ŠOLSKI CENTER VELENJE
ELEKTRO IN RAČUNALNIŠKA ŠOLA VELENJE
Trg mladosti 3, 3320 Velenje

MLADI RAZISKOVALCI ZA RAZVOJ ŠALEŠKE DOLINE

RAZISKOVALNA NALOGA

KAJ JE BLOCKCHAIN?

Tematsko področje: RAČUNALNIŠTVO

Avtor:
Domen Ramšak, 4. letnik

Mentor:
Simon Konečnik, univ. dipl. inž.

Somentor:
Islam Mušić, prof.

Velenje, 2018

Raziskovalna naloga je bila opravljena na Šolskem centru Velenje, Elektro in računalniški šoli.

Mentor: Simon Konečnik, univ. dipl. inž.
Somentor: Islam Mušić, prof.

Datum predstavitve: marec, 2018

KLJUČNA INFORMACIJSKA DOKUMENTACIJA

ŠD Elektro in računalniška šola Velenje, šolsko leto 2017/2018

KG Blockchain / Kriptovalute / Bitcoin / Kriptografija

AV RAMŠAK, Domen

SA KONEČNIK, Simon / MUŠIĆ, Islam

KZ 3320 Velenje, SLO, Trg mladosti 3

ZA ŠC Velenje, Elektro in računalniška šola, 2018

LI 2017/2018

IN KAJ JE BLOCKCHAIN?

TD Raziskovalna naloga

OP VIII/ 36 str./ 3 graf./ 23 sl./ 60 vir.

IJ SL

JI sl/en

AI Kriptovalute kot bitcoin so v zadnjih petih letih dosegle izjemno širitev popularnosti in uporabnosti. Izobražujem se v programu Tehnik računalništva in skozi delo pri strokovnih modulih sem dobil idejo, da raziščem, kako kriptovalute delujejo, kako se je vse skupaj začelo in kaj je blockchain tehnologija. Tehnologije, ki se uporabljajo v kriptologiji, sem podrobno proučil, prav tako naprednejše funkcije, ki jih uporabljajo skoraj vse blockchain tehnologije. Raziskovanje zmožnosti tehnologije blockchain je potekalo v smeri uporabe v današnjih sistemih. Predstavil sem nekaj obstoječih tehnologij, ki uporabljajo blockchain za svoje delovanje. Rezultat moje raziskovalne naloge je izdelana aplikacija, s katero sem preizkusil svoje srednješolsko znanje v programiranju na tem področju. Izdelana aplikacija uporablja za delovanje tehnologijo blockchain. Pri tem sem želel raziskati njene zmožnosti in pomanjkljivosti ter navezati pridobljeno znanje na aplikacije, ki ne uporabljajo blockchain tehnologij.

KEY WORDS DOCUMENTATION

ND Elektro in računalniška šola Velenje, 2017/2018

CX Blockchain / Cryptocurrency / Bitcoin / Cryptography

AU RAMŠAK, Domen

AA KONEČNIK, Simon / MUŠIĆ, Islam

PP 3320 Velenje, SLO, Trg mladosti 3

PB ŠC Velenje, Elektro in računalniška šola, 2018

PY 2017/2018

TI WHAT IS BLOCKCHAIN?

DT RESEARCH WORK

NO VIII/ 36 p./ 3 graf./ 23 pic./ 60 ref.

LA SL

AL sl/en

AB Cryptocurrencies, such as bitcoin, have seen an exceptional growth of popularity and usability in the last five years. Since I am studying to become a computer technician and thus work in professional modules, I got the idea and motivation to research how cryptocurrencies work, how it all began and what blockchain technology is. I studied the technologies that are in use in cryptology, as well as more advanced functions that are being used by almost all blockchain technologies. Researching capabilities of blockchain technology proceeded in the direction of use in today's systems. I presented a few existing technologies that use blockchain for their operation. The result of my research paper is a built application, with which I tested my high-school-level knowledge in programming in that area. The built application uses blockchain for its operation, thus enabling me to research its capabilities and shortcomings, as well as attach my gained knowledge to applications that do not use blockchain technology.

KAZALO VSEBINE

KAZALO SLIK

KAZALO GRAFOV

UPORABLJENE KRATICE

angl. - angleško
DApp - angl. Decentralized Application
ETH - Ethereum
EVM - Ethereum Virtual Machine
GB - gigabajt
ICO - initial coin offering
itd. - in tako dalje
JS - JavaScript
JSON - angl. JavaScript Object Notation
MB - megabajt
oz. - oziroma
P2P - angl. Peer-To-Peer
PHP – angl. PHP Hypertext Preprocessor
prof. - profesor
slo. - slovensko
t. i. - tako imenovani
UTXO - angl. Unspent Transaction Output
ZDA - Združene države Amerike

1 UVOD

Trend sodobnega časa prinaša spremembe na širšem področju informacijskih tehnologij, ki svoj razvoj širijo tudi na področje ekonomije, kamor spada denar in pogodbeni odnosi.

Pred desetimi leti je neznana oseba z vzdevkom Satoshi Nakamoto izdala dokument, v katerem je bil prvič opisan koncept za kriptovaluto. Takrat je malokdo verjel, da bo ta ideja uspela, mnogi so koncept blockchaina ignorirali. Danes vemo, da blockchain spreminja svet in da je Satoshijevo odkritje nekaj izjemnega.

Kriptovalute omogočajo varno plačevanje po celem svetu in dosegajo astronomske vrednosti. Decentralizirane aplikacije in pametne pogodbe pomagajo z varovanjem in verodostojnostjo pomembnih dokumentov, nekatere države eksperimentirajo z volilnimi sistemi, ki so izdelani na blockchainu …

Aplikacije za to tehnologijo so izjemne. Mnogi to tehnologijo nazivajo kot »novi internet«, ki bo v prihodnosti lahko prisoten na vseh področjih: finance, nepremičninski trg, javni sektor, medicina … Ta raziskovalna naloga predstavlja moj prvi skok na to področje, kjer upam, da bom našel veliko razlogov, da še naprej razvijam svoje znanje. Priložnosti vsekakor ne mislim izpustiti.

1.1 HIPOTEZE

Pred začetkom raziskovanja sem si postavil štiri hipoteze:

1. Kriptovalute niso edini izdelki, ki uporabljajo blockchain tehnologijo.
2. Obstaja vsaj 3 vrste sistemov oz. tehnologij, ki brez blockchaina ne bi bili mogoči.
3. Za izdelavo aplikacij, ki temeljijo na blockchain tehnologiji, so razvita vsaj 3 orodja.
4. Lahko izdelam lastno aplikacijo, ki temelji na blockchain tehnologiji in omogoča nesporno shranjevanje dogovorov v obliki pametne pogodbe.

2 PREGLED OBJAV

2.1 ZGODOVINA BLOCKCHAINA

2.1.1 Prvi pojav principa v kriptologiji

Že od začetka kriptologije je vedno obstajala želja po sistemu, ki bi omogočal varno označevanje datotek z bodisi časovnim žigom ali posebno identifikacijsko številko. Namen tega je bilo preprečevanje prevar in ugotavljanje zgodovine sprememb na dokumentih.

Predvsem v akademskih krogih bi takšna tehnologija omogočala avtorjem znanstvenih dokumentov zavarovanje pred morebitnimi obtožbami o plagiatorstvu del. Seveda bi takšna tehnologija imela še veliko različnih uporab tudi v bolj preprosti obliki. Bistvo ideje je bilo: kako lahko potrdimo, da je nek izdelek res prišel od tam, kjer nekdo trdi, da je in kako vemo, če je bil spremenjen in kdaj?

Leta 1991 sta Stuart Haber in W. Scott Stornetta napisala raziskovalni članek v »Journal of Cryptology« z imenom »How to time-stamp a digital document« (v slovenščini »Kako označiti digitalni dokument s časovnim žigom«), v katerem sta opisala idejo za kriptografsko verigo blokov. Ta bi omogočal varno in pregledno overjanje sprememb digitalnega dokumenta in avtorja le-tega z uporabo časovnih žigov na sami datoteki.

Naslednje leto sta s sodelavcem Dave Bayerjem koncept nadgradila z uporabo t. i. »Merkeljevega drevesa«. Posledično izboljšan sistem so opisali v članku »Improving the Efficiency and Reliability of Digital Time-Stamping« (v slovenščini Izboljševanje učinkovitosti in zanesljivosti digitalnega časovnega žigosanja), kjer so dodali, da to omogoča zbiranje več dokumentov v en dokument – t. i. blok. [1] [2]

2.1.2 Blockchain in bitcoin

Leta 2008 je neznana oseba (ali skupina) pod vzdevkom Satoshi Nakamoto izdala dokument, imenovan »Bitcoin: A Peer-to-Peer Electronic Cash System«, v katerem je opisala koncept delovanja za kriptovaluto (bitcoin) in kako rešiti problem dvojnega porabljanja, kar prej ni uspelo še nobeni kriptovaluti. V dokumentu sicer beseda »blockchain« ni bila uporabljena, ampak sta bili besedi »block« in »chain« uporabljeni ločeno za opis delovanja dnevnika transakcij, ki ga uporablja bitcoin. [3]

2.1.3 Razvoj blockchaina

Prvi blockchain je bil namenjen predvsem overjanju transakcij med uporabniki bitcoina, a je narava koncepta hitro dokazala, da je zmožen veliko več. Ta prvotni koncept se imenuje »blockchain 1.0«, saj je bil razvit za kriptovalute, njegove zmožnosti so bile zaradi tega nekoliko omejene. Njihov namen je bil predvsem zasnova kriptovalutnih sistemov, ki bi se uporabljali za plačevanje s pomočjo digitalnega denarja.

Leta 2014 so se začeli pojavljati t. i. »blockchain 2.0«, katerih namen je bil ustvarjanje aplikacij in podatkovnih baz s pomočjo pametnih pogodb (angl. »smart contracts«). Njihova vključitev je razširila uporabnost blockchaina ter omogočila razvoj mnogih idej in aplikacij, ki so izjemno varne in verodostojne. Takšen blockchain se lahko uporablja kot valuta, vendar je njegova največja prednost v tem, da služi kot platforma za razvijanje decentraliziranih aplikacij in tudi novih blockchain sistemov po vrhu že obstoječih.

Tretja stopnja razvoja, ki se trenutno dogaja, je »blockchain 3.0«. Nanaša se predvsem na tehnologije, ki uporabljajo blockchain za izdelavo oz. prenovo sistemov v finančnem, javnem in vladnem sektorju v različnih državah po celem svetu. [1] [4]

2.2 KAJ JE BLOCKCHAIN?

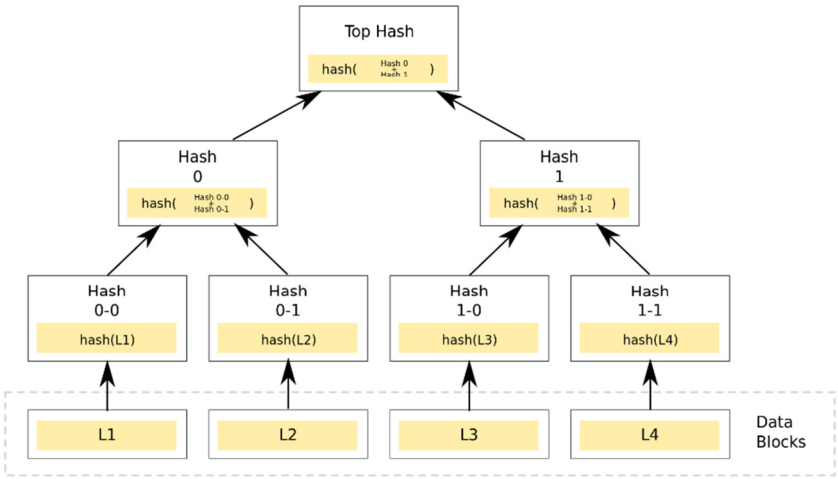
Blockchain je princip oz. koncept za sistem, katerega namen je varno in verodostojno shranjevanje podatkov. Ni točno določen načrt, ampak osnovni koncept za izdelavo decentraliziranega »peer-to-peer« sistema, ki razporedi moč nad nekim sistemom med njegove uporabnike ter poskrbi, da je zloraba moči (kot je to možno v centraliziranem sistemu) praktično nemogoča.

