Domen Gašperlin
Vrbnje 9c, 4240 Radovljica, Slovenija
Študijski program: Računalništvo in informatika, MAG
Vpisna številka: 63150096

Komisija za študijske zadeve
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko
Večna pot 113, 1000 Ljubljana

Vloga za prijavo teme magistrskega dela
Kandidat: Domen Gašperlin

Domen Gašperlin, študent magistrskega programa na Fakulteti za računalništvo in informatiko, zaprošam Komisijo za študijske zadeve, da odobri predloženo temo magistrskega dela z naslovom:

Slovenski: **Integracija verige blokov in tehnologij semantičnega spleta**
Angleški: **Integration of blockchain and semantic web technologies**

Tema je bila že potrjena lani in je ponovno vložena: ***NE***

Izjavljam, da so spodaj navedeni mentorji predlog teme pregledali in odobrili ter da se z oddajo predloga strinjajo.

Magistrsko delo nameravam pisati v slovenščini.

Za mentorja predlagam:

Ime in priimek, naziv: Slavko Žitnik, Assist. Prof. dr.
Ustanova: Fakulteta za računalništvo in informatiko
Elektronski naslov: Slavko.Zitnik@fri.uni-lj.si

V Ljubljani, 23. december 2020.

PREDLOG TEME MAGISTRSKEGA DELA

1 Področje magistrskega dela

slovensko: računalništvo in informatika, verige blokov, semantični splet
angleško: computer science, blockchain, semantic web

2 Ključne besede

slovensko: semantični splet, verige blokov, ontologije
angleško: semantic web, blockchain, ontologies

3 Opis teme magistrskega dela

Pretekle potrditve predložene teme:
Predložena tema ni bila oddana in potrjena v preteklih letih.

3.1 Uvod in opis problema

Kot decentralizirana baza tehnologija verige blokov pridobiva uporabnost na številnih področjih kot so finance, oskrbovalne verige in medicina [1]. S porastom števila aplikacij na verigi blokov se pojavljajo nove zahteve za bolj učinkovite in fleksibilne načine dostopa do podatkov na njej [2, 3, 4]. Večino verig za shranjevanje podatkov uporablja pare ključ in vrednost. V njih se hranijo podatki in zgostitve, ne pa tudi semantične informacije [3, 4] npr. v primeru pametnih pogodb na Ethereumu se privzeto ne hranijo pripadajoči metapodatki, ampak zgolj bitna koda. Tehnologije semantičnega spleta po drugi strani omogočajo definicijo sheme in podatkov na takšen način, da lahko po njih učinkovito poizvedujemo in preko njih sklepamo. Zanima nas, v kakšni meri lahko z dodatkom semantičnih lastnosti verigi blokov in pametnim pogodbam izboljšamo poizvedovalne in inferenčne možnosti ter kako se bo naš sistem obnašal v praktičnem scenariju. Tako bi področje semantičnega spleta obogatilo tehnologijo verige blokov in s tem bi obe področji pridobili uporabno vrednost.

3.2 Pregled sorodnih del

Obstoječi pristopi so koncepte verig blokov in semantičnega spleta združili za učinkovito poizvedovanje podatkov po njih ali po kombinirani shrambi izven njih. Drugi so ontologije uporabili za učinkovito poizvedovanje po pametnih pogodbah ali za predstavitev pravil za potrjevanja transakcij. Mogoč način uporabe pa je tudi shramba podatkov ontologij na verigi blokov zaradi njene varnosti in sledljivosti.

Predhodni deli, ki verigi blokov dodata novo komponento za bolj učinkovito poizvedovanje po podatkih, in se ne osredotočata na pametne pogodbe sta Naim et. al. [2] in Pei et. al. [3]. Naim et. al. [2] so zasnovali prototip semantične verige blokov (SEMBC) za upravljanje s kompleksnimi podatkovnimi modeli v obliki RDF, ki jih zaradi težav z implementacijo shranijo izven verige, ker se ne želijo ukvarjati z redefinicijo osnovnih gradnikov verige blokov. Pei et. al. [3] pa v primerjavi s predhodnimi deli, ki v večini optimizirajo zgolj ekstrakcijo podatkov iz same verige, upoštevajo možnost kombinirane shrambe. Njihov pristop upošteva korelacijo med podatki na verigi in izven nje s tem, da ji doda dodatno komponento t.i. hibridno strukturo, ki pa ne zahteva spremembe že obstoječe podatkovne baze.

