ITSELF - Information and Finance Technology, Software Engineering and Learning, 2022 Nr. 3, p. 10–12
ISSN 2669-0969, http://ojs.kaunokolegija.lt/index.php/ITSELF

IŠMANIEJI KONTRAKTAI IR JŲ KŪRIMO TECHNOLOGIJOS

Arminas Kurlianskis, vadovas Eligijus Sakalauskas
Kauno kolegija

Anotacija

Blokų grandinės technologijos suteikia daug naujų galimybių. Išmanieji kontraktai leidžia aprašyti sąlygas kaip transakcijos turėtų būti vykdomos tarp dviejų šalių. Transakcijos bei patalpinti įrašai yra vieši, taip pat duomenys blokų grandinėje yra nekintami. Šios savybės leidžia finansinius sandorius vykdyti kitaip, nei įprasta. Atliekant apžvalgą ir tyrimą bus aprašomi išmaniųjų kontraktų privalumai ir technologijos, kurios leidžia tokius kontraktus kurti.

Raktiniai žodžiai: blokų grandinės, išmanieji kontraktai, transakcijos.

ĮVADAS

Blokų grandinės technologijos evoliucijos raida atvėrė naujų galimybių spektrą informacinėms ir finansinėms technologijoms. Viena iš svarbiausių savybių yra decentralizacija – nebuvimas vienos sistemą valdančios esybės. Tai suteikia galimybę internetą, kaip ekosistemą, perimti vartotojams į savo rankas. Taip pat dalis blokų grandinės platformų turi savo išmaniuosius kontraktus. Jie leidžia vykdyti sandorius, apibrėžiant sąlygas kaip esybės, kurios gali bendradarbiauti, kaip žetonai bus perkeliami priklausant nuo sandorio vykdymo, kontrakto galiojimo.

Pritaikius šį išmaniųjų kontraktų sprendimą finansinėse srityse būtų galima sumažinti pinigus, išleidžiamus tarpininkavimo mokesčiams. Kadangi išmanusis kontraktas vykdo funkcijas pagal tai, kaip jis yra sudarytas ir kokios funkcijos yra iškviečiamos, dalykai, kuriuos atlieka tarpininkas, sandoryje tampa nebereikalingais. Žinoma, skirtingos blokų grandinės platformos siūlo skirtingus išmaniųjų kontraktų kūrimo būdus. Vienas iš populiariausių sprendimų yra „Ethereum“ platformos „Solidity“ išmaniųjų kontraktų programavimo kalba. Jos pagalba yra sukurta nepakeičiamų žetonų įsigijimo platformos, kriptovaliutos žetonų keityklos, decentralizuotos programėlės, kompiuteriniai žaidimai, naudojantys mikrotransakcijas. Kita pradedanti decentralizuotų finansų (*angl. DeFi*) implementaciją yra platforma „Cardano“, suteikianti galimybę kurti išmaniuosius kontraktus „Plutus“ platformos pagalba.

Tikslas: apžvelgti išmaniuosius kontraktus ir juos palaikančias platformas.

Uždaviniai:

1. Apibūdinti išmanųjį kontraktą.
2. Apžvelgti „Ethereum“ platformą ir „Solidity“ išmaniųjų kontraktų programavimo kalbą.
3. Apžvelgti „Cardano“ platformą ir „Plutus“ išmaniųjų kontraktų programavimo kalbą.
4. Palyginti apžvelgtas išmaniųjų kontraktų kūrimo technologijas.
5. Apibendrinti technologijas.