Razne tehnologije, ki so osnovane oz. temeljijo na tem principu, rešujejo tehnične težave in pomanjkljivosti na različne načine, zato lahko izraz blockchain zajema tudi izdelke, ki ne vsebujejo nekaterih delov, ki jih imajo druge tehnologije. [1]

2.2.1 Osnovni pojmi kriptologije

Blockchain tehnologija je osnovana na principu kriptologije, zato je za zadostno razumevanje potrebno razložiti nekatere kriptografske koncepte.

- Enkripcija in dekripcija – enkripcija je postopek kodiranja podatkov, kjer berljive podatke spremenimo (s pomočjo nekega algoritma in ključa) v neberljive. Dekripcija je obratni postopek, kjer s pomočjo podanih podatkov (ključa) poskušamo spremeniti besedilo nazaj v berljive podatke. [5]
- Hash funkcija **–** je funkcija, s pomočjo katere lahko iz variabilno velikega kosa podatkov pridobimo podatek fiksne velikosti. Funkcija uporabi razne algoritme, da iz nekega uporabnega podatka (npr. e-poštnega sporočila, dokumenta, slike itd.) pridobi t. i. podpis datoteke, iz katerega je praktično nemogoče pridobiti nazaj prvoten dokument, saj v procesu funkcija »odreže« dele, da lahko končen podatek zapolni določeno velikost. Tako imenovani hash ali zgoščena vrednost je za enak dokument vedno isti, s čimer omogoča preverjanje verodostojnosti. [6]
- Merkle tree (drevo) ali hash tree je skupina blokov, ki so med seboj povezani v obliki drevesa s pomočjo zakodiranih zgoščenih vrednosti blokov pod seboj. Najpomembnejša lastnost takšne razporeditve je ta, da je praktično nemogoče spremeniti blok na nižji stopnji ter s tem spremeniti tudi vse bloke nad njim in tako razveljaviti celotno strukturo oz. drevo. [6]



Slika 1: Merklovo drevo, vir: [7]

- Asimetrična enkripcija uporablja dva ključa: javnega in zasebnega. Javni ključ je prosto dostopen; uporabi ga lahko vsakdo, vendar lahko z njim podatke le enkriptiramo. Za dekriptiranje podatkov pa moramo uporabiti zasebni ključ, ki ga ima po navadi v lasti le lastnik. V ta namen sta oba ključa generirana skupaj. [5]

2.2.2 Sestava blockchaina

Blockchain je sestavljen iz različnih blokov podatkov, navezanih v digitalno verigo, zato ga je tako tudi najlažje upodobiti. Osnove blockchaina lahko razdelimo na štiri koncepte: blok, veriga, vozlišča ter rudarjenje. [1] [27]

2.2.3 Blok

Vsebino posameznega bloka lahko običajno razdelimo na štiri dele:

- naslov ali arbitrarna številka (nonce) je naključno zaporedje številk oz. karakterjev, ki se nikoli ne ponovijo. Nonce se uporablja za hitrejše brskanje po blockchainu in je kritičen element procesa rudarjenja;
- podatki – namen blockchaina je shranjevanje podatkov, le-te pa shranjujemo v posameznih blokih. Kot podatek lahko vstavimo kakršnokoli informacijo, vendar je najpogostejša uporaba blockchaina kot digitalnega dnevnika za beleženje transakcij, zatorej so te tudi najpogostejši podatek, ki ga vpišemo v blok;
- podpis (hash) predhodnika – za preprečitev retroaktivnega spreminjana blockchaina

vsak blok vsebuje hash ali podpis predhodnega bloka in ga potem vključi v svoj lasten hash;

- podpis (hash) **–** vse dele blok s pomočjo hash funkcije zgosti in spremeni v hash, s pomočjo katerega lahko overjamo bloke ter jih tudi poiščemo v sklopu blockchaina;
- časovni žig – za pravilno ugotavljanje časovnega zaporedja je vsak blok opremljen s časovnim žigom, po navadi ko je vpisan v blockchain.[8] [9] [27]

2.2.4 Veriga

Posamezni bloki so skupaj povezani s pomočjo prej omenjenih hashev. Vsak naslednji blok v hash vključi vse podatke v bloku, identifikacijsko številko ter hash njegovega predhodnika.
Prvi blok v verigi se imenuje »genezi« (angl. »genesis«) ali izvirni blok in je vedno vgrajen v blockchain. Kot prvi blok v verigi nima hasha predhodnika, saj ta ne obstaja. Po navadi takšen blok vsebuje tudi prve transakcije. [1]
Takšen sistem deluje na podobnem principu kot Merklevo drevo. V primeru, da bi nekdo spremenil podatke v enem bloku, bi ta blok postal neveljaven, saj je bila uničena njegova verodostojnost - kredibilnost. Če se razveljavi en blok, se razveljavijo tudi vsi njegovi nasledniki, s čimer se posledično razveljavi celoten del blockchaina od prvega razveljavljenega bloka naprej.
V kolikor hočemo, da blok spet postane veljaven, mu moramo spremeniti identifikacijsko številko oz. nonce, tako da bo hash blok izpolnjeval določene pogoje (npr. vrednost prvih petih karakterjev hasha se mora ujemati s prvotnim hashom tega bloka). Takšnemu procesu pravimo rudarjenje. [1] [8] [9]

Slika 2: Poenostavljen prikaz verige blokov, vir: [10]

2.2.5 Node – vozlišče

V primeru, da bi nekdo hotel spremeniti blockchain, mora ponovno overiti vsak blok, kar pa

ni težava, če ima ta oseba za sabo veliko računalniško moč.

Ta problem je rešen tako, da blockchain razdelimo med vse uporabnike, ki za dostop do njega morajo na svojo napravo namestiti t. i. node oz. vozlišče. S tem mora vsakdo, ki hoče blockchain spremeniti, postati eden od uporabnikov le-tega.

To je pomembno, ker se blockhain overja demokratično – v kolikor vsa vozlišča potrdijo trenutno stanje blockchaina (sploh pri več tisočih uporabnikih), ga je praktično nemogoče spreminjati, saj bi spremenjen blockchain omrežje zavrnilo.

Tu lahko ločimo vozlišča na dve vrsti:

- »Polno« vozlišče (angl. full node), ki prenese celoten blockchain, kar lahko pri večjih blockchainih znaša tudi več 100 GB. Samo polna vozlišča lahko overjajo blockhain.
- »Lahko« vozlišče (angl. light node) lahko prenese samo določen (zadnji) del blockchaina, kar zmanjša velikost potrebnega prenosa na nekaj GB, a takšno vozlišče ne more overjati blockchaina. [11]

2.2.6 Rudarjenje

Zaradi decentralizirane oblike blockchaina bi bilo zelo težko dodajati nove transakcije v bloke in te na blockchain, ker bi to ustvarjalo konflikt, saj bi vsako posamezno vozlišče prejelo transakcije in bloke ob različnih časovnih terminih. Brez načina, da bi lahko te bloke dodajal na blockchain po nekem redu ter jih s pomočjo vozlišč overjal, bi celoten sistem razpadel.

Tu nastopi proces rudarjenja. Posamezne tehnologije (bitcoin, ethereum itd.) imajo svoje rešitve, vendar je princip podoben.

Da je blok lahko sprejet na blockchain, mora ustrezati nekaterim pogojem (pri bitcoinu je ta pogoj, da se mora hash bloka začeti z določenim številom ničel). Običajno je za izpolnjevanje tega pogoja potrebna velika in konstantna računalniška moč. Temu procesu pravimo overjanje.

Ko blok končno izpolni pogoje, se v blok vtisne t. i. dokaz dela, ki potrdi, da je za overjanje tega bloka bila izpolnjena zahteva po računalniški moči, času in energiji. Tiste naprave (rudarji), ki so prve overile podane transakcije v bloku, pridobijo del novonastale kriptovalute kot nagrado.

Brez takšnega sistema bi bilo veliko lažje transakcije ponarediti in celo izvesti dve različni transakciji, ki bi uporabljale isto surovino (kriptovaluto). [12] [13]

2.2.7 Pametne pogodbe

Decentralizirana narava blockchain tehnologije ponuja edinstveno priložnost za izdelavo sistemov, ki so odporni proti goljufiji in zlorabi moči. S tem namenom so nekateri blockchain sistemi (imenovani »blockchain 2.0«) ustvarili t. i. pametne pogodbe (angl. smart contracts).

Za vsako transakcijo v resničnem življenju po navadi določimo pravila, ki jih morata obe strani pri transakciji upoštevati, ki so zapisana v pogodbi. Kupec npr. mora prodajalcu dati neko količino denarja, prodajalec pa mu v zameno mora dati izdelek, hkrati pa potrdilo o transakciji – račun.

Pri kriptovalutah je takšna transakcija težja, saj nekega izdelka oz. storitve ne moremo videti, narava digitalnih valut pa otežuje sledenje denarju in potrditvi, da sta obe strani res upoštevali pravila.

Tu vstopijo pametne pogodbe, ki so programi, shranjeni na blockchainu, ki se izvedejo, ko so pogoji, določeni v pogodbi, izpolnjeni. Če ti pogoji niso izpolnjeni do določenega časa (ali drugega merila), lahko pogodba avtomatično izvede vračilo denarja.

Primer: recimo, da plačujete naročnino na digitalno revijo z neko kriptovaluto. Vsak mesec bo pogodba naročnino zadržala do takrat, ko revija prispe. V kolikor revija ne bi bila izdana, bi pametna pogodba vrnila denar. [14]

```
pragma solidity ^0.4.16;

interface tokenRecipient { function receiveApproval(address _from, uint256 _value, address _token, bytes _extraData) publi

contract TokenERC20 {
    // Public variables of the token
    string public name;
    string public symbol;
    uint8 public decimals = 18;
    // 18 decimals is the strongly suggested default, avoid changing it
    uint256 public totalSupply;

    // This creates an array with all balances
    mapping (address => uint256) public balanceOf;
    mapping (address => mapping (address => uint256)) public allowance;

    // This generates a public event on the blockchain that will notify clients
    event Transfer(address indexed from, address indexed to, uint256 value);

    // This notifies clients about the amount burnt
    event Burn(address indexed from, uint256 value);

    /**
     * Constrctor function
     *
     * Initializes contract with initial supply tokens to the creator of the contract
     */
    function TokenERC20(
        uint256 initialSupply,
        string tokenName,
        string tokenSymbol
    ) public {
        totalSupply = initialSupply * 10 ** uint256(decimals);  // Update total supply with the decimal amount
        balanceOf[msg.sender] = totalSupply;                // Give the creator all initial tokens
        name = tokenName;                                   // Set the name for display purposes
        symbol = tokenSymbol;                               // Set the symbol for display purposes
    }
```

Slika 3: Primer (dela) pametne pogodbe na ethereum blockchainu, vir: [15]

2.2.8 Token ali žeton

Ker so aplikacije blockchain tehnologije več kot samo kriptovalute, pri nekaterih sistemih ugotovimo, da izraz »denar« ali pa »valuta« ni najbolj primeren za opis sredstva, ki predstavlja vrednost v našem sistemu. S pomočjo pametnih pogodb lahko po vrhu obstoječega blockchaina naredimo t. i. žetone (angl. tokens). Te lahko uporabimo kot točke zvestobe, predmete ali celo popolnoma nove kriptovalute.

Za izdelavo žetona ni potrebno narediti popolnoma novega blockchaina, zato so žetoni idealni za izdelavo decentraliziranih aplikacij. Lahko so uporabni tudi za izvedbo ICO (angl. Initial Coin Offering), oz. prvotno ponudbo kovancev, kjer lahko žeton svojega blockchaina ponudimo voljnim kupcem kot način financiranja razvijanja ideje (donacije). [15] [16] [17]

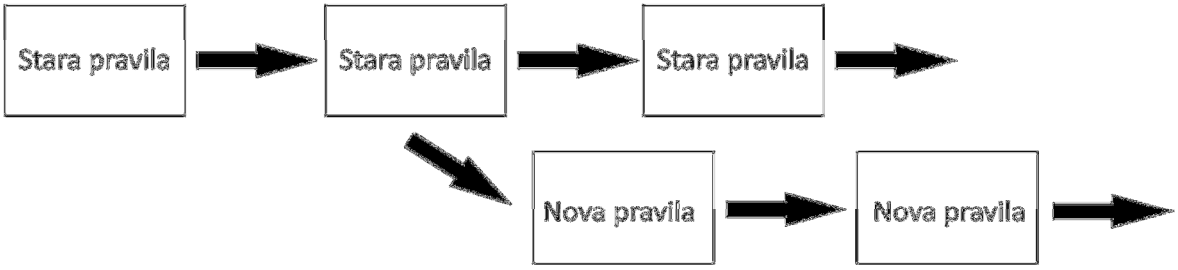
2.2.9 Razcepitve ali »forks«

Ker narava blockchaina ne podpira spreminjanja pravil, moramo blockchain zaustaviti in ga ponovno izvesti vsakič, ko ga hočemo korenito spremeniti. To bi popolnoma porazilo namen tehnologije, zaradi česar se za uveljavljanje novih pravil na blockchainu izvede t. i. razcepitev (angl. fork). Ta razdeli blockchain na dva dela, ki imata različna pravila. Takšna razdelitev je lahko začasna ali stalna.