Nekateri so opisali domeno verige blokov ali pametnih pogodb z ontologijo s ciljem boljšega razumevanja in poizvedovanja po samih konceptih le-te (po transakcijah, blokih) ali po več verigah. Ontologija Ethereuma (EthOn) [5] npr. opiše osnovne koncepte v omrežju Ethereum (bloke, transakcije, pogodbe) s shemo RDF in OWL. Vendar zajame le relacije med pametnimi pogodbami na omrežju Ethereum, ne zajame pa drugih omrežij. Ontologija BLONDiE [6] pa je bolj splošna in razširljiva, le-ta namreč zajema koncepte treh najbolj relevantnih tehnologij verig blokov Bitcoin, Ethereum in Hyperledger Fabric.

Drugi pa so prej omenjene ontologije še razširili z neko drugo ontologijo in tako pridobili večjo domeno za iskanje ter možnosti za nove funkcionalnosti. Baqa et. al. [4] so ontologijo EthOn razširili z ontologijo OWL-S, ki se uporablja za opis semantičnih spletnih storitev. Tako so pametnim pogodbam na omrežju Ethereum dodali nivo za odkrivanje storitev in omogočili iskanje in sklepanje po njih preko domenskih konceptov obeh ontologij npr. pridobivanje razlage zakaj je bila storitev oz. pogodba odkrita. Izpostavijo, da ni veliko raziskav na temo integracije in razvoja semantike v verigi blokov za pametne pogodbe.

Potem imamo še pristope, ki semantične tehnologije uporabijo za predstavitev poteka določenega primera uporabe (npr. poslovnega procesa), verigo blokov pa uporabijo zaradi njene odpornosti na napade in sledljivosti. Markovic et. al. [7] razvijejo pogodbe za predstavitev procesa upravljanja s hrano po sistemu HACCP. Z ontologijo FS-PROV pa predstavijo strukturo podatkov, ki jih naprave IoT pošiljajo o stanju hrane med transportom, kar se shranjuje na zasebno verigo blokov (Hyperleger Fabric). Semantične storitve nam prinašajo možnosti za sklepanje o izvoru in skladnosti transporta hrane s predpisano

zakonodajo in za opis podatkov za uporabo v drugih sistemih.

Choudhury et. al. [1] izpostavijo, da je pretvorba določenega primera uporabe v sistem pametnih pogodbo težavna in časovno potratna. Razvijejo sistem za avtomatsko grajenje pametnih pogodb za določen primer uporabe. Iz dane predstavitve znanja tako avtomatsko zgradijo pametno pogodbo, ki zagotavlja skladnost pravil z ontologijo.

Primer uporabe se lahko v določenih situacijah spremeni, v pametnih pogodbah bi v teh primerih lahko uporabili mehanizem glasovanja [8], vendar si moramo za takšne scenarije vnaprej zamisliti, ker so pametne pogodbe po objavi nespremenljive[1]. Moshin et. al. [9] delovanje verige v nepredvidljivih situacijah usmerja z uporabo prerokov (angl. oracle), ki so podprti z ontologijo in semantičnimi pravili za preverjanje veljavnosti transakcij.

3.3 Predvideni prispevki magistrske naloge

Glavna prispevka bosta:

- integracija tehnologij verige blokov in semantičnega spleta,
- način hranjena podatkov in za to uporabljenih podatkovnih struktur.

