VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ KATEDRA

Skaitmeninės tapatybės valdymas taikant blokų grandinę

Digital Identity Management using Blockchain

Bakalauro darbas

Atliko:	Jurgis Kargaudas	(parašas)
Darbo vadovas:	asist. Aurimas Šimkus	(parašas)
Darbo recenzentas:	TO BE ADDED	(parašas)

Vilnius – 2018

Santrauka

Šiame darbe nagrinėtas blokų grandinės technologijos tinkamumas skaitmeninių tapatybių valdymui. Apžvelgus esamų identifikavimo sprendimų savybes, tirta blokų grandinė ir jos charakteristikos, kurios leistų įveikti dabar kylančius naudotojų atpažinimo iššūkius.

Nustatyta, kad blokų grandinė gali būti taikoma skaitmeninės tapatybės valdymui tokioje srityje, kur ši technologija padeda išspręsti tokias bėdas. Sukurtas pateikto sprendimo prototipas, parašytas su Language3000 programavimo kalba.

Raktiniai žodžiai: autentifikavimas, tapatybės atpažinimas, skaitmeninė tapatybė, skaitmeninės tapatybės valdymas, blokų grandinė

Summary

In this paper, blockchain applicability for digital identity management was investigated. After an overview of current identification solution properties, blockchain and its characteristics were examined, in order to find out whether the technology is suitable to overcome present user identification challenges.

It was determined that blockchain can be used for digital identity management in this/these fields, where it allows to solve those issues. A prototype of the solution was presented, which was written using Language3000 programming language.

Keywords: authentication, identity recognition, digital identity, digital identity management, blockchain

Įvadas

Naudojimasis interneto paslaugomis šiais laikais yra neatsiejama žmonių gyvenimo dalis. Norėdami individualizuoti turinį, sustiprinti taikomosios programos saugumą ar siekdami iš anksto išvengti kenkėjiškų tikslų turinčių asmenų ar sukurtų robotų, paslaugų tiekėjai neretai prašo naudotojų prisijungti. Interneto naudotojų skaičiui perkopus 4 milijardus [Min18], o kiekvienam naudotojui vidutiniškai turint po 7 skirtingas socialines paskyras [MM17], asmenų autentifikavimas tampa vis didesniu iššūkiu.

Susidariusi situacija kelia problemų tiek paslaugų tiekėjams, tiek jų naudotojams. Kiekvienas paslaugų tiekėjas turi skirti papildomų resursų naudotojų tapatybių valdymui, jų autentifikavimui, jautrių duomenų saugumo užtikrinimui. Paslaugų naudotojams bene didžiausi atsiradę keblumai - milžiniškas įsimintinų slaptažodžių kiekis bei sunkumai kontroliuojant savo asmens duomenų sklaidą skirtingose sistemose. Prisijungimo vardui ir slaptažodžiui išliekant populiariausiais asmens atpažinimo įrankiais, naudotojai dėl per didelio įsimintinų slaptažodžių kiekio neretai paaukoja saugumą dėl patogumo ir pradeda naudoti tą patį slaptažodį sirtingoms sistemoms [PM03; Sam99]. Naudotojas, turėdamas keletą paskyrų skirtingose sistemose, taip pat praranda dalį savo asmens duomenų kontrolės. Jam tenka pasitikėti taikomosios programos naudojamomis technologijomis ir metodais ir tikėtis, kad jie bus pakankamai saugūs ir stabilūs bei suteikti asmens duomenys nepasieks nepageidaujamų adresatų. Didėjant naudojamų paslaugų kiekiui, naudotojo skaitmeninės tapatybės duomenis turi vis daugiau taikomųjų programų ir bent vienai iš jų patyrus programišių įsilaužimą ar kitokią nesėkmę, jautrūs naudotojo duomenys būna paviešinti.

Pagrindiniu skaitmeninės tapatybės valdymo keliamų problemų sprendimu išlieka vienkartinis prisijungimas (angl. *Single Sign-On*). Šis sprendimas leidžia naudotojui pasirinkti vieną tapatybės tiekėją (angl. *identity provider*) ir patikėti jam skaitmeninės tapatybės valdymą. Tuomet naudotojas prie visų paslaugų, palaikančių pasirinkto tapatybės tiekėjo (pvz. *Facebook*) prisijungimą, gali autentifikuotis naudodamas ta pačia paskyra. Tokiu būdu naudotojui pakanka prisiminti tik slaptažodžius, užregistruotus tapatybės tiekėjų sistemose, o paslaugų tiekėjai neturi patys rūpintis autentifikavimu ar autorizavimu, o jį užtikrina integruodami sistemą su tapatybės tiekėju. Tačiau šis sprendimo būdas taip pat turi aiškių trūkumų - naudotojas negali prisijungti prie paslaugų, nepalaikančių pasirinkto tapatybės tiekėjo, dėl paslaugų tiekėjų priklausomybės nuo tapatybės tiekėjo pastarojo pasiekiamumas tampa vieninteliu nesėkmės tašku (angl. *single point of failure*), naudotojas taip pat praranda dalį savo asmens duomenų kontrolės. Naršantis internete asmuo yra priverstas pasitikėti tapatybės tiekėjo gebėjimu perduoti tik naudotojo leistus asmens duomenis ir tik toms trečiosioms šalims, kurias jis patvirtina. Kaip rodo *Cambridge Analytica* neleistino duomenų perdavimo incidentas [Gra18], net didžiosios kompanijos, tokios kaip *Facebook*, ne visada sugeba tai užtikrinti.

