Mogućnosti i opasnosti korištenja pametnih ugovora

Mamut, Jelena

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University Department for Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:993004

Rights / Prava: Attribution-NoDerivs 3.0 Unported/Imenovanje-Bez prerada 3.0

Download date / Datum preuzimanja: **2024-03-29**

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

Repository / Repozitorij:

Repository of University Department for Forensic Sciences

zir.nsk.hr

UNIVERSITY OF SPLIT

dabar

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA
FORENZIČNE ZNANOSTI

FINANCIJSKO-RAČUNOVODSTVENA FORENZIKA

DIPLOMSKI RAD

MOGUĆNOSTI I OPASNOSTI KORIŠTENJA PAMETNIH UGOVORA

JELENA MAMUT

Split, rujan 2019.

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA
FORENZIČNE ZNANOSTI

FINANCIJSKO-RAČUNOVODSTVENA FORENZIKA

DIPLOMSKI RAD

MOGUĆNOSTI I OPASNOSTI KORIŠTENJA PAMETNIH UGOVORA

MENTOR: DR. SC. MARKO PERKUŠIĆ

JELENA MAMUT

400/2017

Split, rujan 2019.

Rad je izrađen u ....Splitu.....
pod nadzorom ....Marka Perkušića.....
u vremenskom razdoblju od ..22.2.. do ..13.9.2019

Datum predaje diplomskog rada: 16. rujna 2019.

Datum prihvaćanja rada: 18. rujna 2019.

Datum usmenog polaganja: 28. rujna 2019.

Povjerenstvo: 1. Prof. dr. sc. Ivica Filipović

2. Prof. dr. sc. Josip Kasum

3. Dr. sc. Marko Perkušić

SADRŽAJ

1. UVOD 1
2. CILJ RADA 3
3. IZVORI PODATAKA I METODE 4
4. TEORETSKI OKVIR 5
4.1 Povijesni razvoj pametnih ugovora 5
4.1.1 Bitcoin blockchain 5
4.1.2 Ethereum 10
4.1.2.1 Programski jezik 10
4.1.2.2 Poruke, transakcije i naknade 11
4.1.2.3 Način skladištenja podataka 12
4.2 Pojam pametnih ugovora 13
5. MOGUĆNOSTI PRIMJENE PAMETNIH UGOVORA 16
5.1 Starter interrupt devices 16
5.2 Know-your-customer 18
5.3 e-Residency 20
5.4 Osiguranje 21
5.5 Građevinska industrija 23
5.6 Internet stvari 24
5.7 Društva temeljena na pametnim ugovorima 26
5.8 Ostale mogućnosti korištenja pametnih ugovora 27
6. OPASNOSTI PRI KORIŠTENJU PAMETNIH UGOVORA 29
6.1 Mogućnosti prijevara uz korištenje pametnih ugovora 29
6.2 Napadi na pametne ugovore 30
6.3 Manjkav kôd pametnih ugovora 30
7. PRAVNO UREĐENJE PAMETNIH UGOVORA U REPUBLICI HRVATSKOJ 32
7.1 Regulacija pametnih ugovora 32
7.2 Pametni ugovori i ugovori u elektroničkom obliku 33
8. REZULTATI 39
9. ZAKLJUČAK 41
10. LITERATURA 42
11. SAŽETAK 47
12. SUMMARY 48
13. ŽIVOTOPIS 49