Torej implementirali bomo funkcionalnosti za hranjenje in preverjanje skladnosti semantičnih podatkov z ontologijo na osnovi tehnologije verige blokov. Kljub temu, da bomo ontologijo shranili na verigo blokov, želimo ohraniti visoko učinkovitost in fleksibilnost poizvedovanja po podatkih, ki jo semantični splet omogoča. Preučili bomo najboljše pristope za hranjenje podatkov in za to potrebne podatkovne strukture. Primerne pristope bomo realizirali in podali omejitve, ki so smiselne pri implementaciji. Uporabnost naše rešitve bomo evalvirali in izmerili njeno zmogljivost v odvisnosti od velikosti podatkov. S testiranjem nad podatkovno množico DBpedia se bo pokazala učinkovitost dodajanja, brisanja podatkov in spreminjanja sheme. Shemo in podatke bomo verzionirali, da bo omogočen vpogled v zgodovino njenih sprememb.

[1] Z določenimi izjemami, v Ethereumu lahko npr. uničimo pametno pogodbo.

3.4 Metodologija

Za namene implementacije bomo naprej naredili enostavno lastno ontologijo, ki jo bomo napolnili s testnimi podatki. Sledil bo pregled možnih pristopov souporabe verig blokov in tehnologij semantičnega spleta za učinkovito poizvedovanje in hranjenje podatkov. Pregledali bomo katera tehnologija verige blokov je najbolj primerna za hranjenje podatkov. Preučili bomo možnosti za verzioniranje ontologije in podatkov. Po preučitvi pristopov bo sledila implementacija (s testiranjem osnovne ontologije) v kateri bomo izdelali funkcionalnosti za hranjenje in zagotavljanje skladnosti podatkov s shemo. Za hranjenje podatkov bomo glede na ugotovitve uporabili več verig blokov (npr. v eni verigi izvlečki v drugi podatki) ali kombinacijo s shrambo izven njih. Evalvacija naše implementacije bo potekala tako, da bomo podatkovno zbirko DBpedia razdelili na različno velike množice in ocenili kakšne zmogljivosti dosežemo glede na njihovo velikost z uporabo že znanih metrik [10]. Na podlagi rezultatov bomo predlagali mogoče scenarije souporabe semantičnega spleta in verige blokov.

3.5 Literatura in viri

[1] O. Choudhury, N. Rudolph, I. Sylla, N. Fairoza, A. Das, Auto-Generation of Smart Contracts from Domain-Specific Ontologies and Semantic Rules, Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree (2018) 963–970.

[2] B. A. Naim, W. Klas, Knowledge Graph-Enhanced Blockchains by Integrating a Graph-Data Service-Layer, 2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019 (2019) 420–427.

[3] Q. Pei, E. Zhou, Y. Xiao, D. Zhang, D. Zhao, An Efficient Query Scheme for Hybrid Storage Blockchains Based on Merkle Semantic Trie (2020) 51–60.

[4] H. Baqa, N. B. Truong, N. Crespi, G. M. Lee, F. Le Gall, Semantic Smart Contracts for Blockchain-based Services in the Internet of Things, 2019 IEEE 18th International Symposium on Network Computing and Applications, NCA 2019 (2019) 19–23.

[5] A. Third, Domingue J., Ethon - an ethereum ontology, dosegljivo: `https://ethon.consensys.net/`, dostopano: 3. 12. 2020 (2020).

[6] H. E. Ugarte-Rojas, B. Chullo-Llave, BLONDiE: Blockchain Ontology with Dynamic Extensibility, arXiv (2020).

[7] M. Markovic, P. Edwards, N. Jacobs, Recording Provenance of Food Delivery Using IoT, Semantics and Business Blockchain Networks, 2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019 (2019) 116–118.

[8] S. Liu, F. Mohsin, L. Xia, O. Seneviratne, Strengthening smart contracts to handle unexpected situations, Proceedings - 2019 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPCON 2019 (2019) 182–187.

[9] F. Mohsin, X. Zhao, Z. Hong, G. de Mel, L. Xia, O. Seneviratne, Ontology aided smart contract execution for unexpected situations, CEUR Workshop Proceedings 2599 (2019) 1–7.

[10] M. Morsey, J. Lehmann, S. Auer, A. C. Ngonga Ngomo, DBpedia SPARQL benchmark - Performance assessment with real queries on real data, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 7031 LNCS (PART 1) (2011) 454–469.