Blokų grandinė (angl. *blockchain*) yra nauja alternatyva skaitmeninės tapatybės valdymui. Ši technologija veikia kaip paskirstytų įrašų platforma (angl. *Distributed Ledger Platform*), kurioje kiekvienas įrašas yra nekintamas (angl. *immutable*), o visi užfiksuoti įrašai atspindi tikslią transakcijų istoriją nuo pat grandinės sukūrimo [Baa16]. Saugant tapatybės duomenis šioje grandinėje ir pritaikius reikiamą blokų grandinės pasiekiamumo lygį įrašų rašymui ir skaitymui,

asmuo visada žinotų, kokia trečioji šalis gali pasiekti kokius tapatybės duomenis. Kadangi blokų grandinė yra decentralizuota, pritaikius ją skaitmeninių tapatybių valdyme taip pat būtų galima išvengti šioje srityje dažnos vienintelio nesėkmės taško problemos. Šiame darbe nagrinėjama, kada verta naudoti blokų grandinę naudotojų skaitmeniniam autentifikavimui bei autorizavimui, kokie to pranašumai, trūkumai bei priėmimo barjerai (angl. *adoption barriers*).

Darbo tikslas - ištirti blokų grandinės tinkamumą skaitmeninės tapatybės valdymui.

Darbe keliami uždaviniai:

1. Išnagrinėti esamus skaitmeninės tapatybės valdymo sprendimus ir jų keliamus iššūkius.
2. Apibūdinti blokų grandines ir jų savybes, leidžiančias išspręsti dabartines identifikavimo problemas.
3. *Apžvelgti esamas blokų grandinės sistemas, taikomas naudotojų autentifikavimui ar autorizavimui*.
4. Išskirti blokų grandinės panaudos atvejį skaitmeninės tapatybės valdymui ir įvertinti jo tinkamumą apibūdinant sprendimo privalumus, trūkumus ir pritaikymo barjerus.
5. Palyginti pristatytą sprendimą su standartiniais naudotojų autentifikavimo ir autorizavimo būdais.
6. Pademonstruoti sudaryto skaitmeninio tapatybės valdymo modelio veikimą naudojantis kažkuriuo blockchainu.

TURINYS

ĮVADAS 3

1. SKAITMENINĖS TAPATYBĖS VALDYMO APŽVALGA 6
   1.1. Tapatybės patvirtinimo poreikis 6
   1.2. Skaitmeninės tapatybės valdymo samprata 6

REZULTATAI IR IŠVADOS 8

LITERATŪRA 9

SĄVOKŲ APIBRĖŽIMAI 10

PRIEDAI 10
   1 priedas. Niauroninio tinklo struktūra 11
   2 priedas. Eksperimentinio palyginimo rezultatai 12

