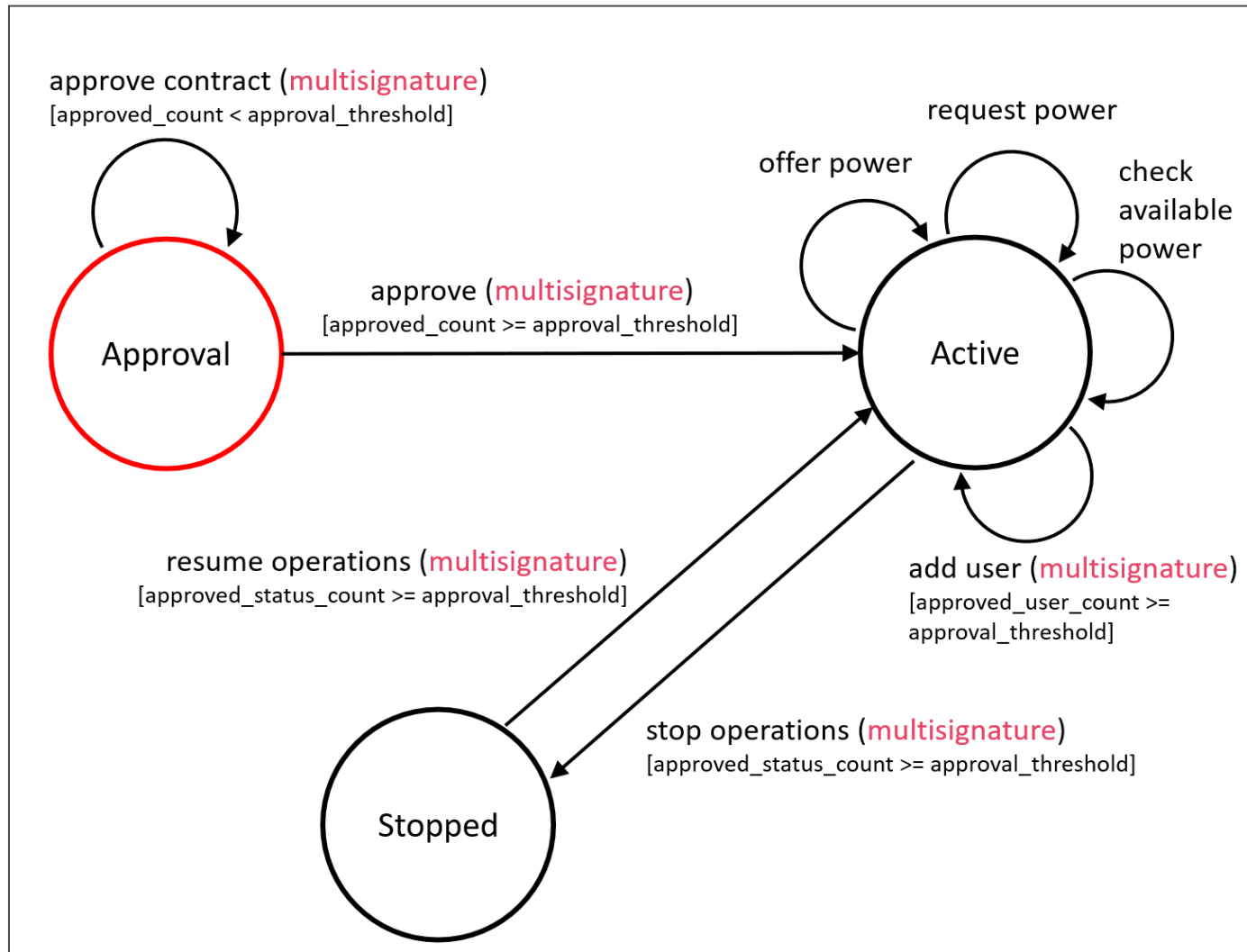
Vilniaus
universitetas

BC platform	Industry focus	Consensus protocol	Programming language	Permissioned/ permissionless	Transactions per second	Native currency
Ethereum	Cross-industry	PoW	Solidity	permissionless	~15	+
Hyperledger Fabric	Cross-industry	pluggable	Go, Java, JavaScript	permissioned	>1000	-
Corda	Cross-industry	RAFT, BFT	Java, Kotlin	permissioned	>100	-
Tendermint	General purpose	BFT	Any via ABCI	permissionless	>10000	-