1. Išmanieji kontraktai

Išmanus kontraktas (*angl. Smart contract*) yra kompiuterio protokolas, skirtas skaitmeniniu būdu patikrinti sutartį ir priversti ją vykdyti. Išmanūs kontraktai leidžia atlikti sandorius tarp dviejų pusių be tarpininkų. Skirtumas nuo paprasto kontrakto yra tai, jog išmanus kontraktas yra savarankiškai vykstantis kodas, kuris savyje turi kontrakto sąlygas. Tas kodas nusiunčiamas į adresą, kuris talpinamas į blokų grandinę, ir identifikuojamas kaip transakcija. Jį paleidžiame nusiųsdami transakciją, tokiu būdu kontraktas yra vykdomas savarankiškai ir automatiškai, kaip buvo suprogramuotas (Christidis, Devetsikiotis, 2016). Kai ši transakcija yra blokų grandinėje, išmanus kontraktas yra inicijuotas ir neatšaukiamas. Tokiu būdu išmanus kontraktas paveldi blokų grandinės savybes, kaip nekintamumas. Tai reiškia, kad blokų grandinės mazgai patvirtina išmanųjį kontraktą ir prideda jį į bloką. Išmanių kontraktų privalumas yra pašalinimas poreikio turėti tarpininką ar brokerį, kuris patvirtintų sutartį. Taip galima išvengti trečiosios šalies manipuliacijos sutartimis ar įsikišimo.

Išmanus kontraktas yra traktuojamas kaip adresas, todėl jis gali priimti apmokėjimą ir laikyti savo adresu žetonus. Taip pat kontraktas saugo informaciją, kuri gali būti sveikasis skaičius, sąskaitų adresai, teksto eilutės, kintamųjų struktūros. Išmanus kontraktas leidžia sukurti verslo logiką ir patalpinti ją blokų grandinėje. Vartotojai gali skaityti kontrakto reikšmes naudodami užklausas bei siųsti užklausą, patalpinti informaciją ar pervesti žetonus į kontraktą. Individai, norintys įrašyti duomenis blokų grandinėje, turi sumokėti kompiutavimo mokestį (*angl. gas fee*) tam, kad blokų grandinės mazgai užšifruotų siunčiamą užklausą kaip transakciją ir patalpintų ją.

2. „Solidity“ programavimo kalba ir „Ethereum“ blokų grandinės platforma

„Ethereum“ platformoje išmanūs kontraktai kuriami „Solidity“ programavimo kalba, kuri leidžia aprašyti aplikacijos logiką ir komunikuoti su blokų grandine. Sintaksė buvo sukurta bendro pobūdžio programavimo kalba – „ECMAScript“, kad būtų atpažįstama žiniatinklių kūrėjams. „Solidity“ išmanūs kontraktai yra sukompiliuojami į programos dvejetainę sąsają (*angl. application binary interface*), tokiu būdu galima suderinti kontraktų funkcionalumą su naudotojo sąsajos programavimo kalba, pvz. JavaScript. „Solidity“ yra imperatyvinė programavimo kalba, kuri naudoja formuluotes išreikšti logiką kaip kodas turi būti vykdomas. „Ethereum“ platforma suteikia integruoto kūrimo aplinką naršyklėje pavadinimu „Remix“. Ji leidžia paspartinti išmaniųjų kontraktų kūrimą, testuoti, derinti programas bei palengvina procesą, nurodydama sintaksės klaidas.

„Ethereum“ platforma naudoja sąskaita pagrįstą modelį (*angl. Account based model*), kuriame likutis yra nurodomas žetonų kiekiu. Tokios sąskaitos yra pasirašomos privataus rakto pagalba (Clifford, 2019). Platformoje yra dviejų tipų paskyros – vartotojų paskyros ir išmaniųjų kontraktų paskyros, kurių identifikacijos numeris yra 40-ties skaitmenų šešioliktainis skaičius.

Vartotojas gali patalpinti kontraktą (*angl. deploy*) į blokų grandinę ir joje atsiradusi kontrakto sukūrimo transakcija parodo, jog išmanusis kontraktas yra paviešintas ir paruoštas naudojimui. Sąveika su paviešintu kontraktu vyksta aprašytomis kontrakto funkcijomis, kurias galima implementuoti naudotojo sąsajoje. Tokiu būdu sistema yra atskirta į dvi dalis – *on-chain* ir *off-chain*. Šios dvi dalys yra „Solidity“ programavimo kalba parašytas kodas sąveikauti su blokų grandine ir „JavaScript“ programavimo kalba sukurta naudoto sąsaja naudotis išmaniojo kontrakto funkcijomis.