Obstajata dve vrsti razcepitev:

- mehka razcepitev (angl. soft fork) se navezuje na razcepitve, ki bi jih kljub spremembam pravil stari blockchain še vedno prepoznal kot pravilne;
- trda razcepitev (angl. hard fork) ustvari dve različici blockchaina, katerih pravila so popolnoma nezdružljiva drug z drugim in morata zatorej delovati (ločeno) drug od drugega. [34]

Eden največjih primerov razcepitve (in verjetno tudi najbolj spornih) je bitcoin cash, ki so ga razvijalci odcepili od bitcoin blockchaina. [35]



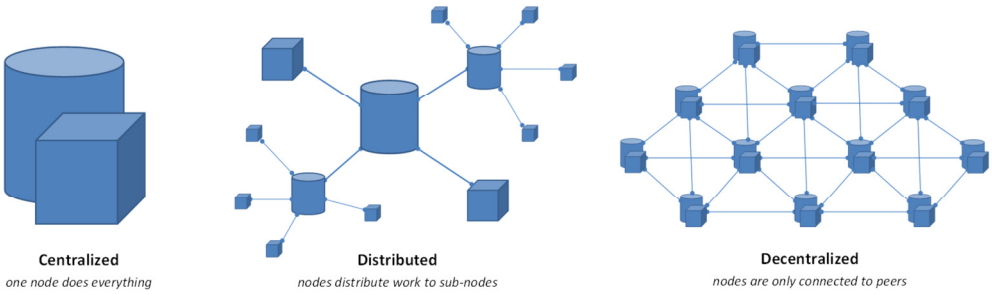
Slika 4: Poenostavljen prikaz razcepitve, vir: lasten

2.3 PREDNOSTI PRED TRADICIONALNIMI SISTEMI

Blockchain zaradi svoje zgradbe omogoča izdelavo varnejših sistemov (kot je to bilo možno prej). Njegova največja prednost je odsotnost centralnega strežnika ali skupine, ki bi lahko s takšnim sistemom nepravilno (ali nemoralno) upravljala. [1]

2.3.1 Decentralizacija

Ena izmed najpomembnejših lastnosti blockchain tehnologije je, da podatki (o transakcijah, uporabnikih, programih, itd.) niso shranjeni na enem mestu. V nasprotju s tipičnim omrežjem strežnik - uporabnik, kjer so vsi podatki shranjeni v podatkovnih bazah na strežniku, blockchain svoje podatke shrani na računalniku oz. napravi uporabnika. Uporabnik mora za dostop do blockchaina namestiti na svojo napravo vozlišče, ki je kopija celotnega blockchaina. Takšen sistem zavaruje blockchain pred zlorabo pozicije ali vdori v eno samo točko ter daje moč uporabnikom. [1] [18] [24]



Slika 5: Vrste razdeljenih sistemov, vir: [19]

Kot je razvidno na sliki 5, je decentraliziran sistem praktično brez kakršnihkoli osrednjih točk, ki bi pri omrežjih ustvarjale varnostne slabosti. Ideja razdeljenega računalniškega omrežja ni nova, saj so podobne rešitve za računalniške strukture razvijali že v 60. letih prejšnjega

stoletja [20]. Seveda takšna ureditev ni popolnoma brez napak ali slabosti, vendar je za namen kriptovalut idealna.

Čeprav so blockchain sistemi razdeljeni fizično (deluje na več napravah, katere niso na isti lokaciji) in politično (ne nadzoruje jih ena sama oseba ali skupina), so centralizirani logično, ker posamezni deli delujejo kot ena celota. [21] [24]

2.3.2 Zaupanje in preglednost

Pri vseh večjih omrežjih hitro nastane problem zaupanja. Kako lahko vemo, da nas oseba, s katero komuniciramo ali poslujemo, noče prevarati? Pri blockchain tehnologiji to ni težava, saj podatki na mreži niso skriti, kar omogoča preglednost sprememb. Podatki so enkriptirani, vendar podpisovanje teh na blockchainu pomeni, da lahko vsakdo pogleda spremembe.

Blockchain omrežja so P2P, kar pomeni, da so vsi uporabniki med sabo povezani. Preko vozlišč, ki jih mora posamezna naprava za povezavo do blockchaina imeti nastavljena, so kopije tega shranjene na več tisoč (ali celo milijonih) mestih. Posamezne naprave overjajo blockchain, s čimer nastane omrežje, ki ga je izjemno težko ogoljufati. Posledica takšnega sistema je nespremenljivost podatkov, ki jih oddamo v blockchain. To pomeni, da lahko v blockchainu shranjujemo pomembne podatke, ki ne smejo biti spremenjeni, saj bi to uničilo njihovo kredibilnost. Pri klasičnih sistemih bi bilo takšne spremembe težko preprečiti, saj bi vsakdo, ki bi imel dostop do omrežja (zakonito ali nezakonito), lahko spremenil podatke. Pri blockchain tehnologiji pa oddane podatke overja celotno omrežje, s čimer zagotavljajo varnost podatkov. Če bi ti bili spremenjeni, bi omrežje, ki ima prave podatke, tisti blockchain označilo za neveljavnega, ter ga izločilo iz omrežja. [1] [3] [27]

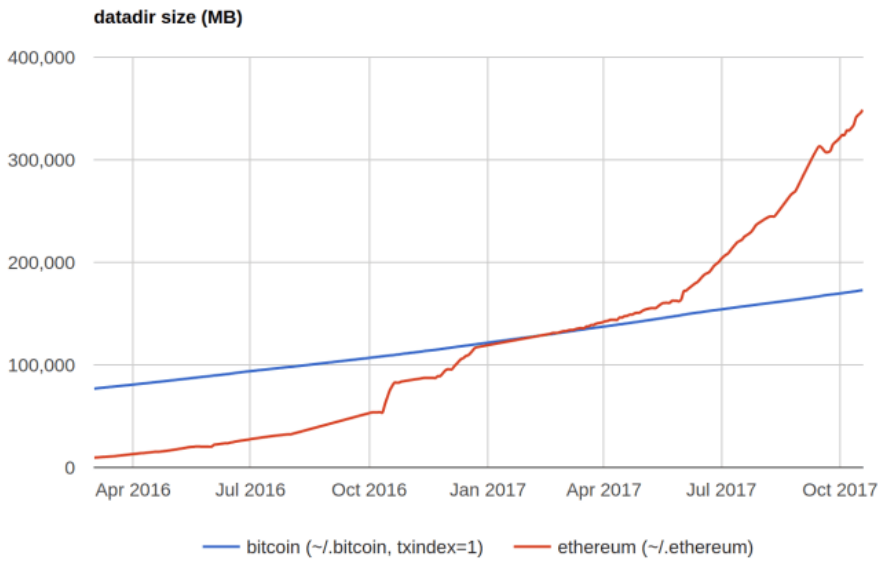
2.4 SLABOSTI BLOCKCHAINA

Kot vsak sistem in tehnologija tudi blockchain ni brez napak in slabosti.

2.4.1 Velikost sistema

Blockchain svojo varnost in zaupanje pridobi iz decentralizirane strukture vozlišč, ki ga mora vsak uporabnik namestiti na svojo napravo, da lahko dostopa do blockchaina. S tem procesom mora vsako vozlišče tudi prenesti na napravo celoten blockchain.

To načeloma ni problem pri manjših, bolj preprostih sistemih, postane pa težava pri večjih in bolj kompleksnih blockchainih, kot npr. ethereum.



Graf 1: Velikost ethereum in bitcoin omrežja, vir: [23]

Kot je razvidno iz grafa, se je velikost ethereum blockchaina v času od aprila 2016 do oktobra 2017 povečala za skoraj 40-krat, (iz prib. 9 GB na prib. 350 GB), in se še vedno veča.

Na ethereum blockchainu danes za ta problem že obstaja delna rešitev - imenuje se obrezovanje, vendar težave ne reši popolnoma. Za vsako vozlišče lahko izberemo eno izmed mnogih (vse bolj agresivnih) oblik obrezovanja, ki na napravo prenesejo blockchain samo za nekaj časa nazaj, kar zmanjša velikost.

Takšno »lahko vozlišče« (angl. light node) sicer omogoča uporabniku dostop do blockchaina, vendar ga ne more uporabljati za overjanje blockchaina, ker ne pozna celotnega blockchaina. Zaradi tega lahka vozlišča ne sledijo pravilom blockchaina v celoti in tako izpostavijo celoten sistem napadu, pri katerem bi lahko skupina rudarjev »odcepila« lahka vozlišča od polnih vozlišč in nad njimi prevzela kontrolo. [22] [27]

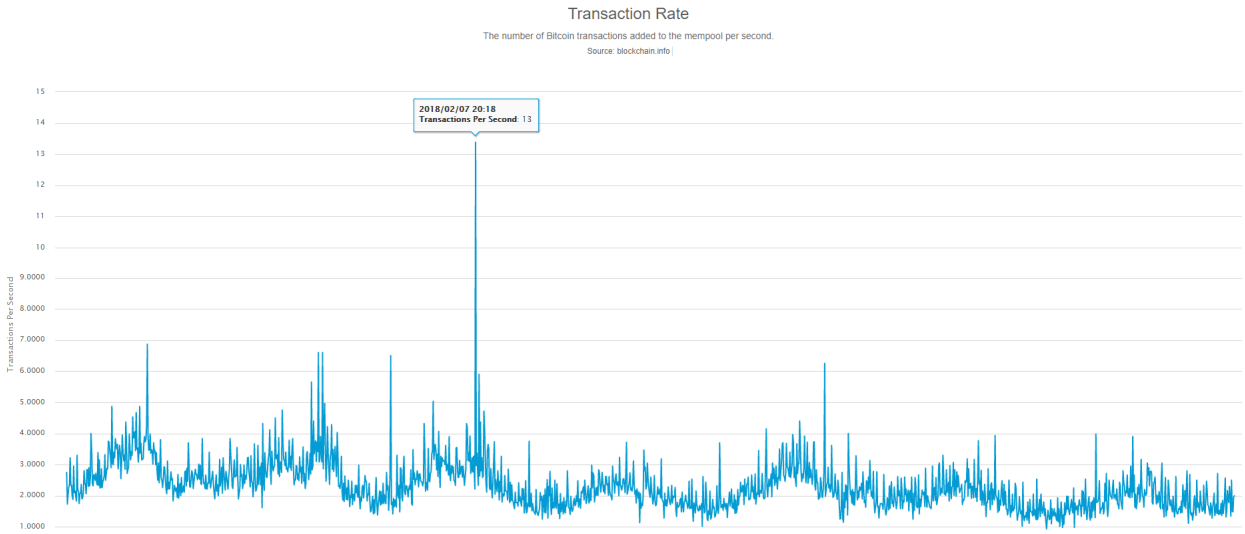
2.4.2 Hitrost in učinkovitost delovanja

Ker se mora vsaka transakcija vpisati v določen blok in ta v celoten blockchain, se lahko čas transakcije zavleče. To je pomembno, če upoštevamo še dodatno čakanje zaradi varnosti (možna je vrnitev na prejšnjo različico blockchaina v primeru napake v sistemu).

Zaradi tega je plačevanje s kriptovaluto lahko izjemno dolgo in težavno, posledica tega pa so lahko tudi neprimerno velike pristojbine zaradi količine rudarjev in dela, vloženega v vsak posamezen blok.

Razlog za takšne upočasnitve in neučinkovitost delovanja leži večinoma v zasnovi vsakega posameznega sistema. Najboljši primer za takšne težave je bitcoin. Zaradi omejene velikosti blokov (1 MB) lahko obdela samo do 7 transakcij na sekundo, pristojbine pa ga zaradi svojih velikosti naredijo neuporabnega oz. neekonomičnega za manjše transakcije (več kot 25 $ na transakcijo, če hočemo, da je ta izvedena v manj kot parih urah).