NEM	Services-oriented	Proof of Importance	Java and C++ via API	permissionless	>100	+
Cardano	Cross-industry	Ouroboros (PoS)	Solidity, Plutus	permissionless	>1000	+
EOS	Cross-industry	delegated PoS	C++	permissioned	>1 Million	+
Stellar	Financial services	SCA (type of FBA)	Multilang. via API	based on proliferated trust	>1000	+
NEO	Smart Economy	Delegated BFT	Multilang. via plug-ins	permissioned	>1000	+

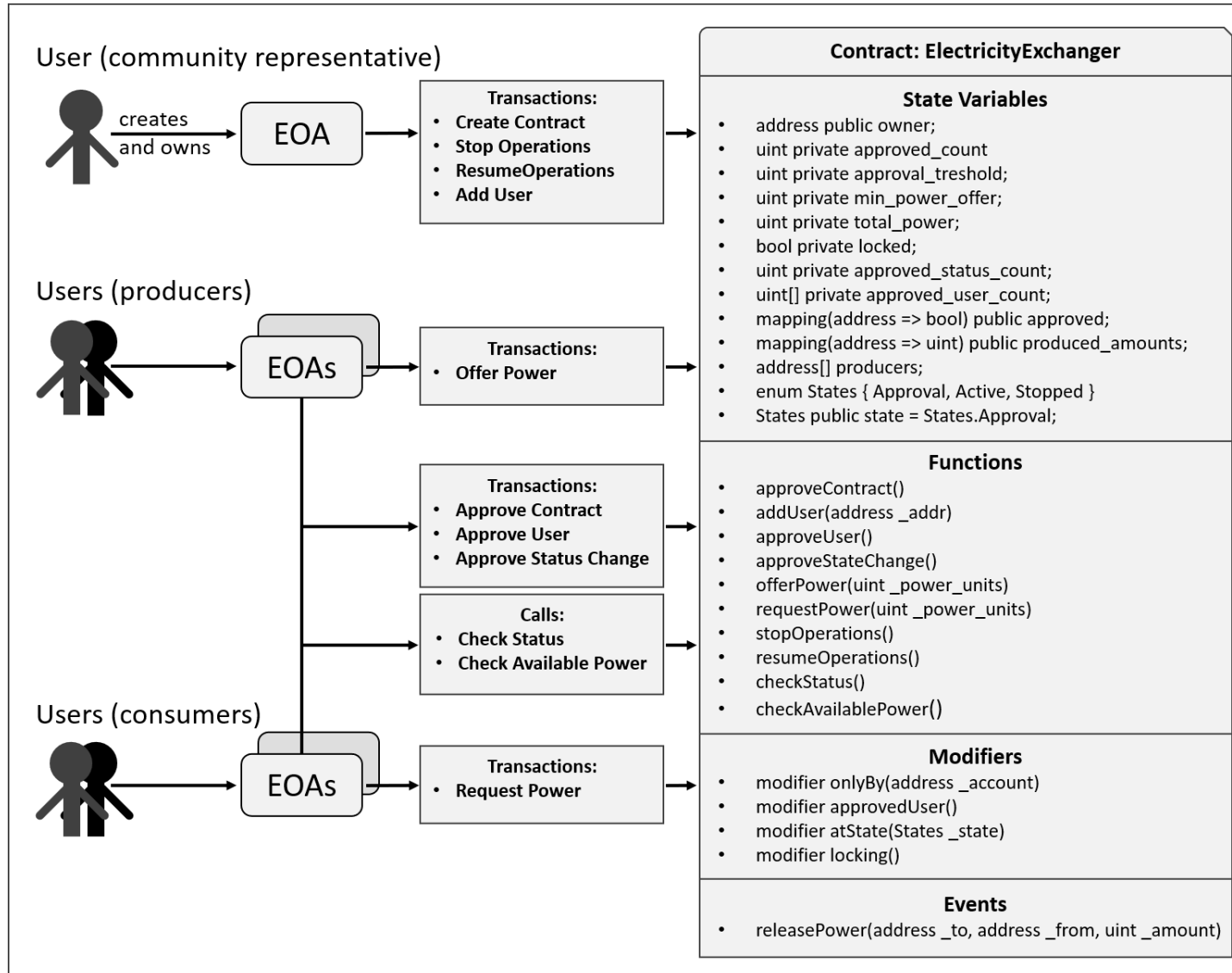
Ethereum išmaniojo kontrakto elektros mainams modelis. Analizės etapas



