Pametni ugovori

Bartolović, Zoran

Undergraduate thesis / Završni rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **The Polytechnic of Rijeka / Veleučilište u Rijeci**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:125:002993

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-05-08**

Repository / Repozitorij:

Polytechnic of Rijeka Digital Repository - DR PolyRi

VELEUČILIŠTE U RIJECI

Zoran Bartolović

PAMETNI UGOVORI

(završni rad)

Rijeka, 2018.

VELEUČILIŠTE U RIJECI

Poslovni odjel

Stručni studij Informatika

PAMETNI UGOVORI

(završni rad)

MENTOR

Mr. sc. Jasminka Tomljanović

STUDENT

Zoran Bartolović

MBS: 2422038733/12

Rijeka, rujan 2018.

VELEUČILIŠTE U RIJECI
Poslovni odjel

Rijeka, 23.01.2018.

ZADATAK
za završni rad

Pristupniku ZORANU BARTOLOVIĆU matični broj 2422038733/12 studentu stručnog studija Informatika izdaje se zadatak za završni rad – tema završnog rada pod nazivom:

PAMETNI UGOVORI

Sadržaj zadatka:

Prikazati povijesni pregled pametnih ugovora. Objasniti što su pametni ugovori i koja je njihova namjena s osvrtom na sigurnost pametnih ugovora. Opisati značajke blockchain tehnologije, njezinu svrha u današnjem digitalnom svijetu, te objasniti kako pametni ugovori funkcioniraju. Definirati glavne prednosti blockchain tehnologije i opisati razliku između centraliziranih i decentraliziranih sustava. Prikazati najpoznatije platforme za pametne ugovore i njihove karakteristike. U praktičnom dijelu rada prikazati i objasniti postupak programiranja jednostavnog pametnog ugovora na Ethereum platformi, njegovo testiranje i objavu na mreži *testNET*.

Rad obraditi skladno odredbama Pravilnika o završnom radu Veleučilišta u Rijeci.

Zadano: 23. 01. 2018. **Predati do: 15. 07. 2018.**

Mentor
(mr. sc. Jasminka Tomljanović, viši predavač)

Pročelnik odjela
(mr. sc. Marino Golob, viši predavač)

Zadatak primio dana: 23.01.2018.
(Monika Bunjevčević)

Dostavlja se:
- **mentoru**
- **pristupniku**

IZJAVA

Izjavljujem da sam završni rad pod naslovom Pametni ugovori izradio samostalno pod nadzorom i uz stručnu pomoć mentorice mr. sc. Jasminke Tomljanović.

Zoran Bartolović

(potpis studenta)

SAŽETAK

U ovom završnom radu opisani su i analizirani pametni ugovori i blockchain tehnologija bez koje pametni ugovori ne bi postojali. U početnom dijelu nalazi se povijesni pregled pametnih ugovora, objašnjeno je što su pametni ugovori i koja je njihova namjena, u nastavku se nalazi kratki osvrt na sigurnost pametnih ugovora. U radu se nalazi opis i značajke blockchaina i njegova svrha u današnjem digitalnom svijetu, pomoću blockchain tehologije objašnjeno je kako pametni ugovori funkcioniraju. Osim toga, navedene su glavne prednosti blockchain tehnologije i opisana je razlika između centraliziranih i decentraliziranih sustava, jer i sama blockchain mreža može biti centralizirana ili decentralizirana. Spominju se partneri koji sudjeluju u mreži i njihovi zadaci unutar sustavu. U drugom dijelu rada navedene su tri najpoznatije platforme za pametne ugovore i njihove karakteristike. Nakon toga su navedeni primjeri uporabe pametnih ugovora i mogućnosti koje donose, korištenjem pametnih ugovora i blockchain tehnologije svakodnevni životnih i poslovni procesi se unaprijeđuju i postaju sigurniji, brži i transparetniji. U zadnjem dijelu rada prikazan je i objašnjen postupak programiranja jednostavnog pametnog ugovora na Ethereum platformi i njegovo testiranje, nakon toga slijedi prikaz objave samog ugovora na test mrežu (engl. *testNET*).

Ključne riječi: pametni ugovor, blockchain tehnologija, DLT, kriptovalute, wallet

SADRŽAJ

1. UVOD

U današnje suvremeno doba osnovni mehanizmi poslovanja i razmjene dobara su transakcije, isto tako ogromna količina današnjih usluga je zasnovana na konceptu transakcija. Međutim, problem koji sa sobom nosi realizacija transakcija je nepovjerenje, gledajući kroz povijest, taj problem je riješen posredovanjem, tu ulogu u današnje vrijeme većinom imaju banke. Posrednici imaju ograničenja koja su nametnuta sa strane države i zakona. Unatoč ograničenja sa strane države, globalizacija tržišta je omogućila širenje banaka izvan granica države tako da danas pojedine banke su postale veće i moćnije od nekih država, samim time država gubi moć kontrole nad njima.

Upravo blockchain tehnologija nudi alternativu tradicionalnim transakcijama koje uglavnom obavljamo putem banaka. Ukoliko imamo zaključenje ugovora o poslovanju na osnovu kojeg se mora izvršiti prijenos sredstava to se može napraviti izravno digitalnim valutama putem blockchaina, bez posredovanja banaka. Na isti način putem pametnih ugovora omogućena je direkna razmjena digitalnih dobara, bez mogućnosti da jedna strana prevari drugu i ne ispuni svoj dio obaveza predviđenih ugovorom. Posrednik, u ovom slučaju banka, je zamijenjen blockchain mrežom i pametnim ugovorima koji nude visoku razinu sigurnosti, brzine, transparentnosti, te štedljivosti jer nema krutih pravila banaka i visokih provizija.

Motivacija za pisanje ovog rada je proizašla iz znatiželje o blockchain tehnologiji i širokim mogućnostima primjene ove suvremene tehnologije u svim sferama društva. Pametni ugovori, koji su konceptualizirani još 90-ih godinama, zaživjeli su u stvarnosti zahvaljujući blockchain tehnologiji i omogućili su decentraliziran transparentan sustav upravljanja sredstvima koji omogućuje direktnu razmjenu, bez posredničkih troškova, uz visoku stopu sigurnosti i zasigurno će prije ili kasnije zaživjeti na globalnoj razini.

Svrha ovog završnog rada je kroz teorijski i praktični dio prikazati na koji način pametni ugovori mogu zamijeniti postojeće, zastarjele, centralizirane sustave posredovanja.

U prvom dijelu rada teoretski se razmatraju pametni ugovori od nastanka koncepta do uporabe u današnjem svijetu, objašnjeno je što su pametni ugovori te na koji način funkcioniraju. Istaknute su glavne prednosti pametnih ugovora, poput brzine, neovisnosti, pouzdanosti, nepogrešivosti i ekonomičnosti. Osim prednosti, navedeni su i glavni nedostaci, poput nedostatka regulacije, poteškoća implementacije i nemogućnosti mijenjanja pametnih ugovora. Posebno je objašnjena sigurnost pametnih ugovora, ono što je navedeno kao nedostatak, a to je nemogućnost mijenjanja pametnih ugovora, može se gledati i s pozitivne strane, s obzirom na to da nitko ne može utjecati na ugovore i proizvoljno ih mijenjati. Za lakše razumijevanje pametnih ugovora, rad objašnjava i tehnologiju izvođenja i decentralizirani sustav u kojem se ostvaruju pametni ugovori putem blockchain tehnologije, osim toga objašnjeni su pojmovi jednostavnog novčanika i rudarenja koje su usko vezano uz pametne ugovore.

U drugom dijelu opisane su najpoznatije platforme za pametne ugovore Ethereum Virtual Machine, EOS i NEO. Nakon opisa platformi opisuju se mogućnosti primjene pametnih ugovora koje su neograničene, ali fokus je stavljen na primjenu u bankarstvu, poreznom sustavu, opskrbnom lancu te zaštiti autorskih prava i intelektualnog vlasništva kao bitnim sustavima u današnjem svijetu.

Zadnji dio rada sadrži praktični primjer jednostavnog pametnog ugovora koji služi za ravnopravno dijeljenje sredstava između partnera. Za programiranje pametnog ugovora korištena je Ethereum platforma zbog njene globalne primjene i širokog spektra razvijenih alata za programiranje.

2. PAMETNI UGOVORI

2.1. Povijest pametnih ugovora

Koncept pametnih ugovora je opisao američki kriptograf i programer Nick Szabo 1996. godine, desetljeće prije nego što predstavljena je blockchain tehnologija. Prema Szabo-vom konceptu, pametni ugovori su digitalni protokoli za prijenos informacija koji koriste matematičke algoritme za automatsko izvršavanje transakcija nakon što se zadovoljeni određeni uvjeti. Ovaj koncept je bio ispred svog vremena jer je 1996. godine bilo nemoguće realizirati takvo nešto zbog nepostojanja potrebne tehnologije pooput distribuiranih struktura podataka (engl. *DLT*). Dolaskom Bitcoin-a 2008. godine, pojavljuje se prva kriptovaluta, sagrađena na temelju revolucionarne tehnologije blockchain-a. Blockchain je vrsta distribuiranih struktura podataka (engl. *DLT*), strukutura blockchaina i njegove mogućnosti su poslužile za razvoj pametnih ugovora kakve danas korisitimo. Pet godina kasnije, blockchain platforma Ethereum omogućila je korištenje pametnih ugovora u praksi. Današnje tržište nudi razne platforme za korištenje pametnih ugovora, ali Ethereum ostaje i dalje jedan od najraširenijih.[4]

2.2. Što su pametni ugovori i kako funkcioniraju

Pametni ugovori su stvoreni za sigurnu, transparentnu i lakšu razmjenu sredstava bez ikakve potrebe za posrednikom. Pametni ugovori predstavljaju programe koji su napisani da automatski kontroliraju prijenos sredstava između dvije ili više strana, nakon što budu zadovoljeni prethodno definirani uvjeti.

Upisani kod je glavna stvar i koncept svakog ugovora, to može biti bilo koji kod unutar blockchaina ako sadrži uvjet da može upravljati kriptovalutom, sredstvima ili imovinom. Značenje pametnog ugovora i karakteristike koda omogućuju automatsko izvršavanje predodređenog, osiguravajući nepovratnost i nepromjenjivosti.

Pametni ugovori omogućuju razmjenu novca, robe, nekretnina, vrijednosnih papira i druge imovine. Ugovori se pohranjuje i repliciraju u decentraliziranu struktura podataka u kojoj informacije se ne mogu krivotvoriti ili izbrisati. Istodobno, enkripcija podataka osigurava

anonimnost partnera u ugovoru. Važna značajka pametnog ugovora je da oni mogu funkcionirati samo s valutom koja je unutar njegovog digitalnog ekosustava, kako povezati virtualne i stvarne sfere ugovora jedan je od glavnih problema pametnih ugovora. To je razlog postojanja "oracle" posebnih programa koji pomažu računalnim protokolima da pribavljaju potrebne informacije iz stvarnog svijeta.[5]

Prednosti pametnih ugovora:

- Brzina - prerada dokumenata ručno koristi puno vremena i odgađa završetak ciljeva. Pametni ugovori pretpostavljaju automatizirani proces i u većini slučajeva ne zahtijevaju ljudsku uključenost što štedi dragocjeno vrijeme.

- Neovisnost - pametni ugovori isključuju mogućnost intervencije trećih strana, jamstvo za transakciju je sam program, čime ne postoji sumnja u integritet ugovora.
- Pouzdanost - podaci unešeni u Blockchain ne mogu se mijenjati ili izbrisati. Ako jedna strana u transakciji ne izvrši svoje obveze, druga će biti zaštićena uvjetima pametnog ugovora.
- Nema pogrešaka - automatizirani sustav za izvršavanje transakcija uklanja ljudski faktor i osigurava visoku točnost prilikom izvršavanja ugovora.
- Štednja - pametni ugovori pružaju značajnu uštedu zbog uklanjanja troškova posrednika i smanjenja operativnih troškova.