Drugi sistemi so te pomanjkljivosti zmanjšali oz. skoraj izničili s pozornim načrtovanjem (npr. ethereum) ali s spremembo svojih pravil (npr. bitcoin bash). [25] [27] [29]



Slika 6: Transakcije na sekundo na bitcoin omrežju, vir: [44]

2.4.3 Vir računalniške moči

Za overjanje posameznih blokov blockchain potrebuje moč uporabnikov – rudarjev. Ti omogočajo, da je blockchain res verodostojen in da so vsi bloki v verigi overjeni. Tu pa nastopi tudi največja težava blockchaina.

V primeru, da bi nekdo (skupina, država itd.) lahko nadzoroval 51 % vse rudarske moči, bi lahko spreminjal blockchain skoraj brez upiranja ostalih rudarjev ter tako nadzoroval celoten sistem. Seveda bi takšne dejavnosti na večji ravni pritegnile pozornost skupnosti okoli blockchaina, nakar bi sicer bilo možno izvesti vrnitev na prejšnje stanje, a bi tudi to lahko skupina rudarjev otežila. [26] [27]

2.5 TEHNOLOGIJE, OSNOVANE NA BLOCKCHAINU

2.5.1 Kriptovalute

Brez blockchaina, ki ureja dnevnik transakcij in preprečuje »dvojno porabljanje«, bi kriptovalute za delovanje potrebovale nek centralni server ali organizacijo, ki bi preverjala omrežje proti takšnemu pojavu. Takšna zgradba bi bila popolnoma nesmiselna, saj ne bi bila valuta nič drugačna od tradicionalnih. [1] [3]

2.5.1.1 Bitcoin

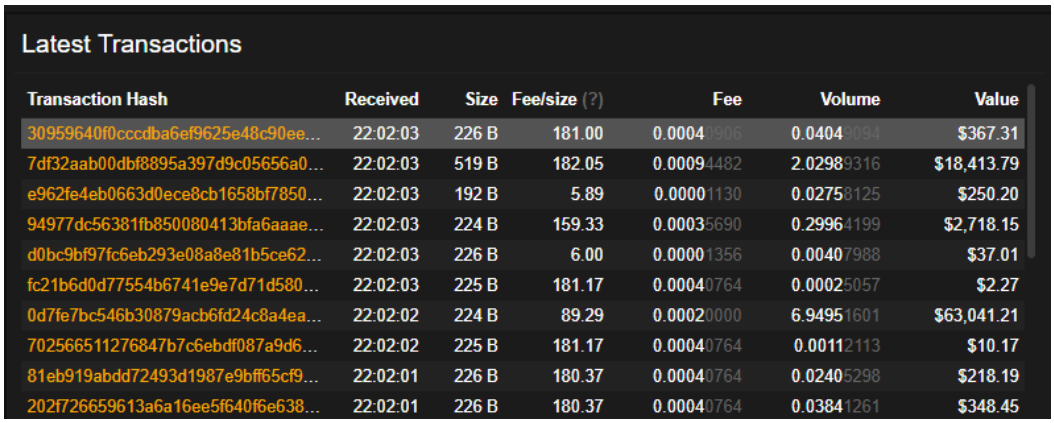
Bitcoin je ustvaril Satoshi Nakamoto leta 2008. Njegovo zgradbo in delovanje je konceptualiziral istega leta v dokumentu »Bitcoin: A Peer-to-Peer Electronic Cash System«, kjer je opisal tudi uporabo blockchain tehnologije za vodenje dnevnika transakcij za bitcoin.

Je prva decentralizirana kriptovaluta, ki deluje brez centralne banke ali enega samega upravljalca. Omrežje bitcoin je peer-to-peer (decentralizirano), kar pomeni, da namesto osrednjega strežnika (banke itd.) uporablja blockchain, da potrdi veljavnost svojih kovancev. [3] [29]

Kot prva (delujoča) kriptovaluta je danes bitcoin verjetno najpopularnejši digitalni denar, čeprav ima zaradi svoje začetne zasnove nekaj težav. Velikost posameznih blokov je omejena na 1 MB, zaradi česar lahko omrežje predela v povprečju od 3 do 7 transakcij na sekundo, kar je izjemno malo, sploh če ga primerjamo z večjimi valutnimi omrežji, kot npr. VISA, ki predela okoli 2000 transakcij na sekundo z vrhi do 56000 transakcij na sekundo. [25] [30]

Slika 7: Logotip bitcoina, vir: [33]

Ena od rešitev za ta problem je različica bitcoin blockchaina, imenovana bitcoin cash, ki to težavo nekoliko omili tako, da poveča velikost blokov na 8 MB, kar teoretično omogoča do 61 transakcij na sekundo. [35] [36]



Latest Transactions

Transaction Hash	Received	Size	Fee/size (?)	Fee	Volume	Value
30959640f0cccdba6ef9625e48c90ee...	22:02:03	226 B	181.00	0.0004 0906	0.0404 9094	$367.31
7df32aab00dbf8895a397d9c05656a0...	22:02:03	519 B	182.05	0.0009 4482	2.0298 9316	$18,413.79
e962fe4eb0663d0ece8cb1658bf7850...	22:02:03	192 B	5.89	0.0000 1130	0.0275 8125	$250.20
94977dc56381fb850080413bfa6aaae...	22:02:03	224 B	159.33	0.0003 5690	0.2996 4199	$2,718.15
d0bc9bf97fc6eb293e08a8e81b5ce62...	22:02:03	226 B	6.00	0.0000 1356	0.0040 7988	$37.01
fc21b6d0d77554b6741e9e7d71d580...	22:02:03	225 B	181.17	0.0004 0764	0.0002 5057	$2.27
0d7fe7bc546b30879acb6fd24c8a4ea...	22:02:02	224 B	89.29	0.0002 0000	6.9495 1601	$63,041.21
7025665112768 47b7c6ebdf087a9d6...	22:02:02	225 B	181.17	0.0004 0764	0.0011 2113	$10.17
81eb919abdd72493d1987e9bff65cf9...	22:02:01	226 B	180.37	0.0004 0764	0.0240 5298	$218.19
202f726659613a6a16ee5f640f6e638...	22:02:01	226 B	180.37	0.0004 0764	0.0384 1261	$348.45

Slika 8: Seznam transakcij za bitcoin, 1. 2. 2018 22:02, vir: [28]

Kljub številnim slabostim v primerjavi z nekaterimi drugimi kriptovalutami je cena (enega samega) bitcoina 16. decembra 2017 narasla na okoli 19343 $. [37]

2.5.1.2 Ethereum

Ethereum je odprtokodna in na blockchain tehnologiji osnovana platforma za distribuirano računalništvo, ki uporablja pametne pogodbe za izvajanje skript. Uporablja ether kriptovaluto (okrajšano tudi kot ETH), ki jo upravlja ethereum blockchain. Poleg tega, da služi kot digitalni denar, se ether uporablja tudi za plačevanje računalniških storitev na ethereum blockchainu. Za izvršitev pametnih pogodb ter njihovo upravljanje in dostop se porablja t. i. gorivo (angl. gas), kar je drug način imenovanja ethra. [31] [32]

2.5.2 ICO – Initial Coin Offering

Ena izmed največjih težav pri samostojni izdelavi projektov, storitev ali izdelkov je denarni vložek, ki ga mora lastnik podjetja pridobiti. Pri pritegovanju finančno močnih vlagateljev se pogosto zgodi, da tem izdelek/storitev ni všeč. Ena izmed rešitev je t. i. »crowdfunding«, kjer projekt podpre množica ljudi z relativno majhnimi vložki. Vendar to ustvari nov problem, in sicer za vlagatelje. Dokler izdelek ne prispe k vlagatelju (digitalno ali fizično), so praktično »vrgli denar stran«.

Ta problem delno reši ICO – Initial Coin Offerin (slo. prvotna ponudba kovancev). ICO lahko uporabljajo že obstoječ blockchain (npr. ethereum), na katerem izdelajo svojo kriptovaluto oz. žetone (angl. token). Lastniki teh žetonov izvedejo ICO, kjer lahko ljudje kupijo te žetone, s čimer finančno podprejo projekt in v kolikor je ICO uspešen, dobijo neko količino žetonov. Če podjetje za ICO dostavi končni projekt oz. izdelek, ti žetoni pridobijo na vrednosti, v kolikor pa se to ne zgodi, lahko vlagatelji žetone prodajo in si tako vsaj delno povrnejo svojo naložbo.

Ta koncept je lahko nadgrajen še naprej s pomočjo pametnih pogodb, ki lahko zakonsko obvežejo izvajalca ICO k vrnitvi vloženega denarja, kar bi bilo s tradicionalnimi sistemi praktično nemogoče. [14] [16] [17]

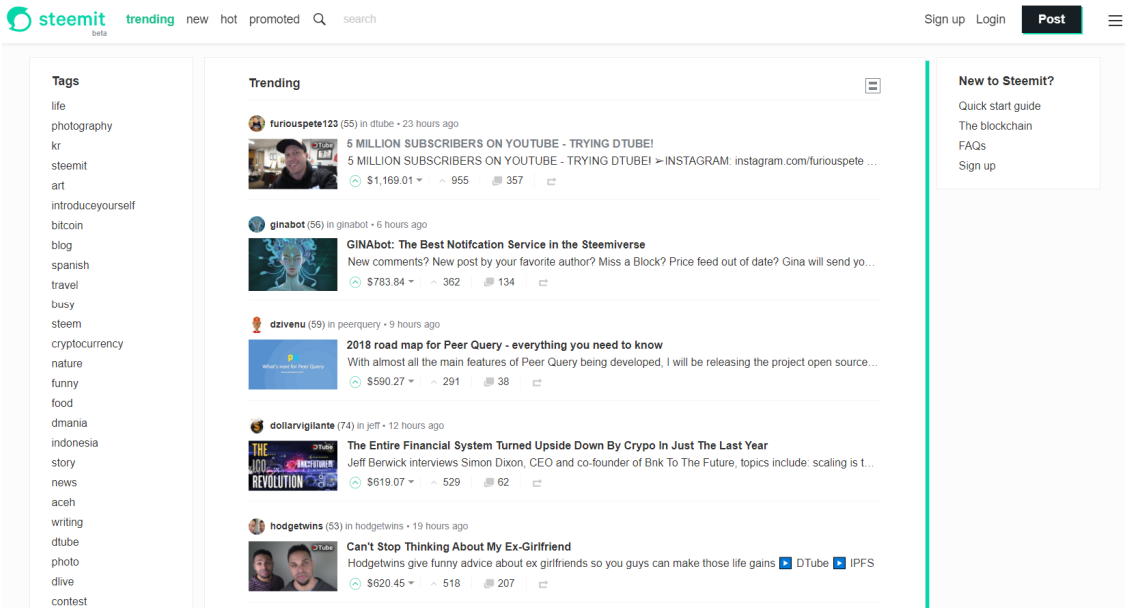
2.5.3 Factom Harmony

Blockchain zaradi svoje zgradbe izjemno oteži (oz. naredi skoraj nemogoče) spreminjanje že zapisanih podatkov na blockchainu. Zaradi tega je idealen in praktično nepogrešljiv za arhiviranje pomembnih dokumentov, kot so: zdravstvene datoteke, listine, intelektualne lastnine, glasovnice, itd. [13]

Podjetje Factom iz Austina (Texas, ZDA) je v sodelovanju z ameriškim oddelkom za domovinsko varnost (angl. United States Department of Homeland Security) razvil produkt, imenovan Factom Harmony. To je na osnovi blockchaina narejena tehnologija, ki je namenjena predvsem podjetjem za shranjevanje in pravilno preverjanje pristnosti pomembnih dokumentov (npr. prodajne listine). [45]

2.5.4 Steemit

Steemit je socialno omrežje, ki deluje na Steem blockchain podatkovni bazi. Za svoje delovanje uporablja kriptovaluto Steem, ki ne potrebuje rudarjenja za validacijo blockchaina, ampak uporablja dejanja uporabnikov Steemit omrežja (kot »lajkanje« posameznih objav) za validacijo posameznih blokov. Takšen proces imenuje »Proof-of-Brain«. Storitev je brezplačna za uporabo in nadomesti tipičen finančni načrt podobnih produktov (oglaševanje na strani) s svojim »Proof-of-Brain« konceptom, kar spodbuja socialne interakcije oseb na omrežju in kaznuje neumestno oz. nepravilno obnašanje s pomočjo »uglednega« sistema. [46] [47]



Slika 9: Spletna stran Steemit omrežja, vir: lasten

2.5.5 BitShares

Poleg shranjevanja dokumentov in kot nadomestek za vir dohodka na socialnem omrežju je blockchain tehnologija dobra tudi za finančni sektor. Ena izmed tehnologij, ki deluje v tem sektorju, je BitShares, ki je odprtokodna javna platforma za izmenjavo sredstev, primarno kriptovalut. Osnovana je na blockchain tehnologiji, kjer trgovanje opravlja omrežje računalnikov, povezanih na blockchain, v nasprotju s tradicionalno izmenjavo, kjer s trgovanjem upravlja centralni strežnik.