Ethereum išmaniojo kontrakto elektros mainams modelis. Projektavimo etapas



Ethereum išmaniojo kontrakto elektros mainams modelis. Realizacijos etapas



Ethereum išmaniujų kontraktų pažeidžiamumų (*vulnerabilities*) tyrimas. Testinis rinkinys

Vilniaus
universitetas

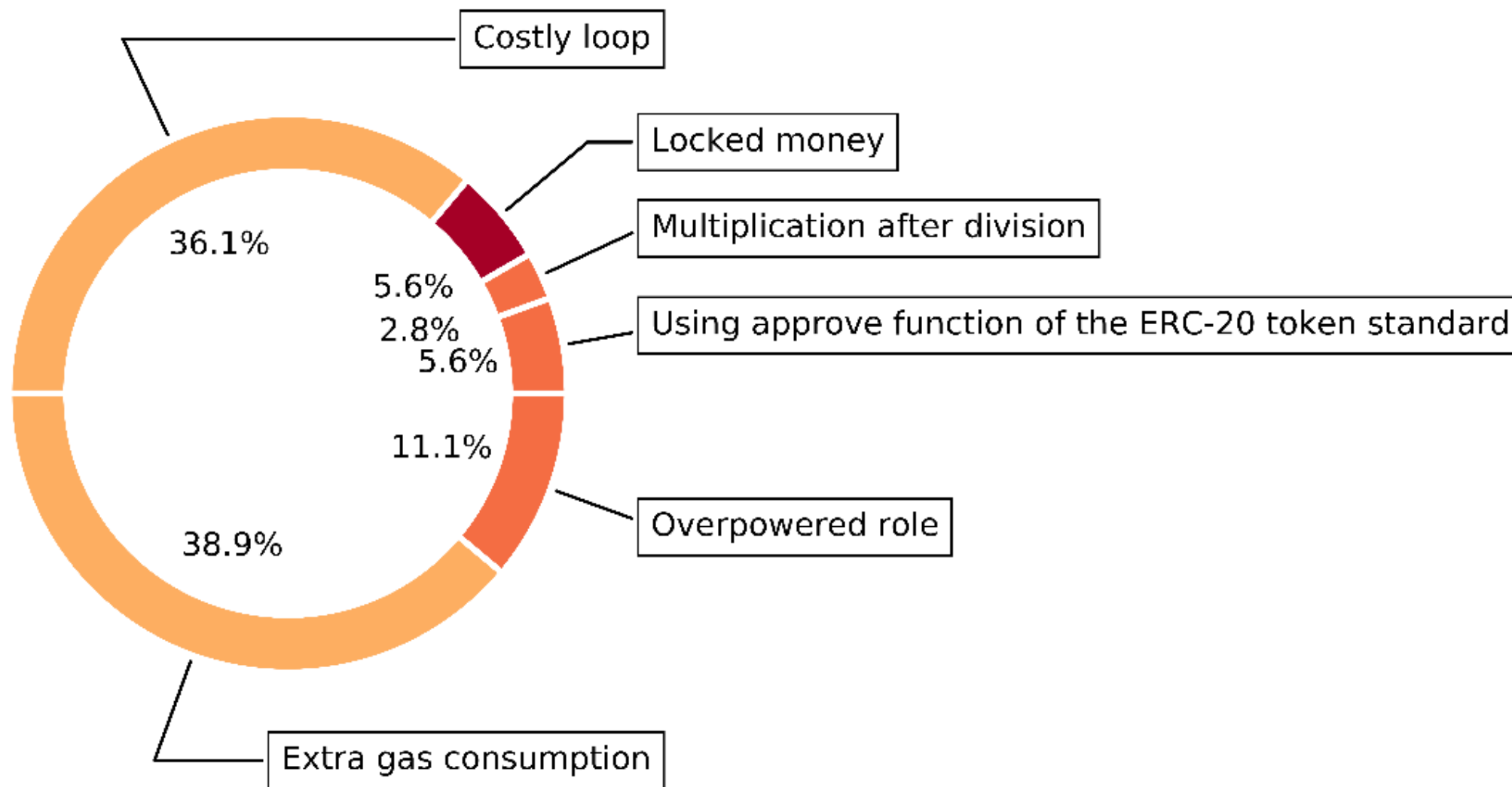
Application Name	Latest version date	Number of files	Number of contracts	External libraries
Carbos	08/04/2019	6	6	0
SunContract	27/11/2019	2	8	0
Grid+	20/12/2018	7	7	0
GoGreenContract	19/02/2019	1	2	0
WePowerNetwork	28/01/2018	19	22	1
HivePower	18/05/2018	17	15	2
TOTAL		52	60	3

