VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ KATEDRA

Pakartotinis kodo panaudojimas pirminio kriptovaliutų platinimo išmaniuosiuose kontraktuose

Code Reuse in Initial Coin Offering Smart Contracts

Bakalauro darbo planas

Atliko: Agnė Mačiukaitė (parašas)

Darbo vadovas: lekt. Gediminas Rimša (parašas)

Vilnius – 2019

TURINYS

1. Bakalauro darbo planas

Pirminis kriptovaliutų platinimas (angl. initial coin offering, toliau ICO) yra reikšminga naujovė, naudojama verslui finansuoti. Tarp 2014 metų sausio ir 2018 birželio ICO surinko daugiau nei 18 milijardų dolerių. Lėšų surinkimas ICO būdu pritraukė verslininkų, investuotojų ir reguliavimo įstaigų dėmesio. Dauguma ICO kuria išmaniuosius kontraktus (automatizuotą programinę įrangą) ir juos talpina Etheruem blockchain [HNY18].

Problema: per trumpą laiką buvo sukurta daug panašių išmaniųjų kontraktų, kurie dažnai kuriami kopijuojant jau esamus ICO išmaniuosius kontraktus bei pridedant reikiamus pakeitimus. Taip sukurta didelė aibė ICO išmaniųjų kontraktų, kurių kodas yra labai panašus arba kartojasi. Pernaudojamumo problemą išspręsti bandoma Ethereum išmaniųjų kontraktų bibliotekomis, tačiau jos ne visada padengia visą ICO išmaniųjų kontraktų savybių aibę.

1.1. Tyrimo objektas

Tyrimo objektas - OpenZeppelin ir TokenMarket savybių modeliai. OpenZeppelin ir TokenMarket - atviro kodo Ethereum išmaniųjų kontraktų bibliotekos, populiariausios GitHub[1] versijų valdymui skirtame tinklapyje.

1.2. Darbo tikslas

Darbo tikslas: remiantis savybių modeliu, atvaizduojančiu Ethereum blockchain patalpintų ICO išmaniųjų kontraktų savybes, patikrinti ar Ethereum bibliotekos padengia visas savybes, bei pasiūlyti būdą ICO išmaniųjų kontraktų kodo pernaudojamumui didinti.

1.3. Darbo uždaviniai

Tikslui pasiekti išsikelti uždaviniai:

1. Parengti ICO išmaniųjų kontraktų savybių modelį iš išmaniųjų kontraktų, patalpintų Ethereum blockchain ir jį validuoti;
2. Parengti ICO savybių modelius iš OpenZeppelin ir TokenMarket bibliotekų;
3. Palyginti savybių modelį, sukurtą iš Ethereum blockchain esančių ICO išmaniųjų kontraktų, su OpenZeppelin ir TokenMarket savybių modeliais;
4. Pasiūlyti pakeitimus vienai iš bibliotekų, remiantis savybių modelių palyginimu.

1.4. Laukiami rezultatai

Atsižvelgus į darbo tikslą ir uždavinius, laukiami rezultatai:

1. Sukurtas ICO savybių modelis iš išmaniųjų kontraktų, patalpintų Ethereum blockchain;
2. Sukurti ICO savybių modeliai iš OpenZeppelin ir TokenMarket bibliotekų;
3. Nustatytos savybės, kurių OpenZeppelin ir TokenMarket nepalaiko;

[1] `https://github.com/`

4. Savybių, kurių neįgyvendina OpenZeppelin ar TokenMarket, įgyvendinimas vienai iš bibliotekų.

1.5. Tyrimo metodas

Produktų linijos programinės įrangos inžinerija (angl. product line software engineering, toliau - PLSE) naudojama įmonėse pakartojamumui susijusiuose programinės įrangos produktuose numatyti. PLSE suteikia bendrą architektūrą ir pernaudojamą kodą programinės įrangos kūrėjams [SVB01]. Toks kūrimas susideda iš savybių išskyrimo ir jų įgyvendinimo produkte. Gerai išskirtos produkto ypatybės padeda sukurti lengvai pernaudojamą programą [LKL15].

Savybių modeliavimas yra pagrindinis metodas atrinkti bei valdyti bendrąsias ir kintamąsias savybes PLSE [CHE04]. Savybių modeliavimas yra populiariausias PLSE kūrime nuo pat pirmojo jo pristatymo [KCH+90].

Savybių pernaudojimo metodas (angl. feature-oriented reuse method, toliau - FORM) praplėčia savybių modeliavimą bei nusako, kaip remiantis savybių modeliu sukurti programinės įrangos architektūrą ir komponentus. FORM teigia, kad savybės apibūdina galimus galutinio produkto variantus, o kodas, kuris įgyvendina savybes, turi būti sukurtas pakartotiniam panaudojimui [KKL+98].