3. „Plutus“ programavimo kalba ir „Cardano“ blokų grandinės platforma

„Plutus“ yra išmaniųjų kontraktų kūrimo kalbos platforma, skirta kurti aplikacijas, galinčias sąveikauti su platinama didžiąja knyga (angl. distributed ledger) „Cardano“ blokų grandinėje. Ji buvo išleista 2021 m. rugsėjo 12 dieną „IOHK“ kūrimo komandos. „Plutus“ yra paremtas „Haskell“ programavimo kalba, kuri suteikia vieną iš svarbiausių savybių, jog ji yra funkcinė programavimo kalba. Funkcinėse programavimo kalbose programos konstruojamos taikant ir komponuojant funkcijas. Tai suteikia labiau nuspėjamą programavimo būdą. Funkcinių programavimo kalbų sintaksė yra suvaržyta. Toks programavimo būdas pasirūpina kaip kodas bus interpretuojamas mašininio kodo lygyje. Skirtumą tarp funkcinių ir imperatyvinių programavimo kalbų galima įvardinti abstrakcija, kad funkcinės programavimo kalbos dėmesys skirtas „Ką išspręsti“, vietoje to „Kaip išspręsti“ problemą.

Didelė „Plutus“ platformos dalis yra tai, jog ji naudoja Extended UTXO modelį, kuriame vyksta apskaita kaip transakcijos vyksta tinkle. UTXO modelis yra skaitmeninių pinigų abstrakcija. Šį modelį galima apibūdinti kaip įvestys, kurios yra neišleistos išvestys iš buvusių transakcijų ir gali būti panaudojamos tolimesnėms transakcijoms, taip pat reprezentuoja nuosavybės grandinę adresų, kuriems priklauso žetonai. Tokios platformos, kurios naudoja UTXO modelį, neturi sąskaitų ar pinigų likučių. Extended UTXO modelis išplečia įvardintą koncepciją dviem būdais (Brunjes Lars, 2021):

- išvestys su savimi gali turėti savavališkus duomenis,
- adresai gali turėti pritaikytą situacijai logiką instrukcijų formate.

Tikrinimo scenarijai (*angl. validator scripts*) yra „Plutus“ platformos dalis kuriant išmaniuosius kontraktus, kurie tikrina veiksmus, vykstančius blokų grandinėje, ir įgalioja išvesčių perleidimą. Šie tikrinimo scenarijai leidžia patikrint ar transakcija bus įvykdyta nenusiuntus jos į tinklą.

„Plutus“ aplikacijų karkasas yra įrankis, skirtas kurti decentralizuotas programėles. Šis karkasas taip pat yra aprašomas Haskell programavimo kalba. Dėl šios priežasties visa kuriamos sistemos logika yra aprašoma viena kalba. Tai leidžia visą verslo logiką ir transakcijų srautus aprašyti tik kartą. Programos, sukurtos šiuo karkasu, suteikia HTTP ir WebSocket sąsają, kuri suteikia galimybę sąveikauti su aplikacija, naudojant naršyklę.

„Plutus Playground“ yra aplinka, patalpinta internete, ir skirta testuoti išmaniuosius kontraktus prieš paviešinimą į „Cardano“ blokų grandinę. Ši aplinka leidžia simuliuoti kontrakto veiklą, veiksmus, pinigines bei rezultatus. Tai suteikia bendrą supratimą, kaip veikia kontraktai realybėje.

4. Palyginimas

Apžvelgus šių dviejų platformų ir išmaniųjų kontraktų kūrimo priemones palyginsime jas pagal keturis kriterijus, kurie apibūdins esminius skirtumus. Šie kriterijai parodys, kokiomis priemonėmis vyksta decentralizuotų finansų sistemos kūrimas, koks modelis naudojamas vykdant transakcijų srautus, kokia paradigma yra sukurta išmaniųjų kontraktų kūrimo kalba bei kokie įrankiai yra suteikti programuotojams.