BitShares za delovanje ne uporablja rudarjenja, ampak za overjanje blokov uporablja t. i. delegirani dokaz o deležu (angl. Delegated Proof-of-Stake), kjer uporabniki določijo tista

vozlišča, ki bodo overila bloke s pomočjo volitvenega sistema. [48] [49]

2.6 PLATFORME ZA IZDELAVO DECENTRALIZIRANIH APLIKACIJ

2.6.1 Ethereum Solidity

Ethereum blockchain ima pred številnimi podobnimi tehnologijami prednost v svoji implementaciji pametnih pogodb. Ethereum omrežje sestavlja t. i. ethereum virtualno napravo (angl. Ethereum Virtual Machine ali EVM), ki uporablja moč vseh naprav, ki so povezane v omrežje, da poganja programe na blockchainu (t. i. pametne pogodbe). [32]

Za implementiranje aplikacije na blockchain obstaja Solidity, ki je objektno orientiran skriptni jezik, namenjen izdelavi pametnih pogodb. Solidity prevzema nekaj funkcij in navdih iz programskih jezikov, kot so C++, Python itd., in je narejen, da vpliva na EVM. [38]

browser/ballot.sol

```
pragma solidity ^0.4.0;
contract Ballot {

    struct Voter {
        uint weight;
        bool voted;
        uint8 vote;
        address delegate;
    }
    struct Proposal {
        uint voteCount;
    }

    address chairperson;
    mapping(address => Voter) voters;
    Proposal[] proposals;

    /// Create a new ballot with $(_numProposals) different proposals.
    function Ballot(uint8 _numProposals) public {
        chairperson = msg.sender;
        voters[chairperson].weight = 1;
        proposals.length = _numProposals;
    }

    /// Give $(toVoter) the right to vote on this ballot.
    /// May only be called by $(chairperson).
    function giveRightToVote(address toVoter) public {
        if (msg.sender != chairperson || voters[toVoter].voted) return;
        voters[toVoter].weight = 1;
    }

    /// Delegate your vote to the voter $(to).
    function delegate(address to) public {
        Voter storage sender = voters[msg.sender]; // assigns reference
        if (sender.voted) return;
        while (voters[to].delegate != address(0) && voters[to].delegate != msg.sender)
            to = voters[to].delegate;
```

Slika 10: Primer pametne pogodbe za volitve (skrajšano), vir: [39]

Za izdelavo aplikacij na ethereum blockchainu se je potrebno naučiti novega jezika, Solidity, ki je sicer podoben JavaScriptu, kar ta proces nekoliko olajša. Za povezavo pametnih pogodb z aplikacijo je potrebno uporabiti web3j, Java knjižnico. [53]

2.6.2 NEO

NEO je blockchain platforma in kriptovaluta, ki podobno kot ethereum podpira razvijanje decentraliziranih aplikacij s pomočjo pametnih pogodb. [50]

Omrežje NEO je tako kot ethereum P2P in sestavlja virtualno napravo (NeoVM), na kateri se vse pametne pogodbe izvajajo. Za razliko od ethereuma NEO ne uporablja lastnega jezika za razvoj pametnih pogodb, ampak uporablja druge programske jezike, kot npr. C#, Java in Python. [52]

Slika 11: Primer pametne pogodbe na NEO, napisane v C#, vir: [51]

2.6.3 Qtum

Qtum je odprtokodni projekt, razvit s pomočjo blockchain tehnologije. Razvija ga singapursko podjetje Qtum Foundation. Osnovan je na razcepu bitcoinovega blockchaina in se trudi biti alternativa ethereumovi virtualni napravi (EVM). Namen Qtum omrežja je razvijanje decentraliziranih aplikacij za poslovno okolje.

Za razliko od ethereum in NEO omrežij, ki za razporeditev pametnih pogodb uporabljata račune, na katere se pošiljajo transakcije, s čimer se pogodbe aktivirajo, uporablja Qtum sistem UTXO. Ta sistem uporablja neporabljene bitcoine (ker je osnovan na bitcoin blockchainu, jih uporablja kot valuto), ki so uničeni, ko je pogodba ustvarjena in so ponovno narejeni, ko se pogodba izvede. [54] [55]

3 METODE IN CILJI RAZISKOVANJA

Začetek mojega raziskovanja je bil povezan z idejo, kako ustvariti decentralizirano aplikacijo (DApp). Za razumevanje blockchain tehnologije je potrebno precej predznanja in časa, zato sem v tem delu raziskave tudi želel preizkusiti svoje programersko znanje in sposobnost.

3.1 ORODJA IN VIRI

3.1.1 Ethereum Solidity

Za izdelavo DApp sem se odločil uporabiti ethereum blockchain, ker je zgradba te platforme prilagojena namenu.

Za lažjo izdelavo aplikacije sem uporabil tudi ogrodje Truffle (angl. framework), ki je najbolj popularno za razvijanje aplikacij na ethereum blockchainu. V ogrodju so združena orodja za kompilacijo, povezavo, namestitev ter testiranje pametnih pogodb na blockchainu. Hkrati omogoča tudi upravljanje omrežij, ko želimo imeti tako testna kot realna omrežja in veliko drugih funkcij, ki olajšajo razvijanje DApp. [38]

3.1.2 Go Ethereum

Go Ethereum je ena od prvih treh implementacij protokola ethereum. Napisan je v programskem jeziku Go in je popolnoma odprtokoden. [41]

Ena izmed najpomembnejših funkcij Go Ethereuma je Geth. Vmesnik je osnovan na ukazni vrstici za zagon in upravljanje polnega vozlišča ethereum blockchaina. Geth omogoča povezavo na blockchain, rudarjenje, prenos sredstev med računi in raziskovanje zgodovine blokov itd. Najpomembnejša funkcija Getha je sposobnost ustvarjanja zasebnega blockchaina oz. zasebne kopije ethereum blockchaina. [42]

3.1.3 Truffle

Za lažjo izdelavo aplikacije sem uporabil tudi Truffle ogrodje (angl. framework), ki je najbolj aktualno za razvijanje aplikacij na ethereum blockchainu. V ogrodju so združena orodja za kompilacijo, povezavo, namestitev ter testiranje pametnih pogodb na blockchainu. Hkrati omogoča tudi upravljanje omrežij, ko hočemo imeti tako testna kot »prava« omrežja in veliko drugih funkcij, ki olajšajo razvijanje DApp. [40]

3.1.4 TestRPC (Ganache)

Za hitro testiranje pametnih pogodb sem uporabil TestRPC (med izvajanjem raziskovalne naloge se je preimenoval v Ganache), ki ustvari testno okolje za izvajanje in testiranje pametnih pogodb. Po funkciji je podoben Gethu, a je lažji za uporabo, sploh v kombinaciji z ogrodjem Truffle. [43]

3.1.5 MetaMask dodatek za Chrome

MetaMask je razširitev za brskalnik Chrome, ki omogoča lahko in hitro povezavo z ethereum blockchain z namenom uporabe decentraliziranih aplikacij. Je zelo koristen, saj tako ne potrebujemo prenesti »polnega« vozlišča, ki je na ethereum omrežju veliko več kot 300 GB. [56]

3.2 IZDELAVA DECENTRALIZIRANE APLIKACIJE

Eden od namenov raziskovalne naloge je bila izdelava aplikacije, ki deluje na blockchainu (DApp). Namenil sem izdelati preprosto aplikacijo za prodajo in kupovanje izdelkov, ki sem jo ljubkovalno poimenoval »Zajec«.

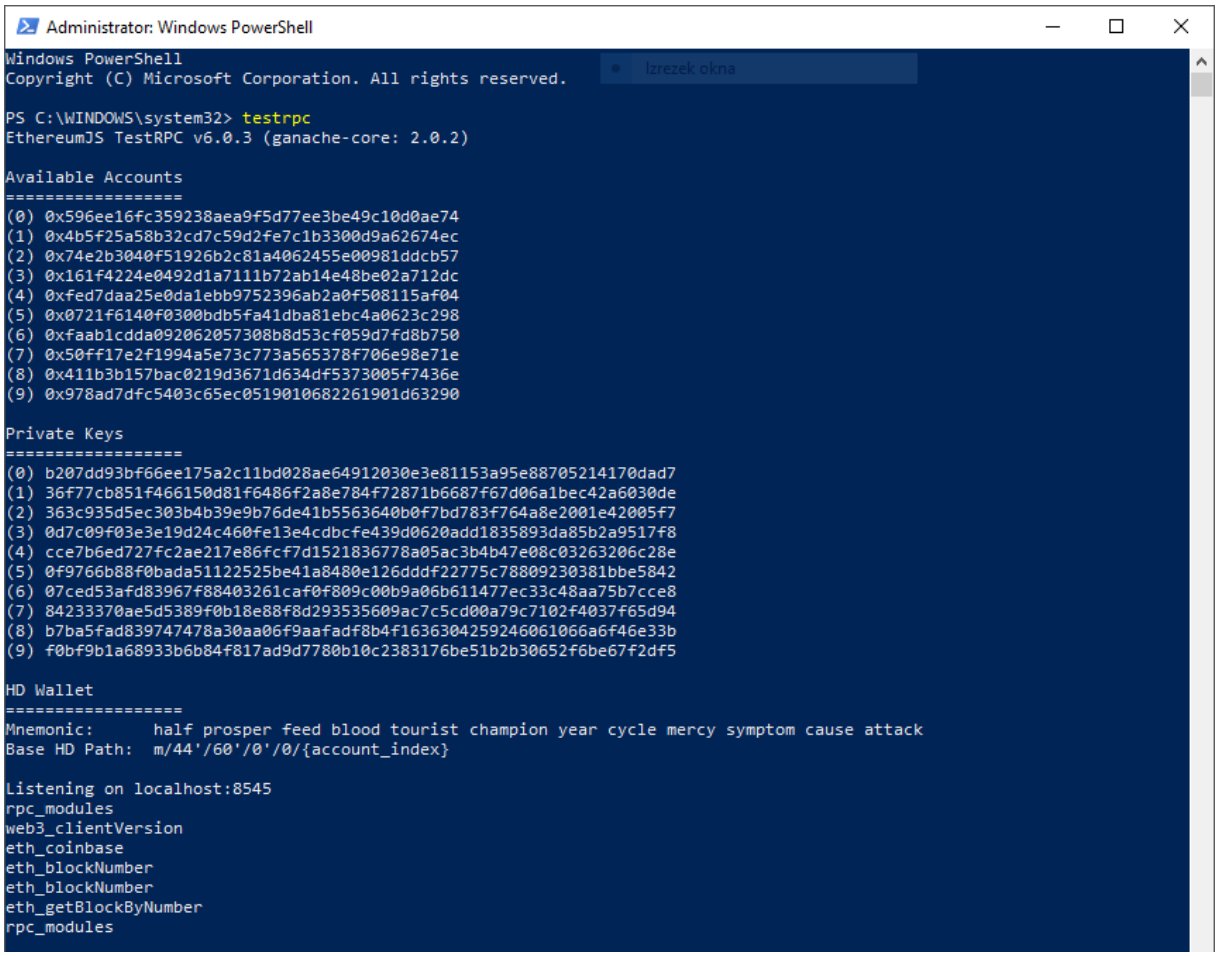
Aplikacijo sem izdeloval na računalniku z operacijskim sistemom Windows 10 s pomočjo vgrajenega orodja PowerShell. Pri vseh prej naštetih orodjih je potrebno povedati, da so to projekti v razvoju, kar pomeni, da lahko postanejo dokaj drugačni v prihodnosti. Pri večini teh orodij nisem uporabljal zadnje verzije, saj je dokumentacija za ta orodja prav tako projekt v razvoju. Starejše verzije imajo zatorej po večini boljšo dokumentacijsko podporo.