Pažeidžiamųjų testavimo rezultatai

Vilniaus
universitetas

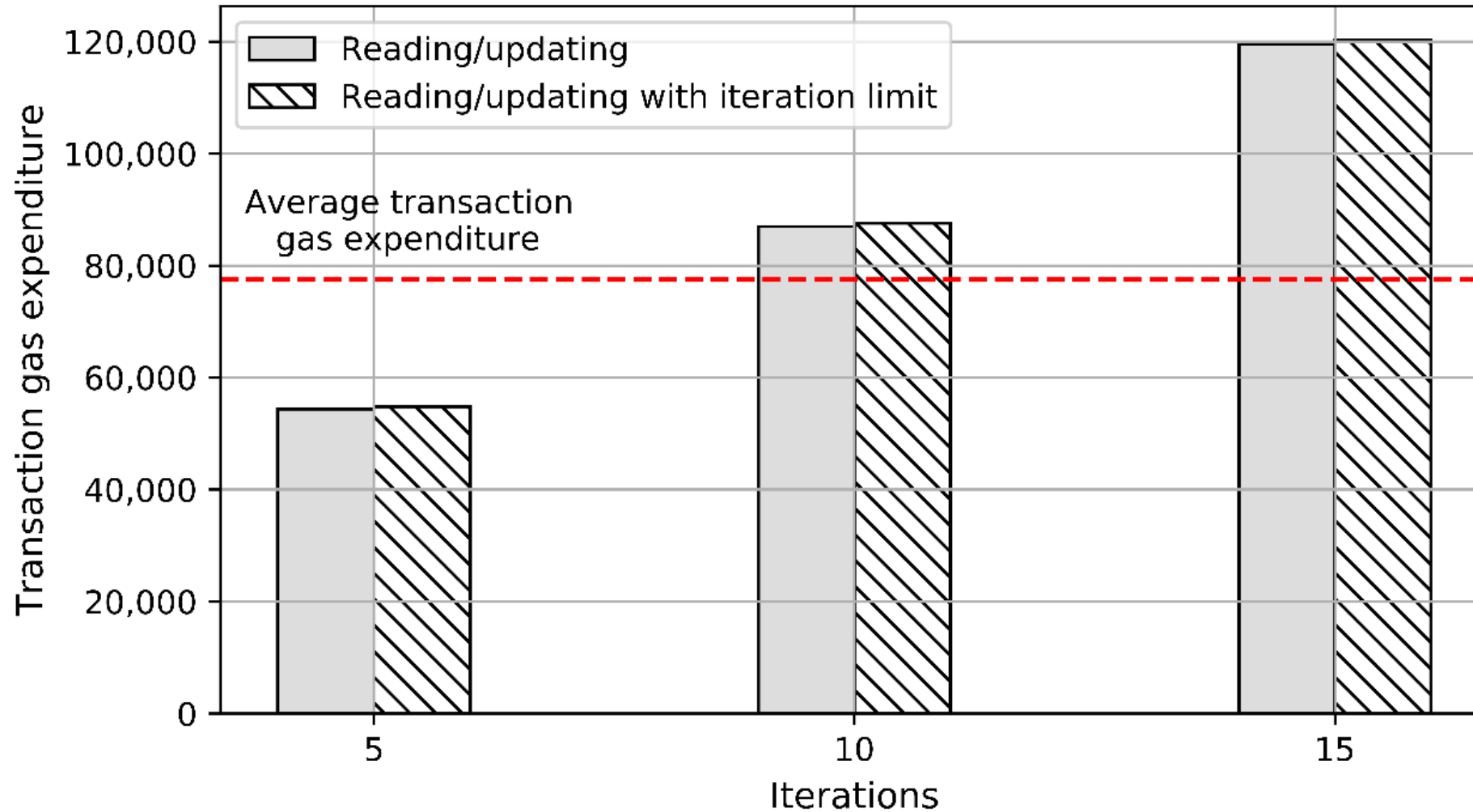
Application Name	Total errors	Errors per SLOC	Severity 1	Severity 2	Severity 3
Carbos	22	0,06	21	1	0
SunContract	156	0,43	154	2	0
Grid+	216	0,38	216	0	0
GoGreenContract	13	0,10	13	0	0
WePowerNetwork	208	0,11	203	4	1
HivePower	90	0,11	89	0	1
TOTAL	705		696	7	2