Atsižvelgiant į tai, išsikeltam tikslui pasiekti pasirinktas savybių modeliavimas.

1.6. Darbo atlikimo procesas

1. Apžvelgti kodo pernaudojimo galimybes, naudojantis savybių modeliu;
2. Surinkti 150-200 ICO išmaniuosius kontraktus, esančius Ethereum blockchain. Sumažinti surinktų išmaniųjų kontraktų aibę iki išmaniųjų kontraktų, kurie realizuoja tik ICO funkcionalumą (nerealizuoja žetono (angl. token) funkcionalumo);
3. Sukurti ICO savybių modelį iš atrinktų išmaniųjų kontraktų, esančių Ethereum blockchain;
4. Sukurti ICO savybių modelį iš OpenZeppelin bibliotekos;
5. Sukurti ICO savybių modelį iš TokenMarket bibliotekos;
6. Palyginti savybių modelį, sukurtą iš išmaniųjų kontraktų, esančių Ethereum blockchain su savybių modeliais, sukurtais iš OpenZeppelin ir TokenMarket bibliotekų;
7. Pasirinkti biblioteką, kuriai reikia daugiau pakeitimų. Jai pasiūlyti pakeitimus, remiantis savybių modelių palyginimu.

1.7. Aktualūs literatūros šaltiniai

1. Kyo C. Kang, Sholom G. Cohen, James A. Hess, William E. Novak ir A. Spencer Peterson. Feature-Oriented Domain Analysis (FODA) Feasibility Study. 1990
2. Kwanwoo Lee, Kyo C. Kang ir Jaejoon Lee. Concepts and Guidelines of Feature Modeling for Product Line Software Engineering. 2015

3. Kyo C. Kang, Sajoong Kim, Jaejoon Lee, Kijoo Kim, Gerard Jounghyun Kim, Euiseob Shin. FORM: A Feature-Oriented Reuse Method with Domain-Specific Reference Architectures. 1998

Literatūra

[CHE04] Krzysztof Czarnecki, Simon Helsen ir Ulrich Eisenecker. Staged Configuration Using Feature Models. 2004. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.95.1586%7B%5C&%7Drep=rep1%7B%5C&%7Dtype=pdf (tikrinta 2019-03-04).

[HNY18] Sabrina T Howell, Marina Niessner ir David Yermack. INITIAL COIN OFFERINGS: FINANCING GROWTH WITH CRYPTOCURRENCY TOKEN SALES. Tech. atask., 2018. URL: http://www.nber.org/papers/w24774.pdf (tikrinta 2019-03-04).

[KCH+90] Kyo C. Kang, Sholom G. Cohen, James A. Hess, William E. Novak ir A. Spencer Peterson. *Feature-Oriented Domain Analysis (FODA) Feasibility Study*, tom. 18 numeris 3-4. 1990. DOI: 10.1080/10629360701306050.

[KKL+98] Kyo C Kang, Sajoong Kim, Jaejoon Lee, Kijoo Kim, Gerard Jounghyun Kim ir Euiseob Shin. FORM: A Feature-Oriented Reuse Method with Domain-Specific Reference Architectures. Tech. atask., 1998. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.95.7568%7B%5C&%7Drep=rep1%7B%5C&%7Dtype=pdf (tikrinta 2019-03-04).

[LKL15] Kwanwoo Lee, Kyo C. Kang ir Jaejoon Lee. Concepts and Guidelines of Feature Modeling for Product Line Software Engineering. 2015. DOI: 10.1007/3-540-46020-9_5. URL: https://www.researchgate.net/profile/Kwanwoo%7B%5C_%7DLee/publication/221553200%7B%5C_%7DConcepts%7B%5C_%7Dand%7B%5C_%7DGuidelines%7B%5C_%7Dof%7B%5C_%7DFeature%7B%5C_%7DModeling%7B%5C_%7Dfor%7B%5C_%7DProduct%7B%5C_%7DLine%7B%5C_%7DSoftware%7B%5C_%7DEngineering/links/558bdbde08ae591c19d8d3ce.pdf (tikrinta 2019-03-04).

[SVB01] Mikael Svahnberg, Jilles Van Gurp ir Jan Bosch. On the Notion of Variability in Software Product Lines, 2001. URL: http://www.diva-portal.org/smash/get/diva2:837870/FULLTEXT01.pdf (tikrinta 2019-03-04).

Santrumpos

ICO - pirminis kriptovaliutų platinimas (angl. initial coin offering).

PLSE - produktų linijos programinės įrangos inžinerija (angl. product line software engineering)

FORM - savybių pernaudojimo metodas (angl. feature-oriented reuse method)