1. Skaitmeninės tapatybės valdymo apžvalga

1.1. Tapatybės patvirtinimo poreikis

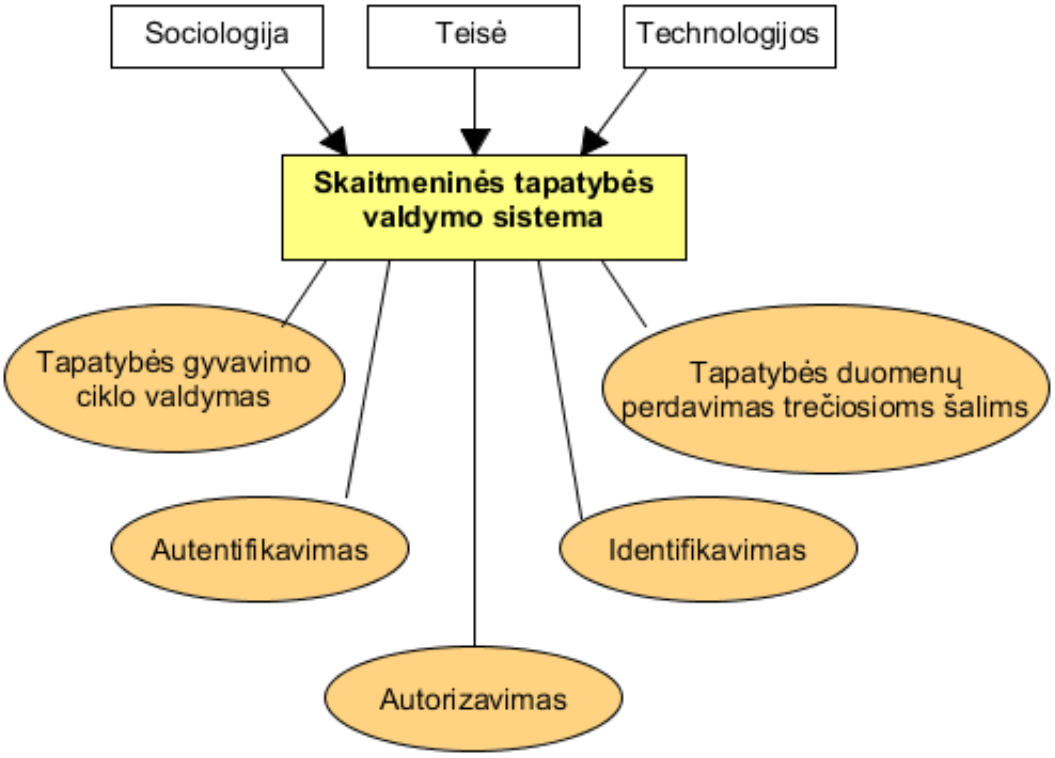
Šiais laikais naudotojo identifikavimas yra svarbi interneto taikomųjų programų dalis. Paslaugų tiekėjai identifikuoja savo naudotojus norėdami [Ral14]:

- registruoti (angl. *log*) naudotojų veiklą,
- užtikrinti, kad naudotojas iš tikrųjų yra asmuo, kuris sakosi esąs,
- suteikti dalį funkcionalumo tik autorizuotiems naudotojams,
- individualizuoti tinklalapio ar taikomosios programos turinį pagal naudotojo poreikius,
- sukurti paslaugos naudotojų bendruomenę,
- išvengti galimų anoniniminių naudotojų atakų.

Dėl išvardytų priežasčių naudotojų identifikavimas atlieka svarbią rolę įvairiose taikomųjų programų srityse - elektroninėje valdžioje, elektroninėje komercijoje, verslo sumanume (angl. *business intelligence*), tyrimuose bei saugume (angl. *homeland security*) [GV09]. Kiekvienas paslaugų tiekėjas turi pasirinkti, kaip autentifikuoti, ir, jei reikia, autorizuoti naudotojus. Programos kūrėjas taip pat turi saugoti naudotojų suteiktus asmens duomenis ir užtikrinti jų saugumą, o naudotojui tenka rūpintis skirtingų turimų paskyrų priežiūra ir savo duomenų sklaida tarp skirtingų sistemų. Minimus tapatybės atpažinimo skaitmeninėje erdvėje aspektus nagrinėja skaitmeninės tapatybės valdymo disciplina.

1.2. Skaitmeninės tapatybės valdymo samprata

Dėl nuolat vykstančios interneto ir jame esančių paslaugų plėtros tapatybių valdymo uždavinys pastaraisiais metais tapo itin svarbus [GV09]. Sprendžiant šį iššūkį, sukurta skirtingų skaitmeninės tapatybės valdymo sistemų, siekiančių išspręsti naudotojų tapatybės atpažinimo problemas. Šioms sistemoms įtaką daro kiti tapatybę nagrinėjantys mokslai (pvz. sociologija), taip pat jos gali atlikti keletą skirtingų funkcijų, susijusių su naudotojų tapatybe. Žemiau pateikiama diagrama, kurioje pavaizduotas tapatybės valdymo sistemų kontekstas bei pagrindinės atliekamos užduotys:



1 pav. Skaitmeninių tapatybių valdymo sistemų kontekstas ir užduotys [GV09]

Paveiksle matomos disciplinos turi skirtingą poveikį tapatybių valdymo sistemoms. Sociologija padeda apibrėžti tapatybę ir jos atitikmenį skaitmeninėje erdvėje, teisės mokslas nusako tapatybės duomenų naudojimo reikalavimus, o esamos technologijos formuoja sistemos įgyvendinimo niuansus. Verta pastebėti, kad tapatybės valdymo sistema gali atlikti ne visas diagramoje nurodomas funkcijas, o tik dalį iš jų. Taip pat, 1-ame paveiksle bei visame darbe naudojamos skaitmeninės tapatybės valdymo sąvokos, tokios kaip *identifikavimas*, *autentifikavimas* ar *autorizavimas* neretai suprantamos skirtingai, o tai sukelia vieningos terminologijos trūkumą ir dėl jo kylančius neaiškumus [GV09]. Dėl to skyriuje „Sąvokų apibrėžimai“ pateikiami darbe dažniausiai naudojamų terminų aiškinimai.