Pažeidžiamųjų dažnis



Sumodeliuoto išmaniojo kontrakto *Gas* sunaudojimas skaitymo ir įrašymo operacijoms

Vilniaus
universitetas



- Atlikta blokų grandinių platformų, kuriose galimas išmaniųjų kontraktų panaudojimas, charakteristikų analizė. Teorinam ir eksperimentiniam tyrimams pasirinkta *Ethereum* platforma.
- Sumodeliuotas *Ethereum* išmanusis kontraktas elektros mainams tarp vartotojų-gamintojų.
- Ištestuota 60 išmaniųjų kontraktų iš 6 energetikos srities atviro kodo projektų, identifikuoti pažeidžiamumai ir trūkumai.
- Gautų rezultatų pagrindu sumodeliuotas *Ethereum* išmanusis kontraktas realizuojantis aukcionui būdingus pasikartojančius veiksmus.
- Jo pagalba nustatyti lūžio taškai duomenų skaitymo bei skaitymo-jrašymo tranzakcijoms – tai yra iteracijų skaičius, prie kurio pasiekiamas *vidutinis Gas sunaudojimas tranzakcijai*.
- *Ethereum* tinkle tikslinga realizuoti elektros prekybą aukciono pagalba tarp nedidelio skaičiaus dalyvių (~10). Didesnis dalyvių kiekis gali lemti tranzakcijų užlaikymą ir prekybos proceso sutrikdymą.
- Tolesni tyrimai bus atliekami su *Hyperledger Fabric* platforma.

2020/2021 m. m. darbo planas

Vilniaus
universitetas

- **Moksliniai tyrimai:**
 - ✓ Tęsiami teorinis ir empirinis tyrimai;
 - ✓ taikomojo modelio sudarymas ir testavimas.
- **Dalyvavimas mokslinėse konferencijose**
 - ✓ Ruošiamas pranešimas tema „Study of blockchain based solutions for sustainable distributed electricity trading network“ dalyvavimui 15-ojoje prof. Vlado Gronsco tarptautinėje mokslinėje konferencijoje;
 - ✓ Dalyvavimas su pranešimu tarptautinėje konferencijoje Information and Software Technologies (ICIST 2021).
- **Mokslinės stažuotės**
 - ✓ 2019/2020 m. m. laikotarpiui numatytos stažuotės planuojamos kompensuoti dalyvaujant online mokomosiose konferencijose, organizuojamose užsienio aukštųjų mokyklų ir/arba verslo įmonių.
- **Parengti mokslinę publikaciją ISI web of Science žurnale**



**Vilnius
universitetas**

Paulius Danielius
VU Kauno fakulteto doktorantas
paulius.danielius@knf.vu.lt