Nedostaci pametnih ugovora:

- Nedostatak regulacije - međunarodno pravno područje nema točno definirane koncepte blockchain-a, pametanih ugovora i kriptovaluta.
- Poteškoće implementacije - integracija pametnih ugovora s elementima iz stvarnoga svijeta traži puno vremena, novca i truda.
- Nemogućnost mijenjanja pametnog ugovora - Paradoksalno, jedna od glavnih prednosti pametnih ugovora, nemogućnost mjenjanja ugovora.

Pametni ugovori postoje u konceptu pravnih ugovora koji su sposobni poboljšati tradicionalne pravne ugovore, a sve je postignuto korištenjem pametnog koda. Kodovi koji se koriste u

ovakvom pametnom ugovoru još nisu zakonski prihvatljivi bez obzira što su u mogućnosti predvidjeti, pojednostaviti i učiniti stvari sigurnijima. Ovakav model još se mora dobro istražiti jer postoji strah od raznih strana da je ovakav kod previše sofiticiran i da bi se njime moglo manipulirati. Za to nema konkretnih dokaza jer je sama tehnologija još u razvitku, proučavanju i analiziranju.[12]

2.2.1. Sigurnost pametnih ugovora

Pametni ugovori koji su zapravo funkcije koje se izvršavaju u slučaju da ih pozove bilo korisnik ili program. Funkcije u pametnim ugovorima se čitaju s blockchaina ili zapisuju na blockchain uz određene uvjete. Funkcije u pametnim ugovorima se izvršavati pomoću „Ethereum Virtual Machine“ (engl. *EVM*) okoline na Ethereum platformi na kojoj je i najveći fokus u ovom završnom radu, te kada se jednom prenesu u blockchain, nemoguće ih je mijenjati.

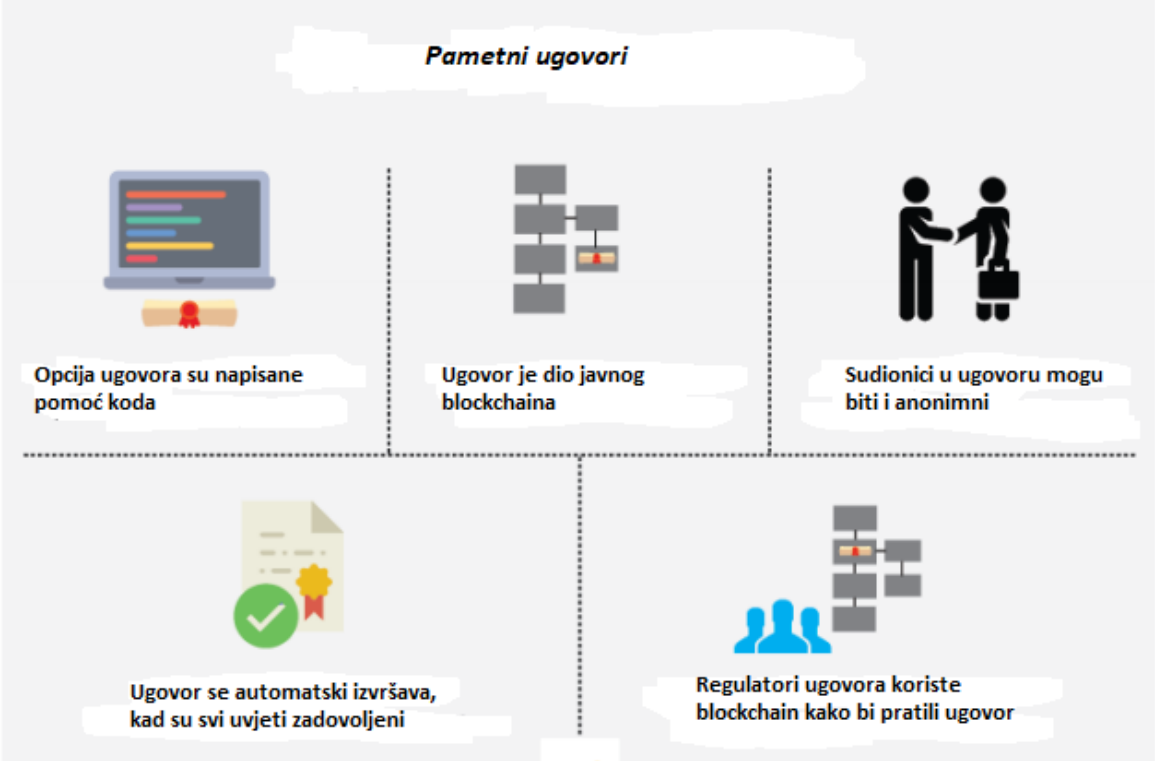
Slika 1. Pametni ugovor

Izvor: (https://www.securityartwork.es/2018/02/23/security-of-blockchain-based-smart-contracts-i/)

Kod pametnih ugovora sigurnost je na velikoj razini jer ih je nemoguće izmjeniti hakiranjem, jedino što može biti problem, ukoliko su određene funkcije nedovoljno dobro programirane, da dođe do propusta u njima samima, a to je onda nepromjenjivo niti sam vlasnik ugovora ih ne može mijenjati jer je to mehanizam blokchaina.

Sigurnosno gledano pametni ugovori jesu sigurni ali mogu postojati mogućnosti za određene probleme ukoliko nije sve isprogramirano u najboljem obliku. Postoje različite mogućnosti i različite situacije od kojih je jedna od tih da „napadač“ krajnjeg korisnika preusmjeri na pametni ugovor „napadača“ i tako stvori pogodnosti za sebe. Uz spomenutu situaciju postoji i situacija u kojoj je postavljena određena enkripcija koja je dodatno provaljena od strane „napadača“, a s ciljem dolaska do pravnih podataka i to u situaciji ukoliko odgovorna osoba za pametni ugovor ne plasira novu verziju, može imati neželjene posljedice. (Ostović, 2017/2018., 7.)

Slika 2. Životni cikulus pametnog ugovora



Izvor: (http://nevena.lss.hr/recordings/fer/predmeti/racfor/2018/seminari/kostovic/seminar.pdf)

2.3. Tehnologija izvođenja

Da bi se lakše razumjelo kako pametni ugovori funkcioniraju, prvo trebamo detaljnije objasnit šta je blockchain. Blockchain koncept je sličan bazi podataka u koju snimamo podatke. Većinom su to informacije koje se odnose na transakcije, ali to nije jedni slučaj korištenja. Možemo gledati na blockchain kao knjigu u koju zapisujemo ugovore i transakcije.

Lista digitalnih informacija podijeljena između svih čvorova (engl. *nodes*) koji su sastavni dio svakog blockchain, a on predstavlja strukturu podataka koja se distribuira.

Blockchain tehnologija nastala je za potrebe digitalne valute Bitcoin, no kasnije su potencijal te tehnologije prepoznale mnoge industrije, naročito financijski sektor. Bitcoin je korištenjem blockchaina i kriptografskih funkcija postigao sigurne transakcije digitalnog novca bez središnjeg autoriteta (banke). Ovdje blockchain igra ulogu glavne knjige u kojoj je zapisana svaka transakcija ikad izvršena u Bitcoin sustavu. (Hozjan, 2017., 9.)

U blockchain tehnologiji, dokumenti su međusobno povezani u blokove kako bi formirali lanac. Blockchain je povezana struktura podataka pomoću hash pokazivača čija tehnika proizlazi iz kriptografije. Kriptografija je grana za proučavanje tehnika za sigurnosnu komunikaciju. Općenito govoreći, kriptografija se odnosi na izgradnju i analizu protokola koji sprečavaju treću osobu ili javnost da čita privatne poruke. Suvremena kriptografija se temelji na matematičkoj teoriji i računalnoj praksi, kriptografski algoritmi su dizajnirani oko računalnih pretpostavki, čineći algoritme koje je teško dešifrirati u praksi. Hash funkcija je bilo koja funkcija koja se koristi za mapiranje podataka, bili oni proizvoljne veličini ili fiksne. Tako da možemo reći da sam blockchain nasljeđuje glavne karakterisitke od same kriptografije poput hash funkcija i hash pokazivača, a te značajke su:

- Bilo kakav unos ima samo jedan izlaz: hash.
- Izlaz je standardiziran: to jest fiksna veličina koja je općenito dosta velika da bi se osigurala otpornost od sudara.

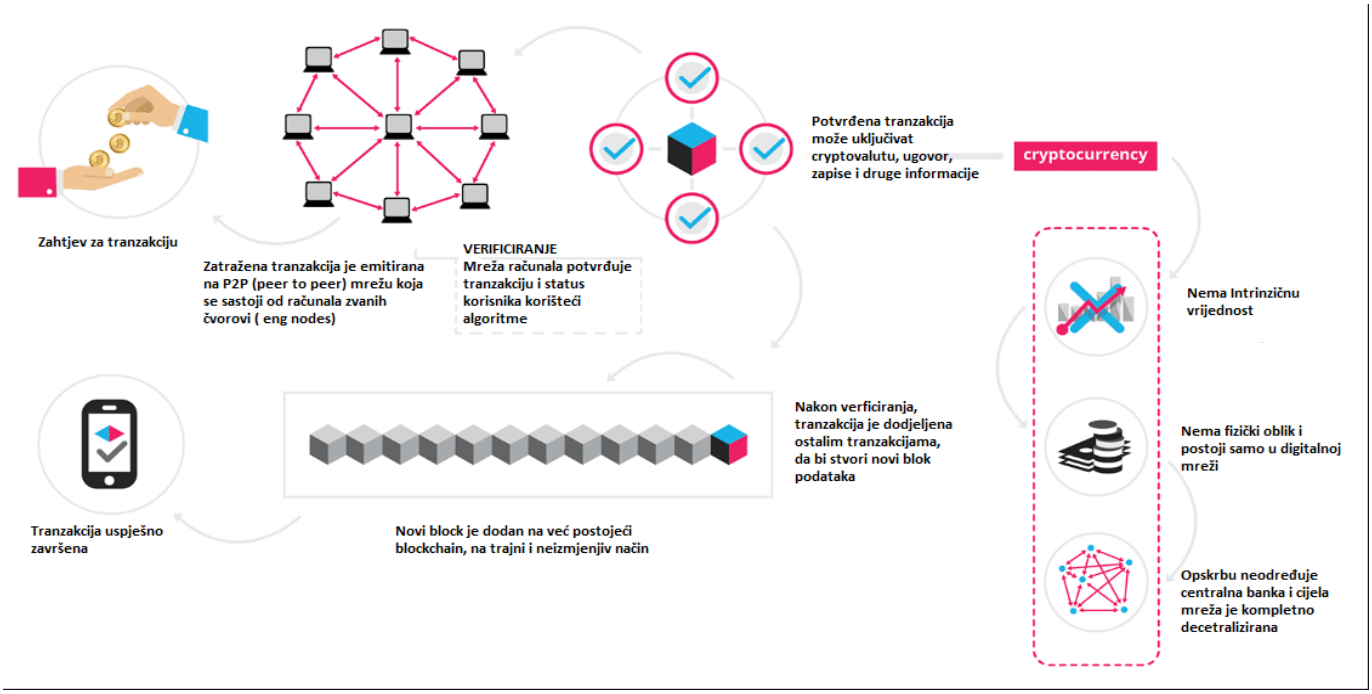
- Lako izračunavanje: možemo odrediti vrijeme potrebno za izračunavanje vrijednosti hash ulaza prema veličini unosa.