Skirtingų tapatybių valdymo sistemo architektūros bei veikimo principai yra itin skirtingi - jie varijuoja nuo lokalaus autentifikavimo kiekvienai programai iki centralizuotos platformos, dedikuotos tik konkrečiai tapatybės atpažinimo funkcijai. S. Clauß ir M.Köhntopp savo tyrime pastebi, kad nėra vieningo standarto identiteto valdymo sistemoms [CK01]. Tolesniuose skyriuose pateikiamos skirtingos technologijos bei sprendimai, naudojami skaiteminių tapatybių valdyme, jų privalumai bei trūkumai.

Rezultatai ir išvados

Rezultatų ir išvadų dalyje išdėstomi pagrindiniai darbo rezultatai (kažkas išanalizuota, kažkas sukurta, kažkas įdiegta), toliau pateikiamos išvados (daromi nagrinėtų problemų sprendimo metodų palyginimai, siūlomos rekomendacijos, akcentuojamos naujovės). Rezultatai ir išvados pateikiami sunumeruotų (gali būti hierarchiniai) sąrašų pavidalu. Darbo rezultatai turi atitikti darbo tikslą.

Literatūra

[Baa16] Djuri Baars. Towards Self-Sovereign Identity using Blockchain Technology. Disertacija, University of Twente, 2016. URL: http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf.

[Cam04] L.J. Camp. Digital identity. IEEE Technology and Society Magazine, 23(3):34–41, 2004. DOI: 10.1109/MTAS.2004.1337889. URL: http://ieeexplore.ieee.org/document/1337889/.

[CK01] S Clauß ir M Køhntopp. Identity Management and its Support of Multilateral Security. Computer Networks, 37 (2):205–219, 2001.

[Gra18] Kevin Granville. Facebook and Cambridge Analytica, 2018. URL: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (tikrinta 2018-03-28).

[GV09] Uwe Glässer ir Mona Vajihollahi. Identity Management Architecture. 9:97–116, 2009. URL: https://link.springer.com/content/pdf/10.1007%2F978-1-4419-1325-8.pdf.

[Min18] Miniwatts Marketing Group. World Internet Users Statistics, 2018. URL: https://www.internetworldstats.com/stats.htm (tikrinta 2018-03-28).

[MM17] Jason Mander ir Felim McGrath. Global Web Index Social. Tech. atask., 2017. URL: https://cdn2.hubspot.net/hubfs/304927/Downloads/GWI%20Social%20Summary%20Q3%202017.pdf.

[PM03] Andreas Pashalidis ir Chris J. Mitchell. A taxonomy of single sign-on systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2727 LNCS:249–264, 2003. ISSN: 03029743.

[Ral14] Raluca Budiu. Login Walls Stop Users in Their Tracks, 2014. URL: https://www.nngroup.com/articles/login-walls/ (tikrinta 2017-06-10).

[Sam99] V Samar. Single sign-on using cookies for Web applications. Proceedings IEEE 8th International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises WET ICE99:158–163, 1999. ISSN: 10801383.

Sąvokų apibrėžimai

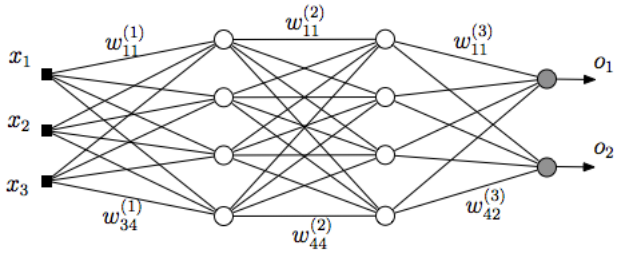
Atributas - charakteristika, susieta su esybe, pavyzdžiui fiziniu asmeniu. Galimi asmens atributai: gimimo data, vardas, ūgis, pirštų antspaudai [Cam04].

Skaitmeninė tapatybė - abstrakti fizinės esybės reprezentacija, sudaryta iš aibės esybės nuolatinių atributų, kurie vienareikšmiškai susiejami su fizine esybe [Cam04; GV09]. Šiame darbe esybė dažniausiai yra fizinis asmuo.

Skaitmeninės tapatybės valdymas -

Priedas nr. 1

Niauroninio tinklo struktūra



2 pav. Paveikslėlio pavyzdys

Priedas nr. 2
Eksperimentinio palyginimo rezultatai

1 lentelė. Lentelės pavyzdys

Algoritmas	$\bar{x}$	σ^2
Algoritmas A	1.6335	0.5584
Algoritmas B	1.7395	0.5647