3.2.1 Priprava okolja

Pametne pogodbe delujejo na blockchainu (v tem primeru na EVM), zatorej jih ne moremo preprosto napisati v poljubnem jeziku in jih izvesti na računalniku. Pametne pogodbe moramo prevesti v strojni jezik, ki ga EVM razume, ter jih »poslati« na blockchain. Če bi to hotel storiti na glavnem ethereum omrežju, bi za takšno dejanje moral porabiti ether v obliki goriva, da bi pametna pogodba lahko delovala. Na takšen način bi bila izdelava aplikacije draga in nasploh zahtevna. Na glavnem blockchainu bi moral pridobiti tudi uporabnike za testiranje, za kar pa bi jih moral prepričati, da porabljajo ether in s tem denar.

Takšen pristop bi po nepotrebnem zapletel in otežil proces izdelave aplikacije, s katero nimam predhodnih izkušenj in je na splošno slab pristop k izdelavi kakršnegakoli izdelka. Za ta

namen sem uporabil orodje TestRPC (oz. Ganache), ki ustvari zaseben blockchain s preprostimi ukazi v ukazni vrstici (PowerShell).

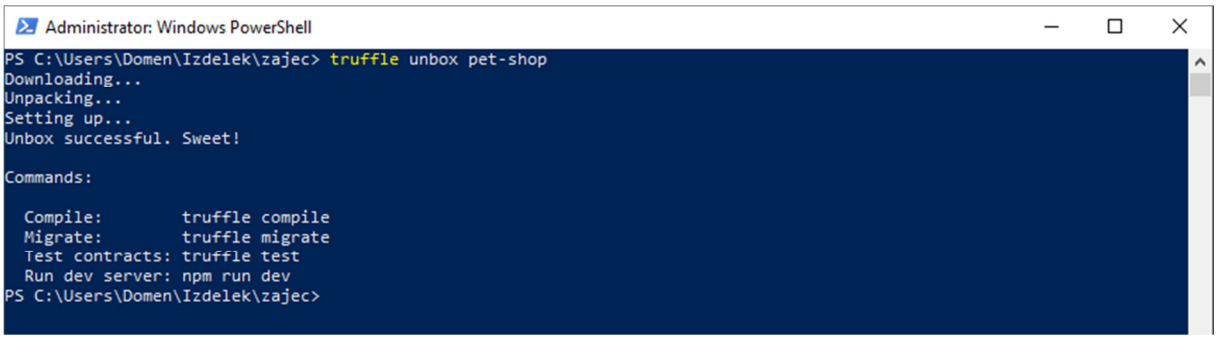


Slika 12: Zagnan TestRPC v PowerShell konzoli, vir: lasten

Vsakič ko TestRPC zaženemo, ta ustvari deset računov, vsak s po 100 ETH. Z vsakim računom ustvari tudi zaseben ključ in zažene blockchain vozlišče. S tem pripravi okolje, v katerem bom pozneje izdajal pametne pogodbe, potrebne za delovanje aplikacije in jih tudi testiral, ne da bi porabljal »pravi« ether.

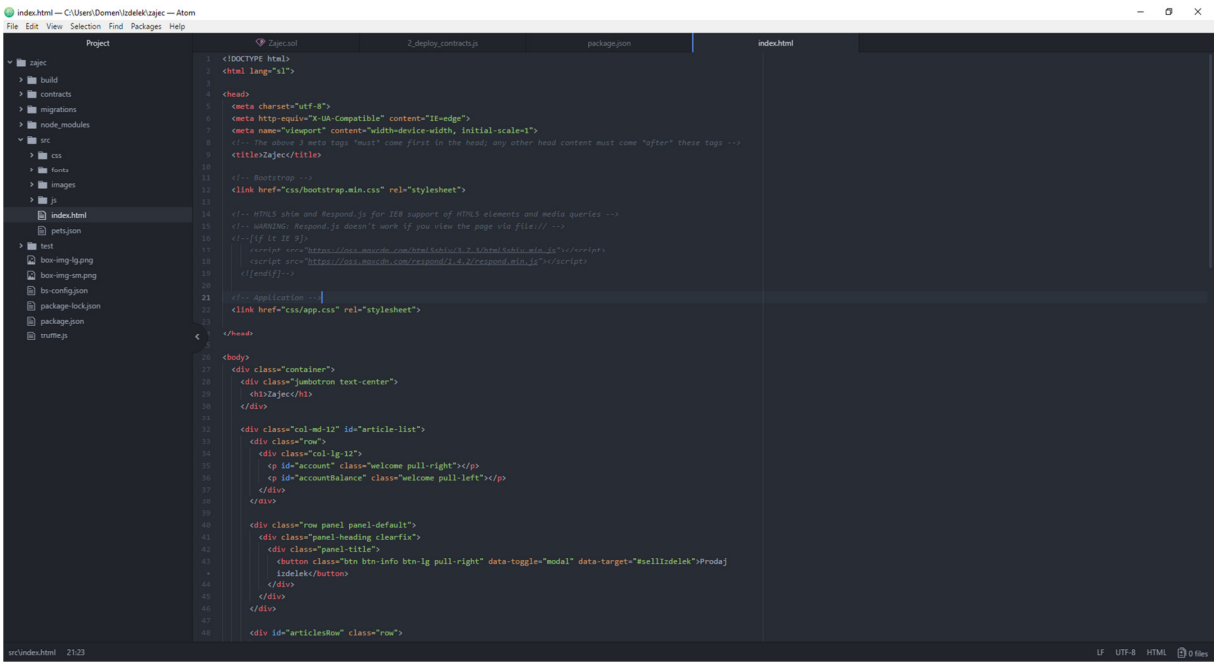
3.2.2 Ogrodje aplikacije

Namen raziskovalne naloge je bilo raziskovanje blockchaina in izdelava aplikacije. Da bi takšna aplikacija bila uporabna, je treba izdelati tudi celoten »sprednji del« aplikacije, kar pa ni namen te raziskovalne naloge. Tu nastopi Truffle, saj omogoča avtomatsko izdelavo ogrodja aplikacije, ki je že pripravljena za razvijanje na blockchainu.



Slika 13: Uporaba Truffle za hitro izdelavo ogrodja aplikacije, vir: lasten

Z ukazom *truffle unbox pet-shop* Truffle izdela vse potrebne konfiguracijske datoteke, ki bi jih bilo nesmiselno »ročno« izdelovati. Ta ukaz tudi doda vse datoteke, ki so potrebne za povezovanje z blockchainom, nekaj orodij za boljšo ustvarjanje spletnih strani ter generiranje privzete HTML datoteke, ki sem jo za svojo aplikacijo prilagodil. Tako je bil večji (nebistveni) del aplikacije narejen brez večjega napora.



Slika 14: Povzetek prilagojene HTML kode, vir: lasten

3.2.3 Pametna pogodba

Najbolj pomemben del decentralizirane aplikacije so pametne pogodbe, ki povežejo tradicionalno aplikacijo (narejeno v HTML, PHP, JS itd.) z blockchainom. Testno omrežje deluje na podlagi ethereuma, zato sem za pisanje pogodbe uporabil Solidity.

Pametna pogodba od aplikacije prejme podatke o opravilih in kdo jih mora opravljati. Te

podatke nato shrani na blockcahinu. Preko aplikacije lahko (s pomočjo JavaScripta) kličemo funkcijo za prikaz teh opravil, ki poda vse shranjene vrednosti nazaj v aplikacijo. Ko so opravila končana, lahko s funkcijo pošljemo nagrado (v obliki ETH) na račune, podane v pogodbi.

```
contract Zajec {
  // Spremenljivke
  address parent;
  address[6] people;
  string[6] tasks;
  string task;
  string person;
  string title;
  string note;
  uint256 reward;

  function toString(address x) returns (string)
  {
    bytes memory b = new bytes(20);
    for (uint i = 0; i < 20; i++)
        b[i] = byte(uint8(uint(x) / (2**(8*(19 - i)))));
    return string(b);
}

  function addTasks(string _title, string _note, uint256 _reward, address[6] _people, string _timestamp) public
  {
    parent = msg.sender;
    title = _title;
```

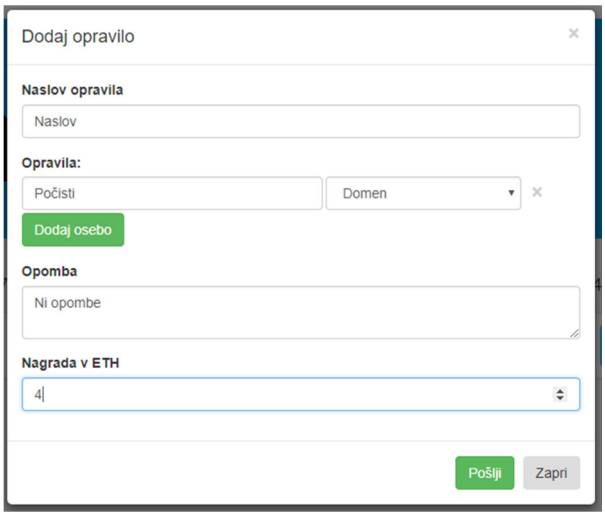
Slika 15: Izvleček pametne pogodbe, vir: lasten

Pri pisanju pogodb sem naletel na eno izmed pomanjkljivosti, ki jih Solidity (trenutno) ima. Ne obstaja lahek način za podajanje tabel podatkov (razen ethereum naslovov), kot je to v mojem primeru tabela opravil, zaradi česar sem moral posamezna opravila dodajati s posebno spremenljivko za vsako iteracijo.

Za premik pogodbe na blockchain sem uporabil Truffle, z njegovo funkcijo migracije. Ko to izvedemo, ta prevede pogodbo v strojno kodo, ki jo bere EVM ter jo prestavi na blockchain. Funkcije pametne pogodbe lahko nato kličem preko web3js, ki je eno izmed številnih orodij, ki so nameščena skupaj s Truffle ogrodjem.

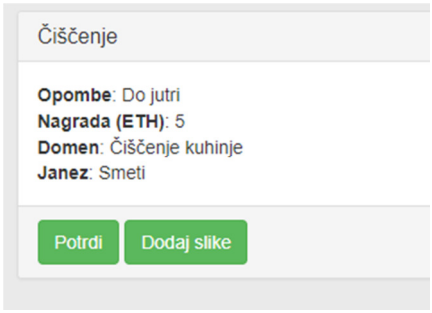
3.2.4 Dodajanje funkcij v aplikacijo

Za pošiljanje vrednosti o opravilih sem v aplikacijo dodal gumb za opravila, ki uporabniku predstavi obrazec za dodajanje opravil. Uporabnik v ta obrazec vnese opravila, izbere osebe, ki bodo ta opravila opravljala, doda opombe ter nastavi končno nagrado (v ETH).



Slika 16: Obrazec za dodajanje opravil, vir: lasten

Ko je obrazec oddan, se opravila prikažejo na glavni strani aplikacije, kjer so zapisane vse prej določene vrednosti. Uporabnik, ki je določil opravila, lahko nato te potrdi ter pošlje nagrado na račune, ki so bili določeni v obrazcu.

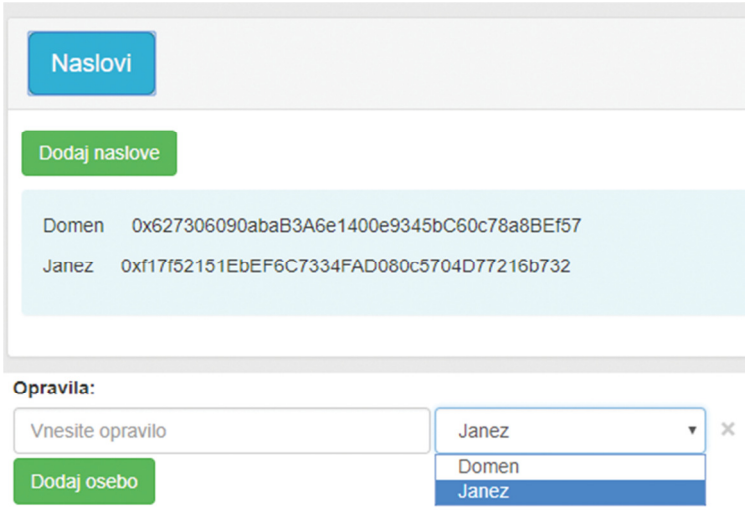


Slika 17: Prikazana opravila, vir: lasten

Na podoben način sem dodal tudi možnost dodajanja in shranjevanja naslovov oseb, za lažjo izbiro pri dodajanju opravil. Namesto na blockchain jih shrani v JSON datoteko, na lokalnemu strežniku, ker ni potrebe trošiti kriptovalute za preprost seznam oseb, ki ni kritičnega pomena.