Gore navedene karakterisitke su jako bitne jer osiguravaju da svaka transakcija može biti šifrirana. Za svaku kreiranu transakciju, izlaz ima istu veličinu, a za svaku konkretnu transakciju možemo utvrditi računalno vrijeme tog hasha. Budući da je blockchain povezana struktura podataka koja sadrži podatke i hash pokazivače koji pokazuju na prethodne podatke. Tipično su to transakcije koje su međusobno povezane. Svaka transakcija koja se ikada dogodila je zabilježena u blockchainu i objavljena je. Gore navedene karakterisitke osiguravaju sigurnost tih transakcija. Kao što je prikazano tehnologija izvođenja vrlo je soficirana i poduzete su sve mjere sigurnosti kaka bi vlasništvo digitalnog novca bilo sigurno. S obzirom da je blockchain u ulozi glavne knjige koja registrira svaku transakciju, možemo reći da je centralni dio svih aktivnosti. Kako bi sve funkcioniralo moraju postojati određena pravila i regulative koje se manifestiraju kroz određene karakteristike.[6]

Blockchain ima slijedeće karakteristike:

- cijelokupni sustav funkcionira bez središnjeg glavnog dijela što znači da je decentraliziran
- kriptografija se koristi za sve važne stvari kao što su dokazivanje autentičnosti, u nekim situacijama korištenje prava pisanja i čitanja te i identifikacija sudionika u sustavu.
- čitanje podataka iz blockchaina mogu čvorovi sustava.
- u praksi se provodi ravnopravnost partnera što znači da svi partneri imaju jednaka prava i mogućnosti u sustavu koji koristi blockchain.
- mehanizam u blockchainu napravljen je tako da je nemoguće mijenjati podatke kada su jednom napravljeni, a u ekstremnim situacijama vrlo brzo pokazuje ukoliko je došlo do promjene.
- sve promjene, a u ovom se slučaju misli na zapise koji se u realnom vremenu, odmah se prosljeđuju kroz čvorove kojih ima puno.
- podatke u blockchain dodavati mogu čvorovi sustav.

Slika 3. Shema blockchain-a



Izvor: (https://blockgeeks.com/guides/what-is-blockchain-technology/)

2.4. Decentralizirani sustav

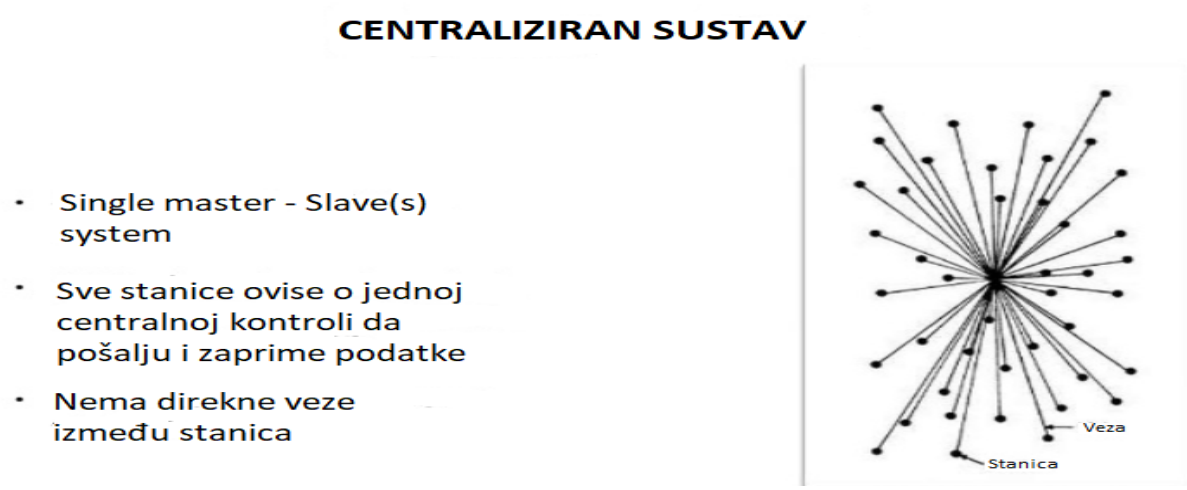
Većina digitalnih valuta je bazirana na decentraliziranom sustavu pomoću blockchain-a, jednako tako većina platformi za pametne ugovore koristi decetralizirani sustav kako bi valuta koju koriste imala veći integritet i veće povjerenje od strane korisnika.

Sustav ravnopravnih partnera, odnosno sustav građen prema modelu ravnopravnih partnera (engl. *peer-to-peer*) sastoji se od velikog broja istovrsnih procesa, takozvanih partnera. Partneri obavljaju zadaće prema potrebama svojih korisnika. Ako je partneru pri obavljanju neke zadaće potrebna pomoć on stupa u komunikaciju sa svojim susjedima, a ti susjedi sa svojim susjedima i tako se komunikacija odvija na razini cijelog sustava. (Hozjan, 2017., 16.)

Gore spomenuti sustavi mogu biti koncipirani na centralizirane i decentralizirane sustave. Centralizirani sustavi su sustavi koji imaju jedno mjesto s kojega se upravlja cijelim sustavom. Dok decentralizirani sustavi imaju mogućnost samostalnog rada kao podsustav unutar velikog sustava.

U ovom slučaju to bi značilo da u Centraliziranom sustavu postoji poslužitelj koji ima za funkciju povezivanja klijenata kako bi oni bili u vezi i kako bi mogli međusobno komunicirati.

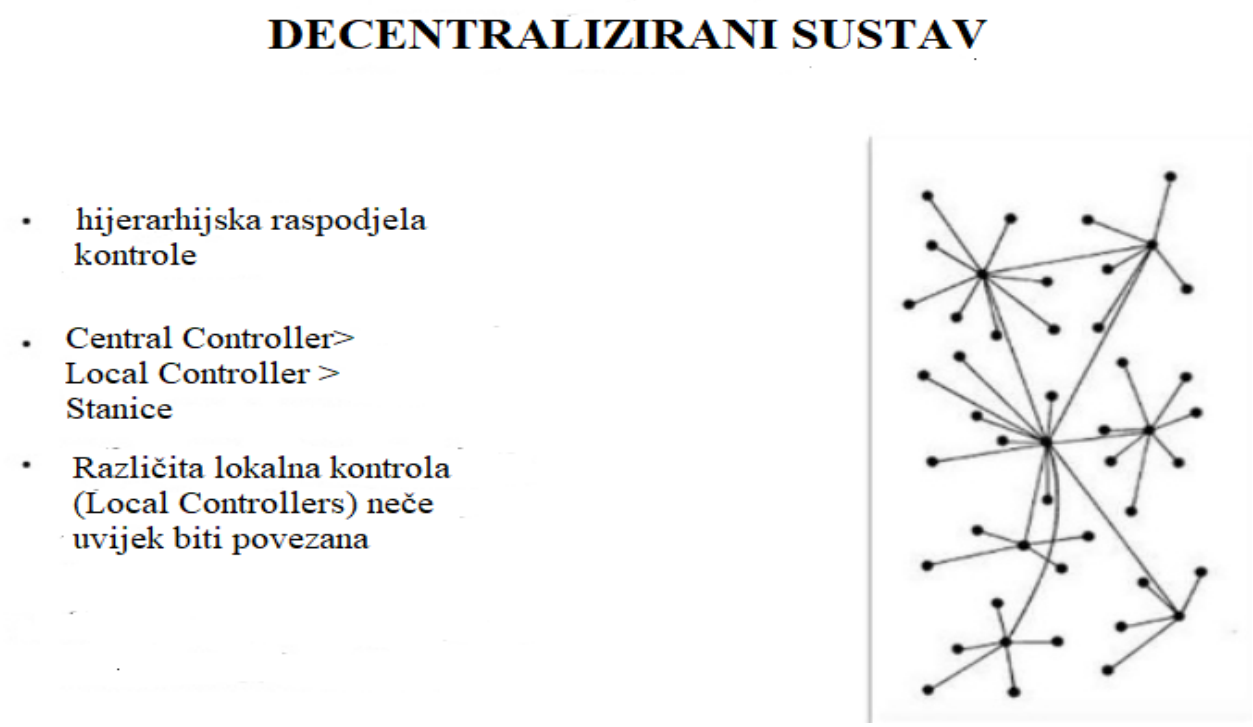
Slika 2. Arhitektura cetraliziranog sustava



Izvor: (https://www.slideshare.net/kcajnas/centralized-decentralized-discrete-control-systems)

Dok u decentraliziranom sustavu situacija je nešto drugačija što znači da u ovom sustavu nema određenog, glavnog poslužitelja što skračuje komunikaciju, ubrzava je i pojednostavljuje.

Slika 5. Arhitektura decetraliziranog sustava



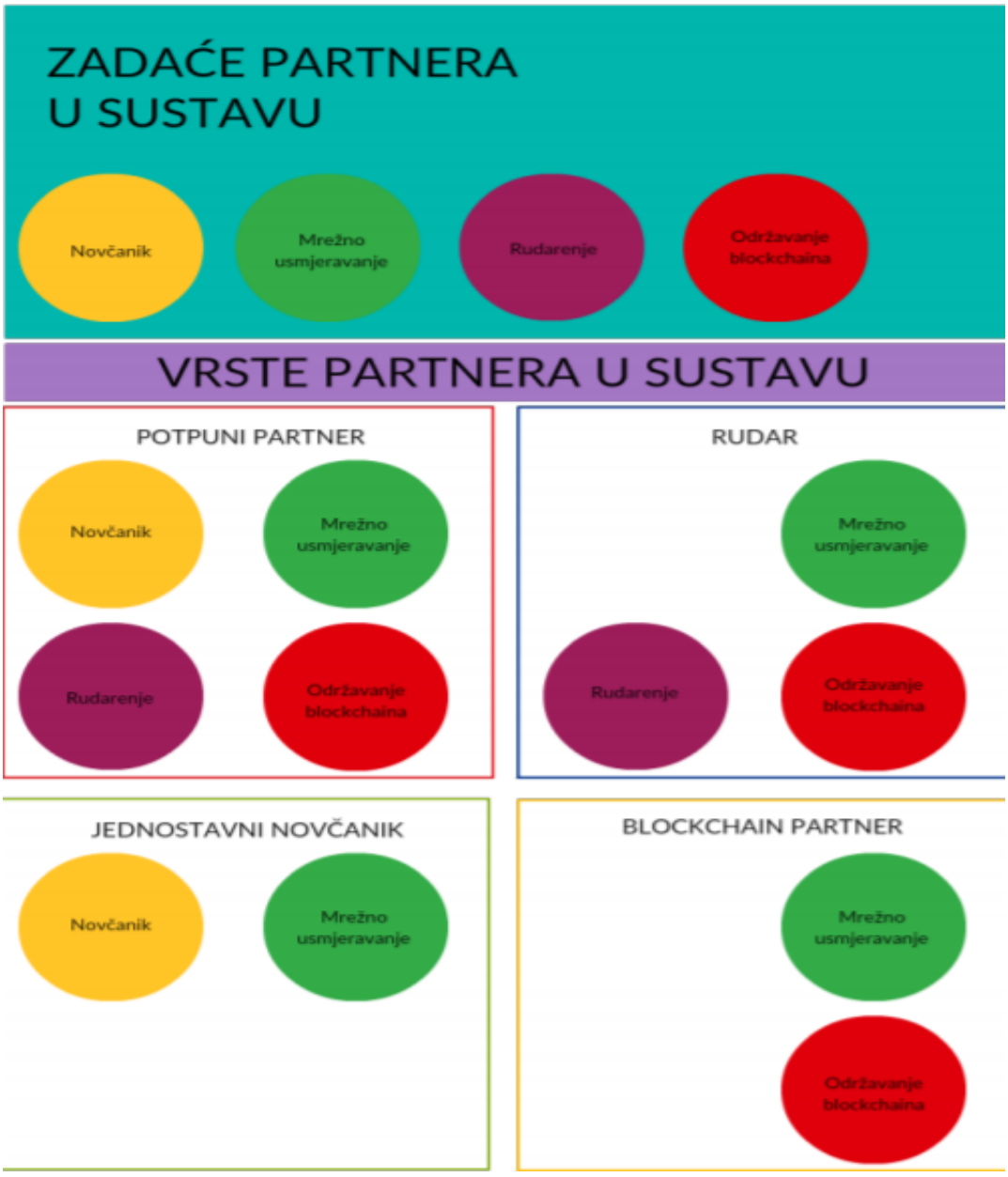
Izvor: (https://www.slideshare.net/kcajnas/centralized-decentralized-discrete-control-systems)

Sustavi koji koriste blockchain tehnologiju spadaju većinom u decentralizirane sustave ravnopravnih partnera. Time je omogućena razmjenu podataka kroz računalnu mrežu pri kojem stanice (engl. *Nodes*) preuzimaju informacije jedni od drugih umjesto s jednog centralnog poslužitelja. Općenito, sustav ravnopravnih partnera pruža najbolji i najjeftiniji način da veliki broj korisnika dođe do neke datoteke, a troškovi takve komunikacije postaju relativno mali i dijele se među korisnicima. (Hozjan, 2017., 16.)

