

Pakartotinis kodo panaudojimas pirminio kripto valiutų platinimo išmaniuosiuose kontraktuose

Code Reuse in Initial Coin Offering Smart Contracts

Agnė Mačiukaitė
Vadovas: lekt. Gediminas Rimša

2018-06-25

- ▶ Pakartotinis kodo panaudojimas:
 - ▶ Produktų linijos;
 - ▶ Savybių modeliavimas.
- ▶ Išmanieji kontraktai:
 - ▶ Blockchain;
 - ▶ Pirminis kriptovaliutų platinimas (angl. initial coin offering (ICO)).

Tikslas

Ištirti pirminio finansavimo kriptovaliutomis išmaniuosius kontraktus, nustatyti, kokios savybės yra pastovios, o kokios – kintamos bei pasiūlyti būdus kodo pernaudojamumui didinti.

Tikslui pasiekti išsikelti uždaviniai:

1. Apžvelgti savybių modeliavimą programinės įrangos produktų linijos sričiai;
2. Surinkti virš 100 išmaniųjų kontraktų skirtų ICO;
3. Išskirti surinktų išmaniųjų kontraktų savybes;
4. Sukurti ICO savybių modelį ir jį validuoti.

Savybių modeliavimas

Savybė



- ▶ Savybė - pastebima ir skiriama sistemos charakteristika, kuri yra matoma įvairioms suinteresuotoms šalims;
- ▶ Savybės yra programinės įrangos atributai, kurie tiesiogiai paveikia naudotoją.

Savybių modeliavimas

Savybių modelis



- Savybių modelis - modelis, kuris turi pavaizduoti standartines sistemos šeimos savybes srityje ir santykius tarp jų;

Santykiai tarp savybių



ir



alternatyva



ar



privaloma



pasirenkama

ICO savybių modeliavimas

ICO išmanieji kontraktai



- ▶ ICO išmaniųjų kontraktų surinkimas;
- ▶ ICO išmaniųjų kontraktų pasirinkimas savybių modeliavimui.

ICO savybių modeliavimas

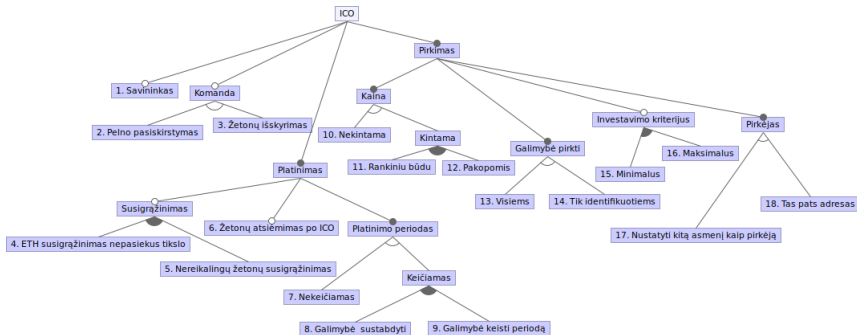
ICO savybės



1. Minimalaus investavimo kriterijus;
2. Kainos už žetoną pakeitimas;
3. Kontrakto savininko nustatymas bei kai kurio funkcionalumo priskyrimas tik jam;
4. Galimybė sustabdyti ICO ir vėl paleisti iš naujo;
5. Pirkimas tik indentifikuotiems naudotojams;
6. ICO pradžios nustatymas;
7. Nustatytas maksimalus galimas žetonų kiekis nupirktas per kartą;
8. Nereikalingų žetonų išsitraukimas iš kontrakto.

ICO savybių modeliavimas

ICO savybių modelis



ICO savybių modeliavimas

ICO savybių modelis



ICO savybių modelio kompozicijos taisyklės:

1. Nereikalingų žetonų susigrąžinimui reikalingas savininkas;
2. Platinimo periodo keitimui reikalingas savininkas;
3. Kainos pakeitimui rankiniu būdu reikalingas savininkas;
4. Žetonus atsiimti po ICO gali tik pirkėjas;
5. ETH susigrąžinti nepasiekus tikslo gali tik pirkėjas.

ICO savybių modeliavimas

ICO savybių modelio validacija



- ▶ Validacijos metodas;
- ▶ Validacijos procesas;
- ▶ Validacijos rezultatas.

1. Apžvelgtos kodo pernaudojimo galimybės naudojantis savybių modeliavimu;
2. Surinkti ICO išmanieji kontraktai bei ištirtos jų savybės;
3. Nustatyta, kurios savybės yra pastovios ir kintamos;
4. Kodo pernaudojamumui didinti sudarytas savybių modelis.

1. Savybių modeliavimas yra geras būdas ICO išmaniųjų kontraktų kodo pernaudojamumui didinti;
2. Yra sukurta pakankamai daug ICO išmaniųjų kontraktų turinčių įvairių savybių, todėl žinant, koks savybių rinkinys yra reikalingas, būtų galima panaudoti esamą kontraktą ar jo dalį.