Slika 18: Okno za dodajanje naslovov oseb, vir: lasten

Ti naslovi se nato prikažejo, ko izbiramo osebe in ko pregledamo naslove oseb pod gumbom za le-te.

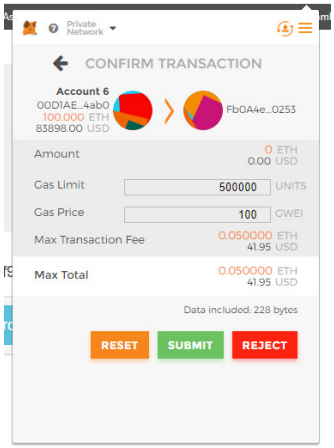


Slika 19: Prikaz naslovov ter oseb, vir: lasten

Aplikacija poda osebam, ki morajo izvesti opravila, možnost, da dodajo slike, ki potrjujejo njihovo delo. Zaradi omejitev, ki jih ima Solidity pri podajanju tabel podatkov (npr. tabele znakov ali besed), je to omejeno pri opravilu na le eno sliko. V kolikor bo možnost za pridobivanje tabel podatkov preko aplikacije v prihodnosti dodana, nameravam to posodobiti.

3.2.5 MetaMask

Da bi uporabnik lahko sploh dostopal do aplikacije, potrebuje dostop do blockchaina. Na glavnem omrežju mora imeti naloženo vozlišče. To večini uporabnikov zaplete proces dostopa. Ena izmed lažjih rešitev je dodatek za brskalnik Chrome, imenovan MetaMask. MetaMask simulira »lahko« vozlišče kar v brskalniku. Ko ga uporabnik nastavi, omogoča preprost dostop do ethereum omrežja in uporabo aplikacije. MetaMask se avtomatično poveže na privzete nastavitve, ki jih je ustvaril Truffle, zato kode za njegovo vključitev ni treba bistveno spreminjati. MetaMask se vključi v proces pošiljanja transakcij in zato vsakič vpraša za potrditev in nastavitev transakcije (količina goriva za hitrost itd.).



Slika 20: MetaMask okno za potrditev transakcije, vir: lasten

Omogoča tudi hitro zamenjavo računov, kar izjemno pomaga pri testiranju aplikacije. Celotna aplikacija torej deluje z naslednjimi opcijami:

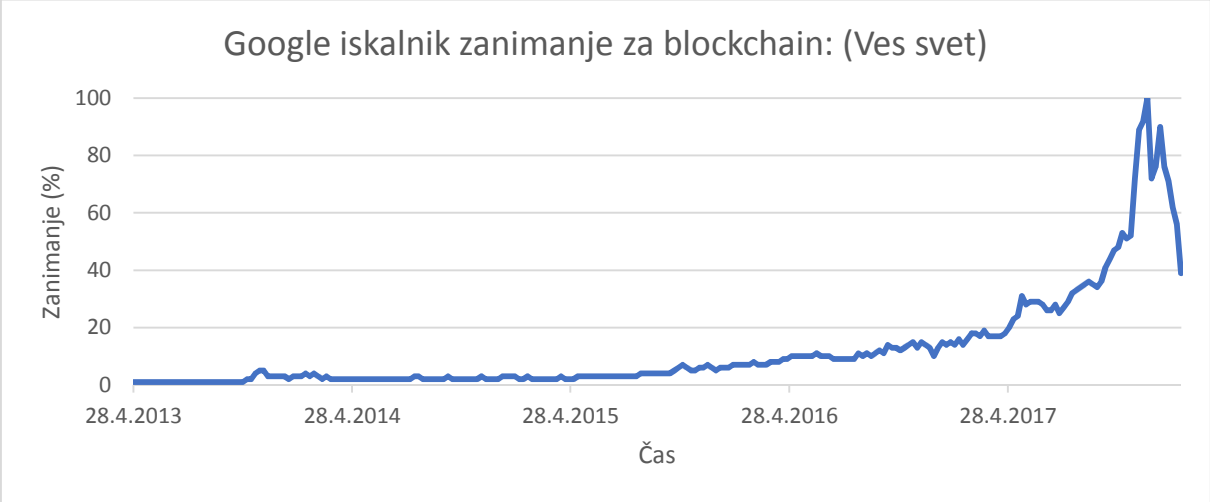
- uporabnik s pravilno nastavljenim MetaMaskom odpre aplikacijo,
- če želi, lahko ustvari seznam opravil,
- MetaMask zahteva potrdilo za oddajo transakcije na pametno pogodbo,
- avtor seznama lahko opravila nato potrdi, s čimer pošlje ETH na račune,
- MetaMask prikaže okno za nastavitev transakcije (vrednost, količino goriva) in za potrditev transakcije,
- pametna pogodba izvede transakcije in pošlje ETH na prave naslove.

4 REZULTATI

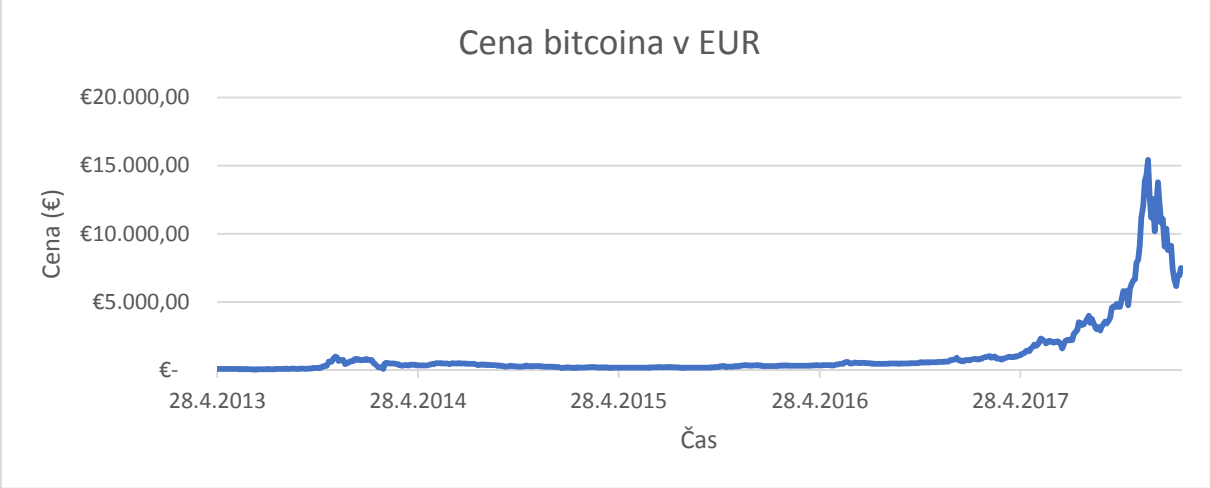
4.1 POTRJEVANJE HIPOTEZ

4.1.1 Izdelki, narejeni s pomočjo blockchain tehnologije

Blockchain tehnologija je pridobila na popularnosti in velikem razvoju v zadnjih desetih letih z vzponom bitcoina (razvidno iz grafa 2 in 3). Zaradi svojih edinstvenih značilnosti je blockchain odličen za izdelavo kriptovalut, kar je danes tudi njegova najpopularnejša uporaba.



Graf 2: Zanimanje za blockchain, Google Trends, vir: [58]



Graf 3: Cena bitcoina od 28. 4. 2013 do 14. 2. 2018, vir: [57]

Kriptovalute niso edini izdelki, ki za svoje delovanje uporabljajo blockchain. Med raziskovanjem sem našel veliko produktov, orodij, platform, ki za svoje delovanje potrebujejo

unikatne lastnosti blockchain tehnologije. Nekatere izmed njih sem tudi opisal v raziskovalni nalogi. Primer takšne tehnologije je ICO orodje za financiranje projektov na blockchainu, ki bi sicer lahko obstajalo brez blockchaina, vendar brez lastnosti, ki ga naredijo edinstvene in drugačne od že obstoječih platform za financiranje projektov (kot npr. Kickstarter).

S tem sem prvo hipotezo, da kriptovalute niso edini izdelek, ki uporabljajo blockchain tehnologijo, **potrdil**.

4.1.2 Sistemi in tehnologije, osnovane na blockchain tehnologiji

V raziskovalni nalogi sem opisal Factom Harmony (sistem za verodostojno shranjevanje in overjanje dokumentov v poslovnem okolju) ter BitShares (izmenjava kriptovalut, ki je zaradi decentralizirane narave varnejša in bolj zaupanja vredna kot druge s centralnim/-i strežniki), ki brez blockchain tehnologije ne bi obstajale. Poleg teh dveh sem opisal tudi Steemit (socialno omrežje brez oglasov), ki bi sicer kot socialno omrežje lahko obstajalo, a ne bi omogočalo »nagrajevanja« ustvarjalcev in zagnanih udeležencev na strani s pravim denarjem (kriptovaluto).
Seveda to niso edine aplikacije oz. sistemi, ki so osnovani na blockchain tehnologiji in zagotovo ne bodo zadnje, sploh zaradi razvojnih orodij, kot je Solidity na ethereum blockchainu in druga.

S tem sem drugo hipotezo, da obstajajo vsaj 3 vrste sistemov oz. tehnologij, ki brez blockchaina ne bi bili mogoči, **potrdil**.

4.1.3 Orodja za izdelavo decentraliziranih aplikacij

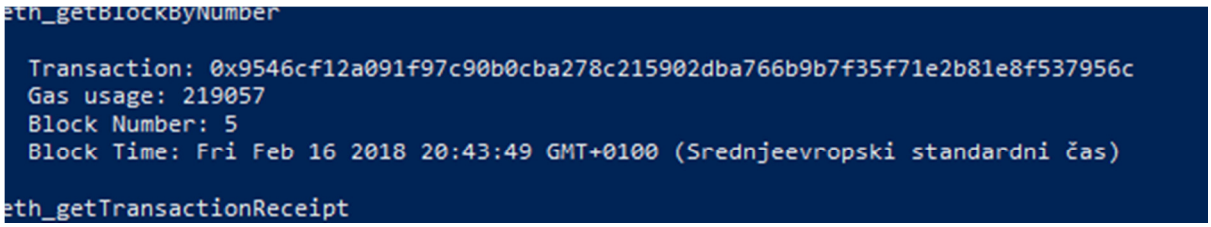
Pri izdelavi decentralizirane aplikacije je bil prvi korak poiskati primerno razvojno okolje in orodja, ki bi jih potreboval za izdelavo aplikacije. Ugotovil sem, da obstajajo številna orodja oz. platforme za izdelavo takšnih aplikacij. V procesu raziskovanja sem se odločil opisati tri, Ethereum, NEO in Qtum. Vsaka od teh platform ima svoje posebnosti, čeprav vse delujejo na principu pametnih pogodb. Ethereum je od vseh najbolj popularen, zato ima tudi večjo skupnost kot drugi dve orodji, kar je tudi razlog, zakaj sem ga izbral za izdelavo svoje aplikacije.

S tem sem tretjo hipotezo, da so za izdelavo aplikacij, ki temeljijo na blockchain tehnologiji, razvita vsaj 3 orodja, **potrdil**.

4.1.4 Izdelava lastne aplikacije

Kot dijak v programu Tehnik računalništva sem se odločil izdelati aplikacijo, ki bi delovala na blockchain tehnologiji. S četrto hipotezo sem si postavil cilj, da bi aplikacija lahko nedvomno shranila dogovore. Aplikacijo sem tematsko izdelal, vezano na dogovore v gospodinjstvu, kdo mora kaj narediti (sprazniti smeti, počistiti kuhinjo itd.). V procesu izdelave sem dodal tudi možnost nagrajevanja za opravljene naloge.

Takšna aplikacije je od tradicionalne drugačna predvsem zaradi tega, ker shranjenih podatkov na blockchainu ne moremo spreminjati ali preprosto izbrisati. »V običajnem svetu« lahko uničimo listke, na katerih so napisane naloge, prav tako lahko spremenimo besedilne dokumente, na blockchainu pa to ne deluje.