U većini blockchain sustava postoje raspodjela poslova između partnera koji imaju određene zadaće. Svaki partner može raditi četiri zadaće od kojih su to slijedeće: network routing (mrežno usmjeravanje), održavanje cijelog blockchain-a, wallet (novčanik) i mining (rudarenje). Obavljanje poslova i zadataka razlikuju se u javnim i privatnim sektorima. Javni sustavi imaju

raspoređen rad na način da su partneri razlikovani na temelju zadataka koje obavljaju, a oni su razlikovani prema slijedećem: rudar, blockchain partner, potpuni partner i jednostavni novčanik. U privatnom sektoru blockchain sustava svaki partner zadužen je za sve zadaće kojih ima četiri.[6]

Slika 6. Zadaće i vrste partnera u sustavu



Izvor: (https://repozitorij.pmf.unizg.hr/islandora/object/pmf%3A779/datastream/PDF/view)

Slika broj 6. prikazuje partnere i njihov način na koji oni izvršavaju svoje zadaće za mrežno usmjeravanje. Do toga dolazi jer svaki partneri ima potrebu za održavanjem i stvaranjem veza s jednim ili više ravnopravnih partnera, jer tako je cijeli model koncipuiran. Svi partneri koji su sudionici sustava isto tako imaju obvezu za difuziju (engl. *Broadcast*) i validiranje novih blokova i novih zapisa.

2.4.1. Blockchain partner

Blockchain partner održava blockchain sa svim zapisima, počevši od prvog bloka koji se naziva generički blok na koji se nadovezuju svi ostali blokovi sve do zadnjeg kreiranog. Za razliku od jednostavnog novčanika blockchain partner nema potrebe za oslanjanjem na ostale partnere u svrhu pretraživanja blockchaina ili provjere integriteta podataka. (Hozjan, 2017., 18.)

Kada se radi o transakcijskom zapisu blockchain-a, u svrhu validacije blockchain partner može u svakom trenutku vidjeti i provijeriti jesu li sredstva o kojima se govori baš od tog korisnika koji ga želi potrošiti. Takve stvari mogu se vidjeti na način da se nova transakcija poveže sa starom transakcijom i to sve do bloka koji je generički. Kako bi u stvarnom vremenu primio novokreirane dijelove koje nakon toga nadovezuje na svoju lokalnu kopiju blockchain-a, nakon verificiranja. Ovakav partner se oslanja na ostatak mreže kako bi zaprimio novo kreirane blokove.

2.4.2. Jednostavni novčanik

U javnim sustavima koji koriste blockchain zbog velike količine podataka svaki korisnik nema mogućnost pohraniti cijeli blockchain. Takav korisnik tada u sustavu sudjeluje kao jednostavan novčanik i na slici 6 prepoznajemo ga po tome što u svojim zadaćama nema crveni krug pod nazivom održavanje blockchain-a. Glavna zadaća koju jednostavni novčanik obavlja je kreiranje novih zapisa u skladu s protokolom koji propisuje sustav. (Hozjan, 2017, 18.)

Kako bi sigurnost bila na nivou i kako se vlasnici ne bi brinuli za svoju imovinu novčanici pospremaju parove privatnih i javnih kriptografskih ključeva, a sve u cilju vlasništva nad digitalnim novcem ili nekom drugom digitalnom informacijom s ciljem zaštite intergriteta na blockchainu. Analogno broju računa u banci iz javnog se ključa skuplja adresa koja služi za

primanje novca od ostalih korisnika. Ovakav način može se dobro usporediti sa zaporkom računa u banci i s osobnim identifikacijskim brojem kao što su JMBG i OIB, te se nikako ne preporuča dijeti te informacije kao što se dijeli adresa.

Jednostavni novčanik provodi takozvani jednostavan način verificiranja jer sam ne sadrži zapis o svim prethodnim transakcijama. Jednostavna metoda verificiranja podrazumijeva pohranjivanje samo zaglavlja blokova umjesto cijelog blockchaina koji sadrži sve zapise. Budući da nemaju punu sliku svih transakcija koje su se dogodile prije one koju žele validirati, oslanjaju se na ostale partnere koji im na njihov zahtjev pružaju uvid u dio blockchaina za određenu transakciju. (Hozjan, 2017, 19.)

2.4.3. Rudar

Partneri rudari preuzimaju nove zapise koje su kreirali novčanici, formiraju ih u blokove i dodaju u blockchain. U blockchain protokolu dodavanje novih zapisa iziskuje korištenje računalnih resursa. Kada rudar pronađe blok u blockchain-u, rješavajući algoritam pod nazivom "proof-of-work" i koristeći svoje računalne resurse, tada sve transakcije u tom bloku postaju potvrđene i zapisuju se u blockchain, a rudar kao nagradu za korištenje svojih računalnih resursa dobiva određeni broj digitalne valute za svoj doprinos mreži. Povećanjem broja rudara koji sudjeluju u mreži, povećava se i sigurnost same mreže. Veći broj rudara omogućuje više različitih lokacija, na kojim se može zapisat blok u blockchainu i nikad se ne zna koji rudar će pronaći blok i zapisat ga. Time se postiže velika sigurnost, jer se ne zna lokacija zapisa i samim time ne može se utjecati na nju. (Hozjan, 2017., 20.)

3. PLATFORME ZA PAMETNE UGOVORE

Danas postoje mnoge platforme za pametne ugovore. Spomenut ćemo tri najpoznatije i njihove glavne karakterisitke, a to su: NEO (NeoVM), EOS i Ethereum Virtual Machine (EVM). Više pozornosti biti će pridano Ethereum-u kao najpozanatijoj platformi za pametne ugovore i u njemu će biti isprogramiran pametni ugovor kao praktični dio ovoga rada.

3.1.1 Ethereum Virtual Machine (EVM)

Ethereum je decentralizirana platforma koja je najjača mreža za stvaranje Pametnih ugovora i decentraliziranih aplikacija (engl. *dApps*). Vitalik Buterin programer i istraživač kriptovalute predstavio je Ethereum krajem 2013. godine. Razvoj platforme je financiran putem online "crowdsalea" koji se odvijao od srpnja do kolovoza 2014. godine. Poput ostalih platformi na blockchainu, Ethereum platforma treba veliku količinu ljudi koji će pokrenut softver na svojim računalima za napajanje mreže. Svaka stanica (računalo) u mreži pokreće program naziva Ethereum Virtual Machine (EVM) koji je poput operacijskog sustava koji razumije i izvršava programe napisane u Ethereum programskom jeziku imena Solidity. Programe koje izvršava EVM nazivamo pametnim ugovorima. Kako bi se određeni kod ili ugovor izvršio na platformi, morate platiti određenu cijenu za njegovu uslugu. Međutim, ne plaćate je u redovnoj valuti kao što su dolari ili slično. Umjesto toga, sve mora biti plaćeno s kriptovalutom koja je standradna u toj mrežnoj infrastrukturi, u ovom slučaju je to ETHER. Korisnici i pametni ugovori se smatraju jednakima na Ethereum platformi i imaju ista prava, tj. bilo što korisnik napravi na mreži isto to može i pametan ugovor. Za svaki ugovor, korisnici će moraju potrošiti određenu količinu Ethera. Količina koju je potrebo platiti za poziv ugovora ili njegovu objavu određuje se na temelju količine posla koju Ethereum platforma treba napraviti kako bi izvršila ugovor. Za izračunavanje cijena pametnih ugovora, svaka radnja ima određenu cijenu. Na primjer, ako napravimo zahtjev koji koristi memoriju stanice, taj zahtjev ima određeni trošak, ukoliko izvršimo zahtjev koji koristi tvrdi disk na stanici, ta vrsta zahtjeva ima isto određeni trošak koji joj je pridružen. Prilikom stvaranja pametnog ugovora, možemo odrediti maksimalnu cijenu za plaćanje usluga

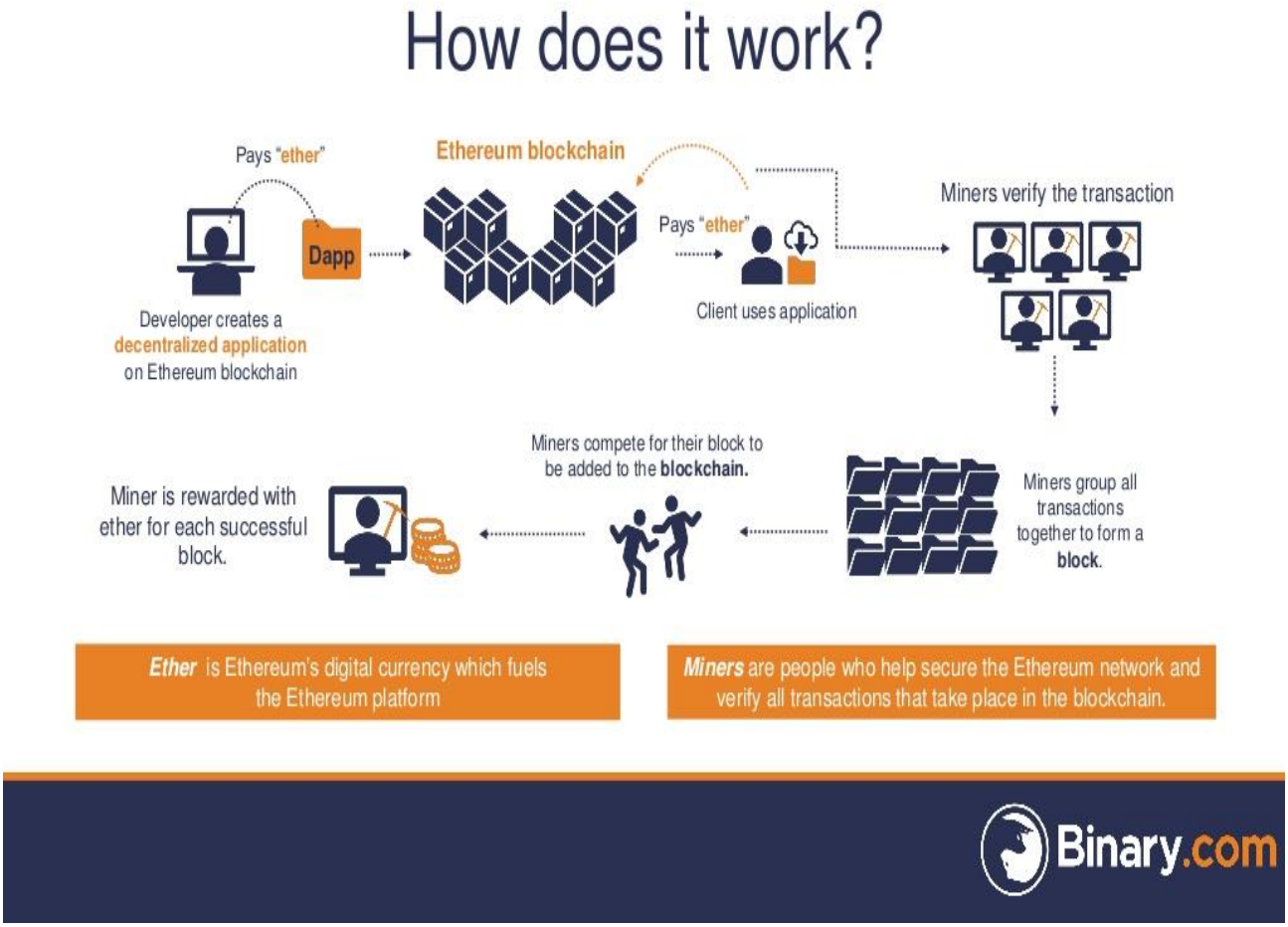
koji ćemo izvršiti. Izvršavanje će se zaustaviti, kada taj zahtjev bude izvršen ili kada je dosegnuta maksimalna cijena za tu uslugu, to je zamišljeno kako bi se izbjegle beskonačne petlje u pametnim ugovorima. Takve situacije nastaju zbog nedovoljno kvalitetno isprogramiranih ugovora. Svakim sljedećim ponavljanjem ponovno se plaća cijena za određenu uslugu i time beskonačna petlja ima kraj. Nema smisla da stanica beskonačno izvršava određenu radnju zbog pogreške programera. Koncept plaćanja za određenu uslugu rješava taj problem. [5,9,10]