1 lentelė. Platformų ir išmaniųjų kontraktų kūrimo priemonių palyginimas

Platforma ir kontraktų kūrimo kalba / Kriterijai	„Ethereum“– „Solidity“	„Cardano“– „Plutus“
Modelis	Account based	Extended UTXO
Integruota kūrimo aplinka	„Remix“	„Plutus Playground“
Programavimo paradigma	Imperatyvinė	Deklaratyvi/funkcinė
Išmaniųjų kontraktų kūrimo kalba	„Solidity“	„Plutus“
Naudotojo sąsajos kalba	„JavaScript“	„Plutus“

5. Apibendrinimas

Atlikus apžvalgą ir palyginimą buvo išsiaiškinta, kaip blokų grandinės funkcionuoja išmaniųjų kontraktų pagalba. Apžvelgtos išmaniųjų kontraktų kūrimo technologijos turi programuotojams suteiktus įrankius kurti programas sąveikauti su blokų grandine. Įvardinti įrankiai nereikalauja pasiruošimo pradėti analizuoti išmaniųjų kontraktų veikimo principą. Tačiau buvo pastebėtas „Plutus“ kontraktų kūrimo kalbos ir jos ekosistemos pranašumas dėl to, jog aplikacijų kūrimui galima naudoti vieną kalbą, kuri padeda išlaikyti aplikacijos logiką viename formate. Taip pat buvo išanalizuota, jog „Cardano“ blokų grandinės transackijų modelis Extended UTXO padeda apsaugoti tinklą nuo pakartojimo atakų (*angl. Replay attacks*) įvesdamas daugiau kintamųjų įrodyti, jog transakcija yra pagrįsta. Dar vienas aspektas, parodantis „Cardano“ blokų grandinės ir „Plutus“ išmaniųjų kontraktų programavimo kalbos pranašumą, yra jų naudojama funkcinė programavimo paradigma, kuri yra išvesta iš deklaratyvinės paradigmos. Ši paradigma turi suvaržytą sintaksę bei yra naudojami pareiškimai kaip programa turi veikti. Toks sprendimas yra geresnis kai yra dirbama su finansais, nes tai sumažina kodo klaidas sandorio metu.

Literatūra

1. CHRISTIDIS, K.; DEVETSIKIOTIS M. Blockchains and smart contracts for the internet of things. Raleigh: Šiaurės Karolinos valstijos universitetas, 2016 [žiūrėta 2021 m. lapkričio 21 d.]. Prieiga per internetą: <https://ieeexplore.ieee.org/abstract/document/7467408> ISSN 2169-3536
2. BRUNJES, L. Plutus: what you need to know. 2021 [žiūrėta 2021 m. lapkričio 25 d.]. Prieiga per internetą: <https://iohk.io/en/blog/posts/2021/04/13/plutus-what-you-need-to-know/>
3. Learn about Plutus. Cardano Docs [žiūrėta 2021 m. lapkričio 26 d.]. Prieiga per internetą: <https://docs.cardano.org/plutus/learn-about-plutus>
4. CLIFFORD, J. Intro to Blockchain: UTXO vs Account based. 2019 [žiūrėta 2021 m. lapkričio 26 d.]. Prieiga per internetą: <https://jcliff.medium.com/intro-to-blockchain-utxo-vs-account-based-89b9a01cd4f5>

SMART CONTRACTS AND THEIR DEVELOPMENT TECHNOLOGIES

Arminas Kurlianskis, supervisor Eligijus Sakalauskas

Kaunas University of Applied Sciences

Summary

Blockchain technology gives us new possibilities. Smart contracts lets to make the conditions for transactions and how they should behave beetween to parties. Records of transactions and data inputs are public, also data in blokcchain is immutable. Because of hese properties of blockchain, transactions can be made differently than before. By doing this technology review and analysis, we will introduce advantages of smart contracts and blockchain technology which brings no concept of digital tranactions and digital money.