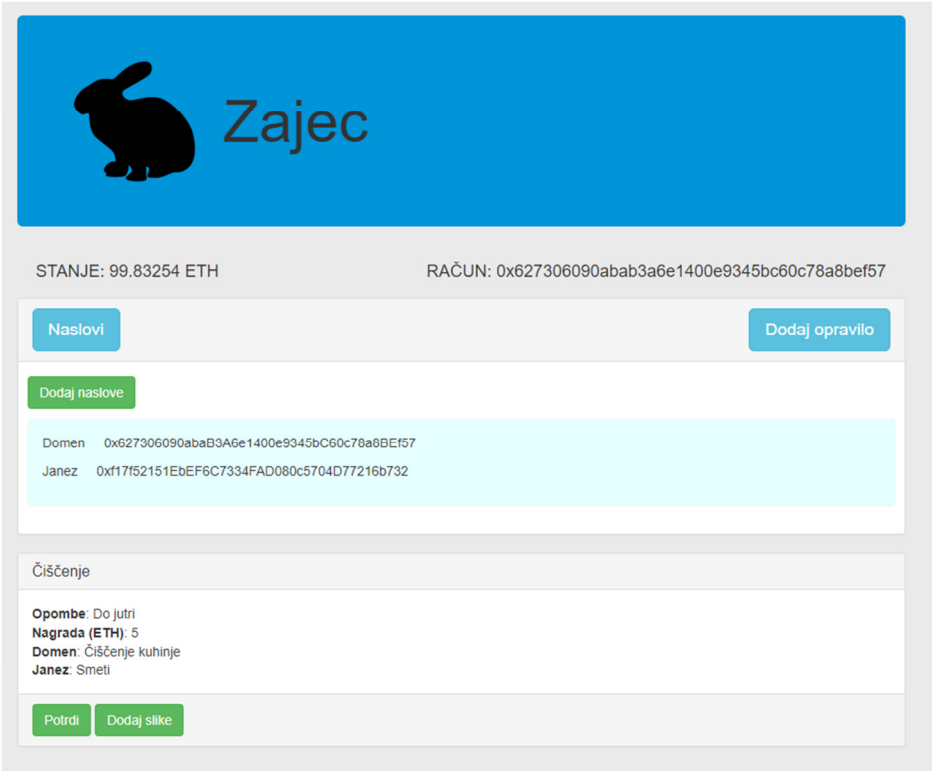
Slika 21: Primer transakcije (v testnem okolju), vir: lasten

Končana aplikacija omogoča zapis seznama opravil na blockchain in njihov pregled ter pošiljanje nagrad, če so bila opravila opravljena.

Ugotovil sem, da je takšna aplikacija sicer dražja od tradicionalne, ker je potrebno za vsako oddano transakcijo ali izvedeno funkcijo pametne pogodbe plačati nekaj goriva (angl. »gas«) zaradi hitrosti izvedbe. Sam teh težav sicer nisem imel, ker sem aplikacijo razvijal v testnem okolju z nepravim ETH.

Pri izdelavi aplikacije in testiranju mi je zelo pomagal tudi dodatek za brskalnik Chrome, MetaMask. Ker za svoje delovanje uporabljajo blockchain, se morajo decentralizirane aplikacije na njega povezati. Za uporabnika je verjetno prenesti nekaj GB veliko vozlišče za dostop do aplikacije moteče, potrebno je tudi nekaj predznanja. Čeprav je z uporabo MetaMaska ta proces lažji in manj zapleten, še vedno zahteva nekaj poznavanja (sploh za nakup ETH in prenos na lasten naslov), zato sem ugotovil, da takšna aplikacija ne bi bila

primerna v domačem okolju, sploh za manj resne dogodke.



Slika 22: Izgled aplikacije, vir: lasten

Z izdelavo delujoče aplikacije sem četrto hipotezo, da lahko izdelam lastno aplikacijo, ki temelji na blockchain tehnologiji in omogoča nesporno shranjevanje dogovorov v obliki pametne pogodbe, prav tako **potrdil**.

5 POVZETEK

Ozadje

Kot dijak programa Tehnik računalništva se zelo zanimam za računalniške vede. Verjamem, da je v tej stroki izjemno pomembno biti na tekočem s tehnološkimi dosežki in novimi tehnologijami. Blockchain je ena izmed novejših tehnologij, ki ustvarja veliko zanimanje. Mnogi jo napovedujejo kot tehnologijo prihodnosti, kar me je tudi vzpodbudilo za raziskovanje na tem področju.

Namen

Glavni namen naloge je bil ugotoviti, kaj je blockchain tehnologija ter kakšne so njene (trenutne) aplikacije. Raziskovalno nalogo sem sprejel kot priložnost, da se sam preizkusim v izdelavi aplikacije, ki temelji na blockchain tehnologiji.

Metode

V raziskovalni nalogi sem uporabil predvsem akcijsko metodo raziskovanja. Ob izdelavi aplikacije sem raziskal trenutno stanje razvoja tehnologij na tem področju. Metodo sklepanja sem uporabil pri raziskovanju zgodovine blockchain tehnologije.

Rezultati

Na začetku sem si zastavil štiri hipoteze, katere sem vse potrdil. Ugotovil sem, da obstaja več izdelkov poleg kriptovalut, ki za delovanje potrebujejo blockchain, hkrati pa obstaja tudi več platform oz. orodij za izdelavo takšnih aplikacij. Uspelo mi je izdelati tudi lastno aplikacijo, ki temelji na blockchain tehnologiji s pomočjo prej omenjenih orodij.

Zaključek

Blockchain tehnologija se je v zadnjih letih razvijala in napredovala, zato njene pomembnosti ter zmožnosti ne moremo ignorirati. Kot dijaka, ki se izobražuje na tehniškem področju, me nove tehnologije in računalniško področje izjemno zanima, zato sem se odločil s to raziskovalno nalogo raziskovati področje teh - novih tehnologij. Svoj cilj sem dosegel in ga nadgradil z izdelavo svoje aplikacije, ki jo nameravam še naprej razvijati, hkrati pa se bom še naprej učil in preizkušal na tem področju.

6 ZAHVALA

Zahvaljujem se mentorju Simonu Konečniku za strokovno pomoč pri pisanju raziskovalne naloge, podporo pri oblikovanju naloge ter somentorju Islamu Mušiću za pomoč pri oblikovanju ideje, tehnični pomoči ter spodbudi za izdelovanje raziskovalne naloge. Prav tako se zahvaljujem učiteljici Jolandi Melanšek za lektoriranje angleškega povzetka in Bojani Vrbnjak za lektoriranje celotne naloge. Hvala tudi staršem za podporo in spodbudo ter vsem, ki so mi pri raziskovanju na kakršenkoli način pomagali.

7 VIRI IN LITERATURA

1. https://en.wikipedia.org/wiki/Blockchain, 1. 2. 2018
2. Haber S., Stornetta W. S., **How to time-stamp a digital document**, (19. 8. 1990), https://link.springer.com/article/10.1007/BF00196791, 1. 2. 2018
3. Nakamoto S., **Bitcoin: A Peer-to-Peer Electronic Cash System**, (31. 10. 2008) https://bitcoin.org/bitcoin.pdf, 1. 2. 2018
4. Swan M., **Blockchain: Blueprint for a New Economy**, (januar 2015), http://shop.oreilly.com/product/0636920037040.do, 1. 2. 2018
5. Kolak A., **Pomen in vloga kriptografije in kriptoanalize na področju zagotavljanja nacionalne varnosti**, (2006), https://www.fdv.uni-lj.si/dela-fdv/iskanje/?lang=slv&cmd=izpis&gID=8459, 17. 2. 2018
6. Becker G., **Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis** (18. 7. 2008), http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/becker_1.pdf, 17. 2. 2018
7. https://upload.wikimedia.org/wikipedia/commons/thumb/9/95/Hash_Tree.svg/1280px-Hash_Tree.svg.png, 1. 2. 2018
8. https://www.code-brew.com/blockchain/, 1. 2. 2018
9. Brownworth A., https://anders.com/blockchain/, 1. 2. 2018
10. https://cdn-images-1.medium.com/max/1600/1*pbyFH4U5sO27UE1EjnImoA.png, 1. 2. 2018
11. https://en.bitcoin.it/wiki/Full_node, 1. 2. 2018
12. https://en.bitcoin.it/wiki/Mining, 1. 2. 2018
13. Tapscott D., Tapscott A., **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**, (2016), http://dontapscott.com/books/blockchain-revolution/, 1. 2. 2018
14. http://www.ethdocs.org/en/latest/contracts-and-transactions/contracts.html, 1. 2. 2018
15. https://www.ethereum.org/token, 1. 2. 2018
16. Zainuddin A., https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/, 1. 2. 2018
17. https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp, 1. 2. 2018

18. Raval S., **Decentralized Applications: Harnessing Bitcoin's Blockchain Technology**, (Julij 2016), http://shop.oreilly.com/product/0636920039334.do?sortby=publicationDate, 1. 2. 2018
19. https://www.delphitools.info/DWSH/node-topology.png, 1. 2. 2018
20. https://en.wikipedia.org/wiki/Distributed_computing, 1. 2. 2018
21. Buterin V., **The Meaning of Decentralization**, (6. 2 .2017), https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274, 2. 1. 2018
22. https://en.bitcoin.it/wiki/Full_node#Why_should_you_run_a_full_node, 1. 2. 2018
23. https://res.cloudinary.com/practicaldev/image/fetch/s--SHFjkIkC--/c_limit%2Cf_auto%2Cfl_progressive%2Cq_auto%2Cw_880/https://i.imgur.com/A5tl3oY.png, 1. 2. 2018
24. Kavšek A., **Analiza uporabe tehnologije blockchain v organizacijah**, https://dk.um.si/IzpisGradiva.php?id=66112, 1. 2. 2018
25. https://en.wikipedia.org/wiki/Bitcoin_scalability_problem, 1. 2. 2018
26. https://www.investopedia.com/terms/1/51-attack.asp, 1. 2. 2018
27. Berlot N., Bernik I., **Varnost kriptovalute bitcoin: diplomsko delo univerzitetnega študija**, https://dk.um.si/IzpisGradiva.php?id=54216, 1. 2. 2018
28. https://tradeblock.com/bitcoin, 1. 2. 2018
29. https://en.bitcoin.it/wiki/Main_Page, 3. 2. 2018
30. https://en.bitcoin.it/wiki/Weaknesses, 3. 2. 2018
31. https://en.wikipedia.org/wiki/Ethereum, 3. 2. 2018
32. http://www.ethdocs.org/en/latest/, 3. 2. 2018
33. https://bitcoin.org/img/icons/opengraph.png, 3. 2. 2018
34. https://en.wikipedia.org/wiki/Fork_(blockchain), 3. 2. 2018
35. https://en.wikipedia.org/wiki/Bitcoin_Cash, 3. 2. 2018
36. https://coinanalysis.io/how-many-transactions-per-second-bitcoin-cash/, (3. 1. 2018), 3. 2. 2018
37. https://coinmarketcap.com/currencies/bitcoin/historical-data/, 17. 2. 2018
38. https://solidity.readthedocs.io/en/develop/, 5. 2. 2018

39. https://remix.ethereum.org/#optimize=false&version=soljson-v0.4.19+commit.c4cbbb05.js, 5. 2. 2018
40. https://github.com/trufflesuite/truffle, 5. 2. 2018
41. https://geth.ethereum.org/, 5. 2. 2018
42. https://github.com/ethereum/go-ethereum/wiki/geth, 5. 2. 2018
43. https://github.com/trufflesuite/ganache-cli, 5. 2. 2018
44. https://blockchain.info/charts/transactions-per-second, 12. 2. 2018
45. https://www.factom.com/solutions, 12. 2. 2018
46. https://steem.io/SteemWhitePaper.pdf, 12. 2. 2018
47. https://steemit.com/, 12. 2 .2018
48. https://en.wikipedia.org/wiki/BitShares, 12. 2. 2018
49. https://bitshares.org/, 12. 2. 2018
50. https://neo.org/, 12. 2. 2018
51. http://docs.neo.org/assets/smart_contract_function_code.png, 12. 2. 2018
52. http://docs.neo.org/en-us/sc/introduction.html, 12. 2. 2018
53. https://github.com/web3j/web3j, 12. 2. 2018
54. https://qtum.org/en/general-faq, 12. 2. 2018
55. Dai P., Mahi N., Earls J., Norta A., **Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform**, https://qtum.org/uploads/files/a2772efe4dc8ed1100319c6480195fb1.pdf, 12. 2. 2018
56. https://metamask.io/, 13. 2. 2018
57. https://min-api.cryptocompare.com/data/histoday?fsym=BTC&tsym=EUR&limit=60&aggregate=3&e=CCCAGG&allData=true, 14. 2. 2018
58. https://trends.google.com/trends/explore?date=2013-04-28%202018-02-14&q=blockchain, 14. 2. 2018