Slika 7. Ethereum paltforma

Izvor: (http://list.wiki/Ethereum_(ETH))

Vrijednost samog Ethera je porasla za 13.000% u 2017. godini što je dovoljan pokazatelj za zainteresiranost korisnika za ovu platformu i njezinu svrhu.

Slika 8. Prikaz mreže

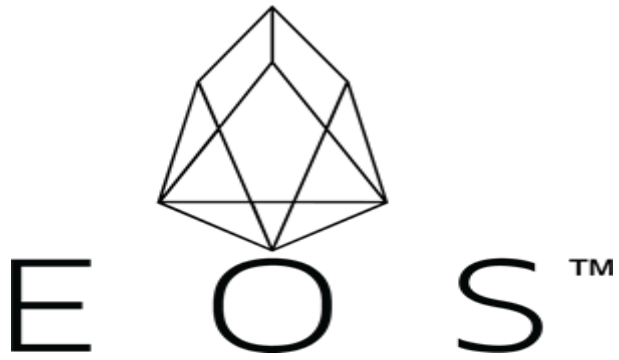


Izvor: (https://www.slideshare.net/cordieliea/binarycom-what-is-ethereum-and-how-does-it-work)

3.1.2 EOS

EOS je još jedna Blockchain platforma koja je trenutno u razvoju i naglašava funkcionalnost pametnih ugovora. Ona koristi Web Assembly (WASM) za izvršavanje pametnih ugovora i C++ te se očekuje da će biti jedan od najbolji jezika za razvoj ugovora. Ugovorne funkcije rade slično onima unutar Ethereum mreže, ali ipak postoje neke značajne razlike među njima. Cilj EOS-a je izgradnja decentraliziranog blockchaina koji može obraditi brzu i besplatnu transakciju. Također će omogućiti izgradnju pametnih ugovora i pružiti podršku za decentralizirane aplikacije (engl. *dApps*). EOS želi izgraditi platformu koja funkcionira poput operacijskog sustava, čime bi njegova upotreba bila znatno olakšana. EOS development tim sadrži iskusne članove iz blockchain tehnologije, uključujući i Daniel Larimer, koji je suosnivač kompanija BitShares i Steem. Larimer-ovi blockchain projekti sada vrijedi milijarde dolara. EOS platforma je prije 3 mjeseca izbacila glavnu mrežu (engl. *mainNET*) s dosta propusta i trenutno je u fazi nadogradnje i izmjene propusta u glavnoj mreži (engl. *mainNET*).

Slika 9. EOS platforma



Izvor: (https://seeklogo.com/vector-logo/322892/eos)

Tehologija koju koristi EOS je Graphene tehnologija s obzirom na to da ona ima sposobnost obrade velikog broja transakcije, a što se kreće od 10.000 do 100.000 tisuća. Kako bi EOS proširio mrežu za još veći broj tranzakcija koristit će mogućnost paralelnosti koje će omogućiti da EOS bude vrlo jednostavan za skalabilnost, čineći ga komercijalno vrlo održivom platformom za pametne ugovore. [5]

3.1.3 NEO (Neo VM)

NEO je nadolazeća kineska Blockchain platforma koja se može koristiti za stvaranje pametnih ugovora i razvijanje kriptovaluta. Ugovori su vrlo slični onima korištenim na Ethereumu. Vjeruje se da NEO ima višu razinu izvedbe u optimalnim okolnostima te da je fleksibilniji od Ethereuma.

Slika 10. NEO platforme

Izvor: (https://news.coinsquare.com/digital-currency/neo-blockchain/)

Programski jezik koji koristi zove se Solidity Neo ima mogućnost razvojnim programerima dati mogućnost kreiranje ugovora putem raznih programskih jezika kao što su: VB.Net, Python, C #, F # i Kotlin. Isto tako radi se i na dodatku novih jezika kao što su: C ++, Golang, C, i JavaScripta. Uz podršku za više jezika, više od 90% programera može izravno sudjelovati u razvoju NEO pametnog ugovora bez ikakve potrebe za učenjem novog jezika, čak postoji mogućnost prenjeti kod već postojećeg poslovnog sustava izravno na blockchain. Predviđa se da će to uvelike povećati ukupnu popularnost same platforme. Solidity Neo ima puno veće mogućnosti u odnosu na Etherium jer jedino on daje mogućnost razvijanja putem svog jezika. S obzirom na sve okolnosti NEO ima veliku perspektivu bez obzira što je na samom početku razvijanja i još uvijek nema objavljnu glavnu mrežu (engl. *MainNET*) može predvidjeti probleme ostalih platformi i unaprijed ispalnirati svoj razvoj da tijekom vremena postane vodeći na tržištu razvoja pametnih ugovora. [5]

3.2. Mogućnosti primjene pametnih ugovora

Temeljni način funkcioniranja pametnih ugovora je taj da se određena zamišljena ili dogovorena pravila u nekom programskom jeziku kodiraju i nakon toga se zapisuju na blockchain. Ukoliko se nešto želi promijenti naknadno, to više nije moguće, pri ispunjenju određenih pravila dolazi do aktiviranja pametnih ugovora. Iako postoji mnoštvo mogućnosti, navest ćemo samo nekoliko primjera gdje pametni ugovori i sama blockchain tehnologija mogu uveliko poboljšati poslovanje.

3.2.1. Bankarstvo

Tijekom izvršavanja prijenosa sredstva s jednog računa na drugi. Obavezno se mora platiti naknada koja iznosi određeni postotak sredstva koja se prenose, a zatim moramo čekati nekoliko dana dok se ta transakcija ne obradi. Iako moderni bankarski sustav trenutačno funkcionira ovakvo kako je, teško je ne primjetiti njegove mane.

Pametni ugovori sami po sebi ne zahtijevaju potrebu za posrednikom. Dakle, ne plaća se skoro nikakva naknada za obične transakcije. Budući da ne postoji birokracija, transakcije postaju veoma brze i jeftine. Štoviše, transparentnost koju obezbjeđuje blockchain smanjuje moguće rizike od prijevara.

3.2.2. Porezni zapisi

Sama prijava poreza u poreznu službu zahtjeva veliku količinu potrebnih dokumenata. Npr. Uzevši u obzir da porezna služba ima određeno radno vrijeme, može imati i nedovoljan broj radnika u potrebnom trenutku. Veliki broj ljudi koji su prijavili porez moraju čekati dok sve informacije prođu kroz sustav, tako da je porezni sustav vrlo spor i neefikasan.

Pametni ugovori omogućuju automatsko plaćanje i dostavljanje informacija koji bi ubrzali i poboljšali cijeli proces, istodobno, svi podaci o porezima bi se bilježili na Blockchain i dostupni svima za provjeru. Transparentnost poreznih evidencija čini varanje unutar sustava gotovo nemogućim.

3.2.3 Opskrbni lanac

Tijekom obične kupnje namirnica u trgovini kupac bi koristeći blockchain tehnologiju mogao vidjeti porijeklo proizvoda i vrijeme proizvodnje. Uzmimo za primjer voće za koje kupci ne mogu točno znati koliko je staro ili odakle je proizvod, jedina opcija je vjerovati onome što piše na deklaraciji. Pametni ugovori kombinirani s elektroničkim uređajima, koji su stalno povezani s internetom, uskoro će napraviti revoluciju u logistici i opskrbnom lancu. Pomoću tih uređaja koji svako skeniranje odmah proslijeđuju na blockchain, praćenje samog proizvoda postaje automatsko i transparentno. U bilo kojem trenutku možete znati gdje se roba nalazi, i u kakvim uvjetima se nalazi. Ista tehnologija može se koristiti za praćenje maloprodajne robe, ugljena, nafte, zlata itd. Zahvaljujući blockchainu, dobavljači postaju vjerodostojniji i rizici od prijevara drastično opadaju.

3.2.4 Autorska prava i zaštita intelektualnog vlasništva

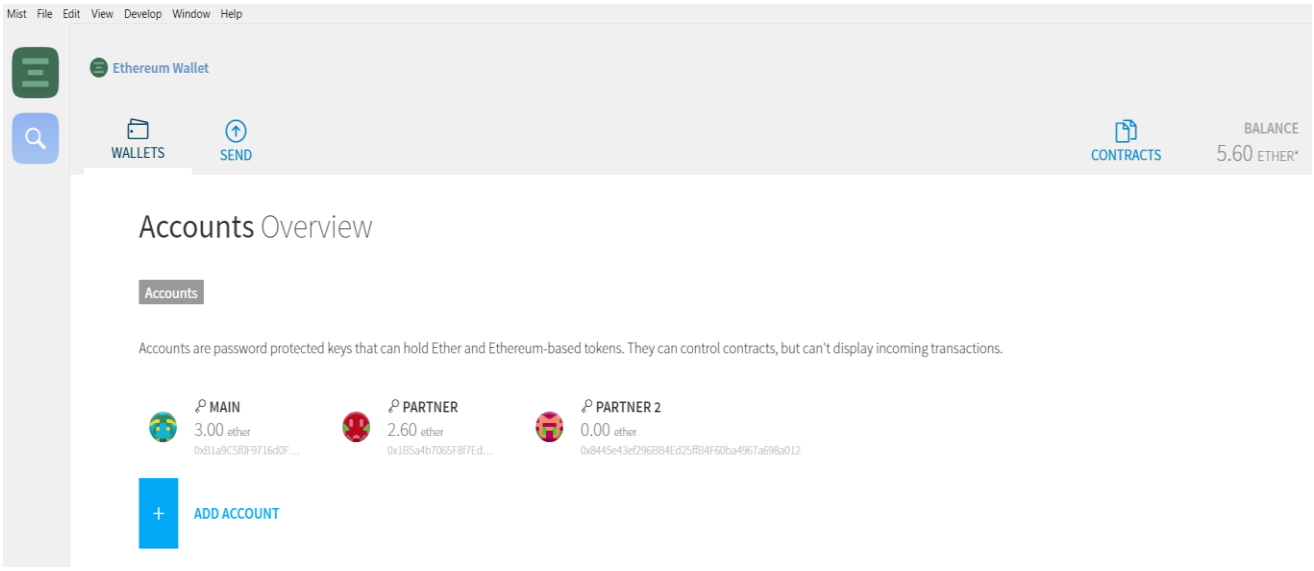
Veliki problem današnje zabavne industrije je piratstvo i kršenje autorskih prava. Glazbenici, fotografi, pisci i drugi umjetnici lišeni su autorskih naknada zbog nepoštivanja njihovih autorskih prava ili intelektualnog vlasništva. Izrada transparentnog registra za autorska djela na blockchainu je veoma odličan i ambiciozan primjer kako pametni ugovori mogu poboljšati trenutno stanje u industriji. Na primjer, kad god netko preuzme nečiji roman, fotografiju ili pjesmu i ta osoba bi automatski dobivala svoju naknadu. Time su prava autora registrirana na veoma siguran, javan, transparentan način i nitko nema mogućnost izmjene ili otuđivanja prava.

Nije teško prepostaviti da su mogućnosti korištenja pametnih ugovora gotovo neograničene. S obzirom na navedeno, može se vidjeti kako pametni ugovori i blockchain tehnologija mogu ubrzati procese i istodobno ih učiniti sigurnijim i transparetnijim od trenutnih rješenja. Svaki ugovor je napisan od strane programera, stoga se ne može isključit ljudski faktor pogrešaka i zbog toga nemožemo reći da su ugovori 100%-tno sigurno rješenje. Uostalom, svatko zna da nije lako promijeniti svijet i revolucionalizirati ga. Pred inženjerima blockchiana i programerima u pametnim ugovorima je još mnogo posla i trebat će još vremena da se tehnologija implementira i da se globalno počnu cijeniti i koristiti sve mogućnosti koje sustav pruža.

4. IZRADA UGOVORA

U praktičnom dijelu je isprogramiran jednostavan pametan ugovor za ravnopravno dijeljenje sredstva između partnera. Neovisno koliko je partnera upisano u ugovoru to jest njihove osobne adrese novčanika (engl. *Wallet*) dok se sam ugovor programira i još nije objavljen na mrežu. Npr. Dva partnera su uključena u ugovor i svatko ima pravo na povlačenje 1/2 svih uplaćenih sredstva sa adrese ugovora. Bilo koji partner odlaskom na adresu ugovora ima mogućnost funkcije „withdraw“ gdje određuje koji iznos želi povući, naravno ne može preći 1/2 svih uplaćenih sredstava. Sam ugovor ima podatak koji je vidljiv svima korisnicima „totalInput“ koji zbaraja sve uplate na ovu adresu ugovora. Ugovor omogućuje partnerima veću razinu povjerenja jer nitko od njih ne upravlja ugovorom i ne može ga izmjeniti niti u jednom trenutku, ne plaća se posrednik za upravljanjem sredstvima, blockchain tehnologija sama po sebi pruža najveću razinu sigurnosti i transparetnosti. Prvi korak je odabrat platformu za pametne ugovore. Za praktični primjer je odabrana Ethereum platforma radi njene najveće globalne primjene i najviše razvijenih alata za programiranje. Ethereum platforma ima dvije testne mreže imena „Ropsten “ i „Rinkeby“, za objavu ugovora odabrana je „Rinkeby“ mreža. Drugi korak je instalirati novčanik (engl. *Wallet*). Odabarani novčanik je imena Mist koji sadrži napredne opcije poput odabira mreže za radno okruženje, stvaranje više korisničkih novčanika na jednom računalu radi lakšeg testiranja ugovora i još nekoliko naprednih mogućnosti.

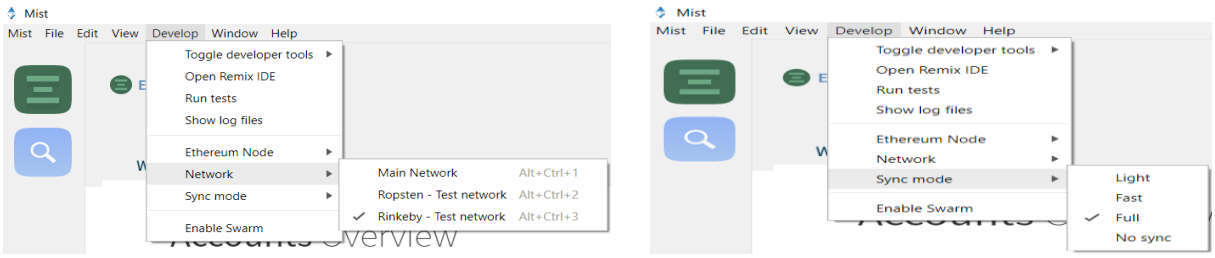
Slika 11. Prikaz glavnog sučelja u Mistu i prikaz svih aktivnih novčanika na jednom računu



Izvor: Autor

Nakon instaliranja mist-a potrebno je u padajućem izborniku imena „develop " odabrati željenu mrežu na koju se želimo spojiti. Nakon toga u istom izborniku odabrati opciju „Full sync" koja će preuzeti cijeli blockchain na naše računalo, jer potreban je cijeli blockchain za pravilno testiranje ugovora.

Slika 12. Podešavanje Mista za Rinkeby mrežu

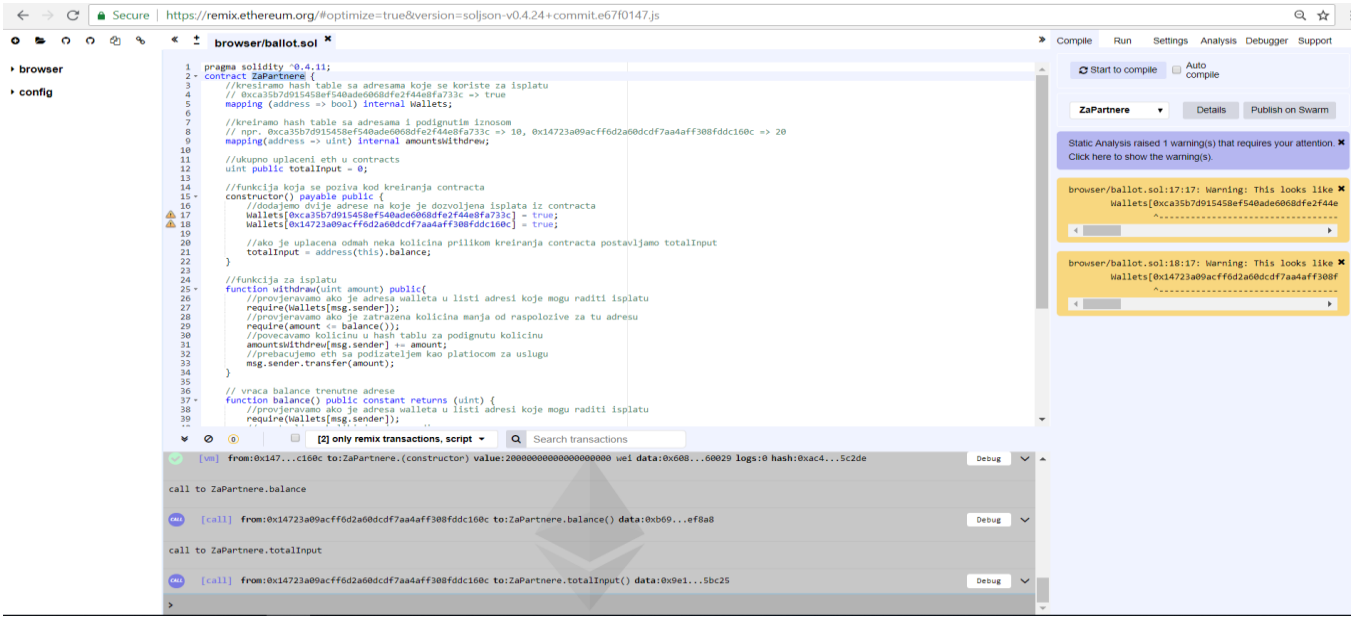


Izvor: Autor

Treći korak je isprogramirati sam ugovor i testirati ga u privatnom okruženju prije objave na mrežu. Programiranje i testiranje ćemo radit u IDE imena „Remix" koji je u web obliku na adresi

https://remix.ethereum.org/. Integrirano razvojno okruženje (engl. *IDE*) je softverski paket koji sadrži osnovne alate koji su potrebni programeru za pisanje i testiranje softvera. Uobičajeno, IDE sadrži uređivač koda, compiler, interpreter i program za ispravljanje pogrešaka i to sve putem jednog grafičkog korisničkog sučelja (engl. *GUI*).

Slika 13. Remix IDE



Izvor: Autor

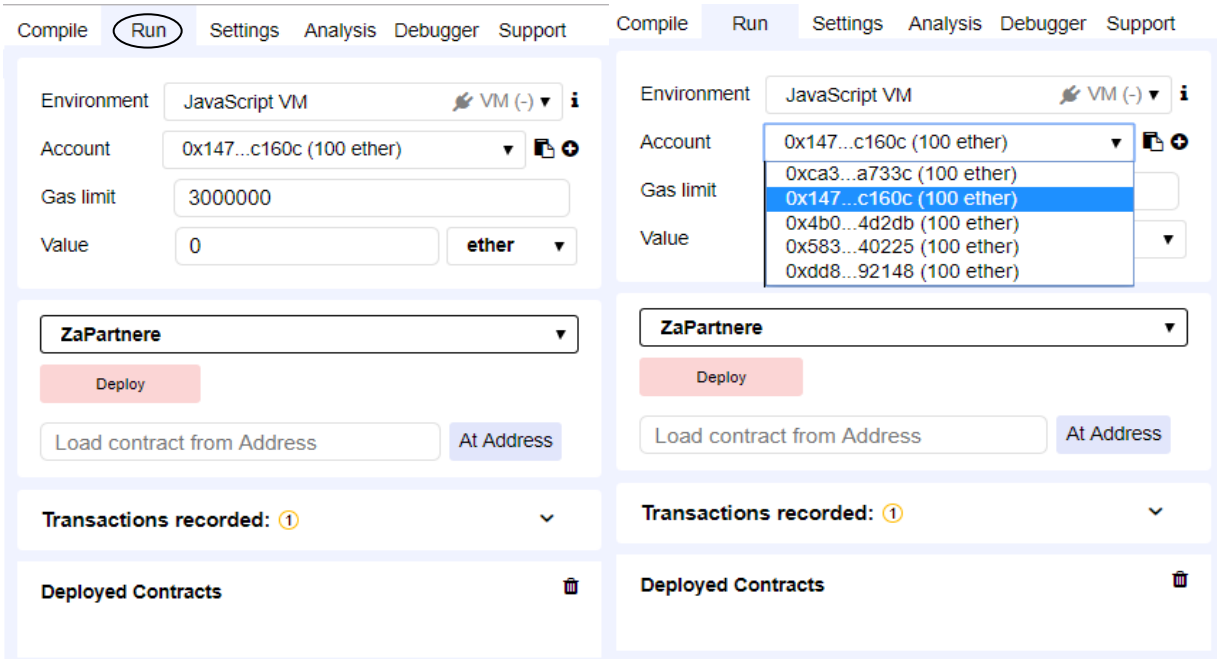
Slika 14. Izkomentirana svaka linija koda za shvaćanje logike programiranja samog ugovora

```
pragma solidity ^0.4.11;
contract ZaPartnere {
    //kresiramo hash table sa adresama koje se koriste za isplatu
    // 0xca35b7d915458ef540ade6068dfe2f44e8fa733c => true
    mapping (address => bool) internal Wallets;

    //kreiramo hash table sa adresama i podignutim iznosom
    // npr. 0xca35b7d915458ef540ade6068dfe2f44e8fa733c => 10, 0x14723a09acff6d2a60dcdf7aa4aff308fddc160c => 20
    mapping(address => uint) internal amountsWithdrew;

    //ukupno uplaceni eth u contracts
    uint public totalInput = 0;

    //funkcija koja se poziva kod kreiranja contracta
    constructor() payable public {
        //dodajemo dvije adrese na koje je dozvoljena isplata iz contracta
        Wallets[0xca35b7d915458ef540ade6068dfe2f44e8fa733c] = true;
        Wallets[0x14723a09acff6d2a60dcdf7aa4aff308fddc160c] = true;

        //ako je uplacena odmah neka kolicina prilikom kreiranja contracta postavljamo totalInput
        totalInput = address(this).balance;
    }

    //funkcija za isplatu
    function withdraw(uint amount) public{
        //provjeravamo ako je adresa walleta u listi adresi koje mogu raditi isplatu
        require(Wallets[msg.sender]);
        //provjeravamo ako je zatrazena kolicina manja od raspolozive za tu adresu
        require(amount <= balance());
        //povecavamo kolicinu u hash tablu za podignutu kolicinu
        amountsWithdrew[msg.sender] += amount;
        //prebacujemo eth sa podizateljem kao platiocom za uslugu
        msg.sender.transfer(amount);
    }

    // vraca balance trenutne adrese
    function balance() public constant returns (uint) {
        //provjeravamo ako je adresa walleta u listi adresi koje mogu raditi isplatu
        require(Wallets[msg.sender]);
        // postavljamo koliki je njegov udio
        uint share = totalInput / 2;
        // udio umanjujemo za vec podignutu kolicinu kako bi dobili raspolozivu kolicinu
        uint available = share - amountsWithdrew[msg.sender];

        //provjeravamo da je raspoloziva kolicina veca od 0, i manja od udjela
        require(available >= 0 && available <= share);
        //vracamo raspolozivu kolicinu
        return available;
    }

    //constructor koji se poziva kada netko uplacuje eth u contract
    function() payable public {
        //povecavamo kolicinu eth u contractu
        totalInput += msg.value;
    }
}
```


Izvor: Autor

Nakon gotovog programiranja koje je izkomentirano u slici 14. Remix nam pruža mogućnost lokalnog testiranja prije nego objavimo sam ugovor na mreži. Njemu pristupamo u gornjem desnom kutu pod opcijom „Run“, gdje simuliramo lokalni blockchain s jednim blokom, pošto je lokano izveden nema potrebe za verifikaciju podataka i čini posupak za testiranje ugovora puno jednostavnjim i bržim. U Lokalnom okruženju imamo mogućnost testiranja s pet adresa ili korisnika, gdje možemo objaviti sam ugovor i poslat mu željenu količinu ethera i testirat lokalno svakog korisnika s ugovorom.

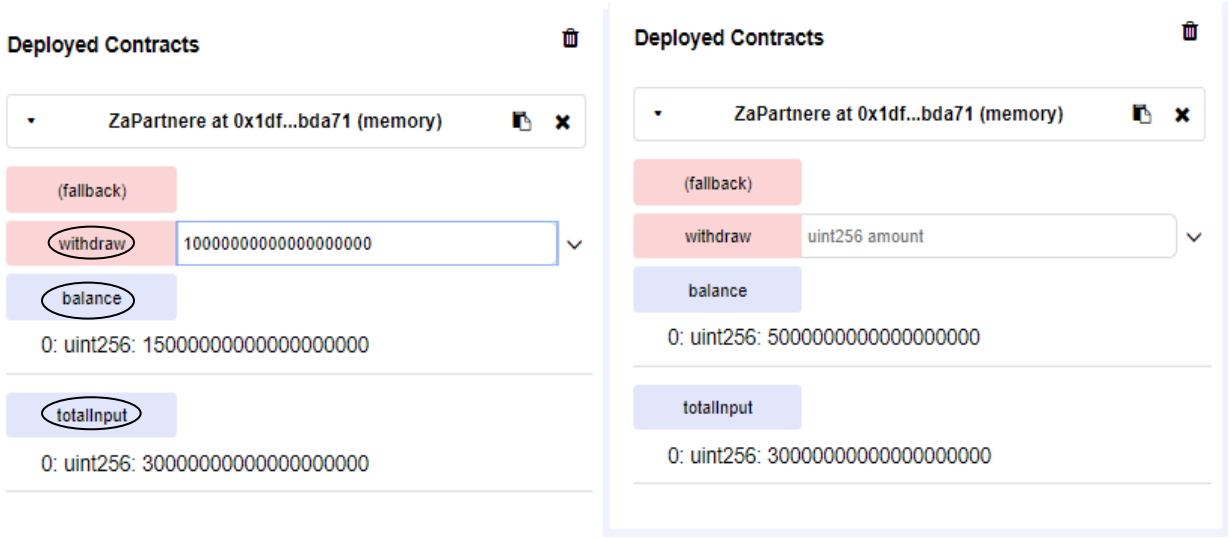
Slika 15. Remix IDE testiranje ugovora



Izvor: Autor

Ugovor se objavljuje pod opcijom „Deploy“ .Nakon objave svaki partner koji je upisan u ugovor ima pravo povući svoj određeni dio od svih uplaćenih sredstva. U sljedećoj slici ćemo prikazat primjer ugovora s dva partnera gdje svako kad pristupi ugovoru vidi sva ukupna uplaćena sredstva i vidi svoj dio sredstva pod „balance“. Pod opcijom „withdraw“ upisuje željeni dio sredstva koji želi povući koji je ograničen ½ od svih uplaćenih sredstva. Nakon povlačenja sredstva s „balance “ on će pokazivati novo stanje za datog korisnika koji je izvršio zahtjev i predstavlja njegov preostali dio sredstava za povlačenje.

Slika 16. Remix prikaz ugovora s tranzakcijama

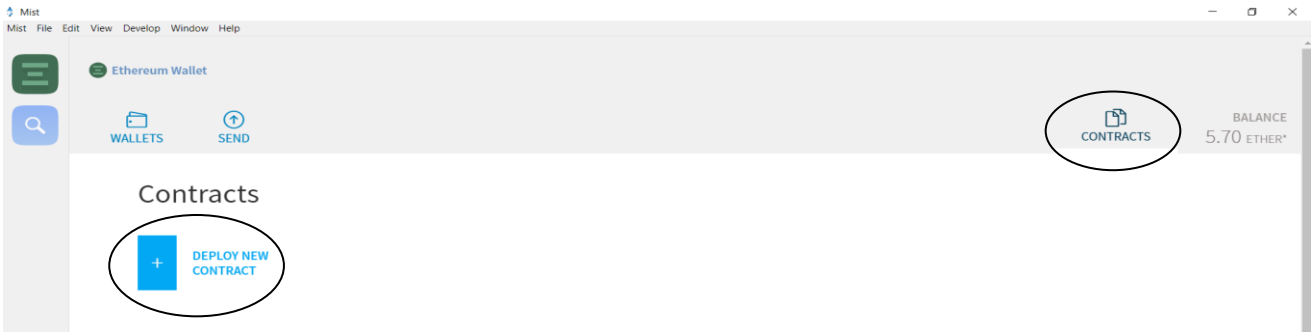


Izvor: Autor

Bilo koji drugi korisnik koji nije upisan u konstruktor tijekom objave ugovora ako želi može pristupiti ugovoru i pokušati napraviti zahtjev za povlačenje sredstva on to može, ali naravno transakcija će mu biti odbijena i nakanadu za korištenja mreže će morat platit korisnik koji ju poziva, neovisno ako je ona odbijena.

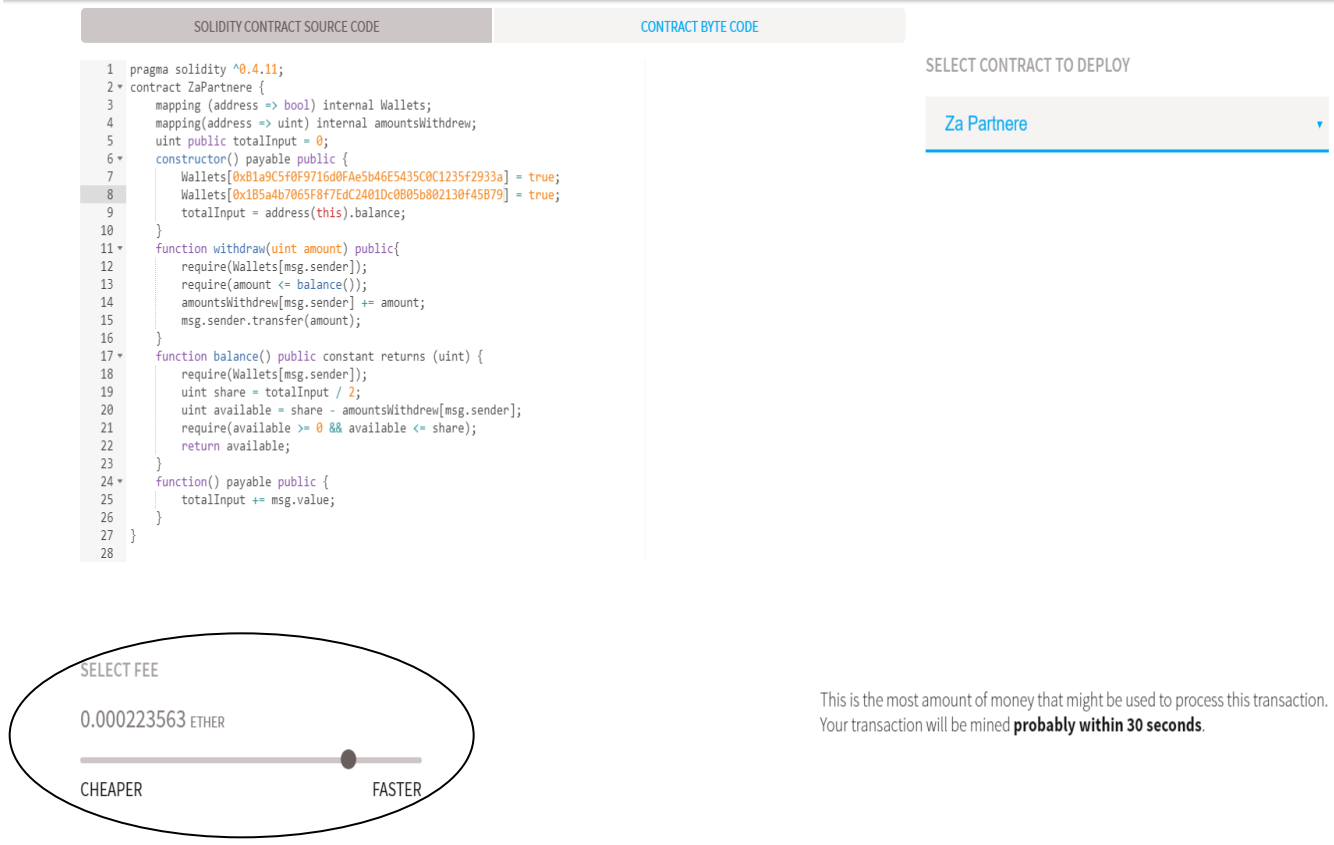
Četvrti korak je obajviti sam ugovor na Rinkeby testNET pomoću Mista. U gornjem desnom kutu odabiremo opciju „Contracts“ i „Deploy new contract“ gdje ćemo kopirati testirani ugovor iz Remixa i objaviti ga. Prilikom objave možemo odabrati maksimalnu količinu naknade pod opcijom „Select fee“ za korištenje ovog ugovora, Veća naknada omogućuje brže transakcije na samoj mreži.

Slika 17. Mist objava ugovora



Izvor: Autor

Slika 18. Mist objava ugovora

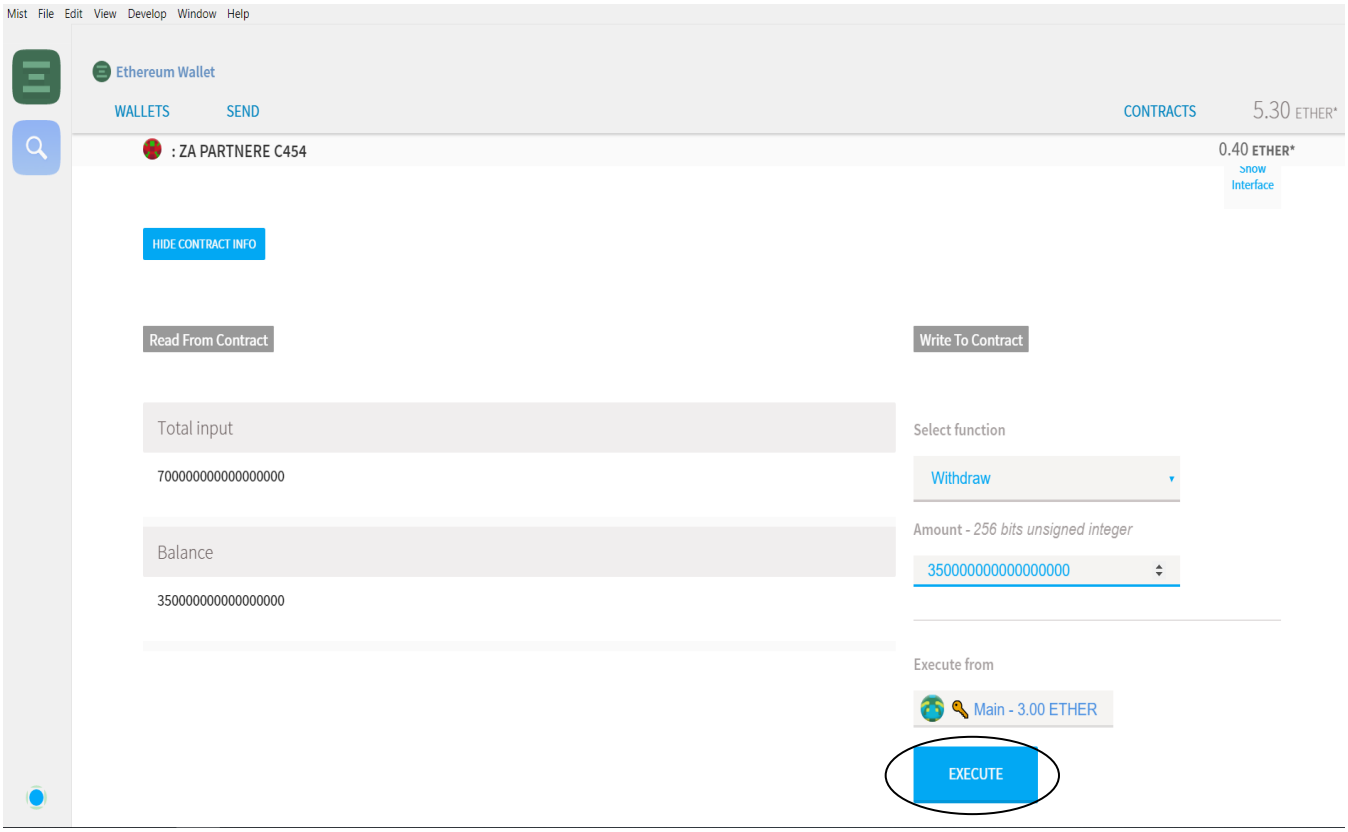


Izvor: Autor

Nakon objave upisani partneri u ugovoru mogu pristupit samom ugovoru i imaju prikazano „Total Input“ i „Balance “ i opciju „Withdraw“ da povuku svoj dio sredstva iz ugovora. Isto kao

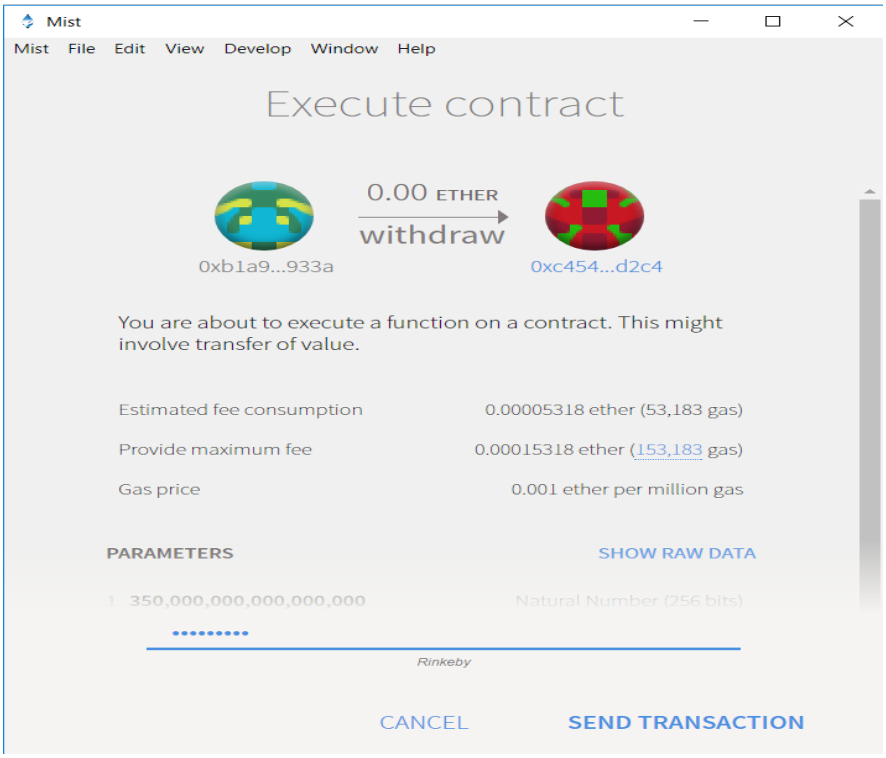
i u Remix okruženju korisnik ili partner može odrediti iznos koji želi povući, naravno taj iznos nesmije biti veći od njegovog „balanca“. Odabirom funkcije „withdraw“ upisuje se željeni iznos koji se želi povući i pomoću gumba „execute“ radi se zahtjev na ugovor. U sljedećem prozoru korisnik unosi šifru svog novčanika za transakciju i prikazana mu je procijena naknade za korištenje mreže u datom trenutku i maksimalna naknada koja je odabrana prilikom objave tog ugovora.

Slika 19. Prikaz objavljenog ugovora putem mista



Izvor: Autor

Slika 20. Potvrda transakcije i prikaz nakande



Izvor: Autor

Sa ovim je završena izrada ugovora kojeg smo testirali u Remix okruženju, objavili ga na testnu mrežu, te je prikazano njegovo korištenje. Očigledno, programski jezik Soldity veoma je sličan C++ i lako razumljiv svima koji imaju osnovu programskog jezika.

5. ZAKLJUČAK

Mogućnosti blockchain tehnologije i pametnih ugovora su ogromne i gotovo neograničene. Pametni ugovori su transparentni jer svaka transakcija je zapisana u blockchainu i cijeli sustav je otvoren i dostupan svima. U radu je navedeno nekoliko primjera kako se pametnim ugovorima i blockchain tehnologijom postojeći sustavi mogu poboljšati. Sve ranije napisano u ovom radu upućuje na zaključak da su pametni ugovori brzi, neovisni, nepogrešivi, transparentni i bez mogućnosti falsifikata i krivotvorenja pojedinih odredbi ugovora. U svakom trenutku smo sigurni da odredbe pametnih se izvršavaju upravo onako kako su dogovorene to jest isprogramirane i gotovo je sigurno da će se sve više transakcija obavljati putem blockchaina i pametnih ugovora, napretkom tehnologije sve više i više. Za očekivati je da će blockchain tehnologija i mogućnosti pametnih ugovora zamijeniti postojeće zastarjele centralizirane sustave posredovanja donoseći sa sobom visoku razinu sigurnosti, brzine, transparetnosti i štedljivosti. Na kraju jednostavno rečeno uvođenjem pametnih ugovora u primjenu uvjeti poslovanja bili bi pošteniji i naravno jednaki za sve.

LITERATURA

Radovi

1. Hozjan, D., Blockchain, Diplomski rad, PMF, Zagreb, 2017.

2. Ostalić, K., Analiza tehnologije i potencijalni napadi, Diplomski rad, FER. 2017.

3. Ostović, K., Ethereum blockchain platforma - analiza tehnologije i potencijalni napadi, FER. 2017/2018.

Internet

4. A Beginner's Guide to Smart Contracts, https://blockgeeks.com/guides/smart-contracts/, pristupljeno 19.8.2018.

5. Blockchain tehnologija, Što su pametni ugovori, https://blockchainonline.blog/2018/04/16/sto-su-pametni-ugovori/ , pristupljeno 20.8.2018.

6. Glodjo, A., Pametni ugovori sa Bitcoinom, http://bosnian.lamareschale.org/bitcoin/coinbrief_bitcoin_smart-contracts-bitcoin/ , pristupljeno 25.8.2018.

7. History of Smart Contarcts, https://www.cryptoninjas.net/what-are-smart-contracts/, pristupljeno 16.8.2018.

8. Minović, M., Blockchain tehnologija: Mogućnosti upotrebe izvan kriptovaluta, https://www.researchgate.net/publication/318722738_BLOCKCHAIN_TEHNOLOGIJA_MOGUCNOSTI_UPOTREBE_IZVAN_KRIPTO_VALUTA 2017 , pristupljeno 27.8.2018.

9. Understanding How Does Ethereum Work, https://www.bitdegree.org/tutorials/what-is-ethereum/, pristupljeno 19.8.2018.

10. What is Blockchain Technology, https://blockgeeks.com/guides/what-is-blockchain-technology/ , pristupljeno 22.8.2018.

11. What is Ethereum?, https://blockgeeks.com/guides/ethereum/ , pristupljeno 24.8.2018.

12. Wikipedia, Etherium, https://en.wikipedia.org/wiki/Ethereum , pristupljeno 22.8.2018.

POPIS SLIKA

POPIS I OBJAŠNJENJE KORIŠTENIH POKRATICA I INFORMATIČKIH POJMOVA

Blockchain – najpoznatija decentralizirana distribuirana struktura podataka

Cryptocurrency – (kripto valuta) digitalna valuta

dApps – (decentralizirane aplikacije) aplikacije koje su decentralizirane i nemoju lokalni server i koriste infrastrukturu decentralizirane mreže.

DLT – (Distributed ledger technologies) distribuirana struktura podataka

GUI – (graphical user interface) grafičko korisničko sučelje

IDE – (integrated development environment) Integrirano razvojno okruženje - softverski paket koji sadrži osnovne alate koji su potrebni programeru za pisanje i testiranje softvera.

MainNET- (Glavna mreža) okruženje za objavljivanje aplikacija

Nodes – (Čvorovi ili stanice) su uređaji ili podatkovne točke na nekoj mreži i predstavljaju pojedinačne dijelove neke veće strukture podataka.

testNet – (mreža za testiranje) okruženje za testiranje aplikacija na mreži

VM – (Virtual machine) emulacija računalnog sustava

Wallet – digitalni novčanik za pohranjivanje kripto valuta