14. IZJAVA O AKADEMSKOJ ČESTITOSTI 52
15. POPIS SLIKA 53

1. UVOD

Skoro sve u životu mora se platiti. Ne preostaje ništa drugo, već prihvatiti tu činjenicu. Međutim, ono na što se sve više može utjecati jesu način i pripadajući troškovi plaćanja. Nezadovoljstvo dosadašnjim praksama koje često iziskuju ne samo visoke transakcijske troškove, već i oduzimaju mnogo vremena, uz tehnološki razvoj urodilo je novim sustavima koji obećavaju trenutna plaćanja uz skoro nepostojeće naknade. Istovremeno sve veći zahtjevi za privatnošću korisnika *online* usluga iziskuju potrebu za sustavima koji će moći prenijeti informacije bez posrednika koji bi ih skladištili i preprodavali. Kao odgovor tomu počeli su se razvijati sustavi koji omogućuju direktnu komunikaciju između korisnika putem internetskih mreža koji istovremeno pružaju sve veću razinu sigurnosti i efikasnosti. U međuvremenu postoje razni takvi sustavi po imenu *blockchain* koji omogućuju razmjenu podataka sigurno i transparentno. S vremenom se otkriva sve veći broj načina primjene te tehnologije i njezinog usavršavanja zbog čega se više ne ograničava samo na sustave plaćanja, već se tom tehnologijom pokušavaju riješiti razni problemi. U neka od potencijalnih polja tako uključuju glasovanja zbog velike transparentnosti. Neki se fokusiraju na financijsku industriju, kako bi povećali financijsku isključenost te smanjili transakcijske troškove. Međutim, središnjica ovoga rada su pametni ugovori. U širem smislu, svaka Bitcoin transakcija mogla bi se gledati kao jednostran, pojednostavljen pametni ugovor. A u užem smislu možemo se susresti i s cjelokupnim poduzećima temeljenim na pametnim ugovorima. S vremenom se javlja sve veći broj što jednostavnijih aplikacija koje omogućuju korištenje tehnologije pametnih ugovora zbog čega se ciljani segment korisnika svakim danim povećava.

Kako bismo bili u mogućnosti kvalitetno objasniti gdje sve možemo primijeniti pametne ugovore i na koji način, bez da pri tome zanemarimo potencijalne opasnosti, kao prvo moramo objasniti tehnologiju koja se iza njih krije. Pri tome se misli na *blockchain* tehnologiju na kojoj se pametni ugovori temelje. Tomu je razlog to što se oni u svojoj biti sastoje od softverskih rješenja odnosno računalnog koda. Neki bi i Bitcoin smatrali svojevrsnim okvirom za pametne ugovore. Međutim, smatra se da zbog svojih karakteristika ne može udovoljiti specifičnim zadacima potrebnim za kvalitetnu izradu i izvedbu pametnih ugovora. Zbog toga se pojavio Ethereum kao potpuni okvir koji omogućuje korištenje pametnih ugovora širokom spektru osoba te koji neki smatraju najboljim načinom korištenja

pametnih ugovora. Usprkos svojoj tehničkoj naravi, pametni ugovori doveli su i do diskusija u sferi pravne struke te pitanja kako u tim situacijama koristiti uobičajeni pravni sustav i sudove. S obzirom na njegovu decentraliziranost, postavlja se pitanje koga i pod kojim uvjetima teretiti u slučaju štete prouzročene pametnim ugovoru. A s obzirom na mnogobrojne pozitivne učinke i sve veću primjenu, važno je što prije osvijestiti postojeće i potencijalne korisnike pametnih ugovora na moguće opasnosti kojima se izlažu kada ih koriste. Zbog toga će se u ovom radu prikazati različit spektar korištenja pametnih ugovora u praksi i s time povezane opasnosti. Pomoću svih tih saznanja, moći će se doći do zaključka zahtijevaju li pametni ugovori zasebne zakone ili se mogu regulirati unutar okvira postojećih zakona.

2. CILJ RADA

Svrha ovoga rada je konstrukcija istraživanja raznih područja u kojima se pametni ugovori koriste ili planiraju koristiti. Pri tome će se posebna pažnja posvetiti prijevarama i zloupotrebama pametnih ugovora na štetu njihovih korisnika te zakonodavstvu koje ih okružuje.

Zbog znanstvenog usmjerenja ovoga rada postavit će se sljedeće hipoteze koje će se u rezultatima rada potvrditi ili opovrgnuti:

1) Pametni ugovori mogu se uspješno koristiti i u djelatnostima nevezanim za financije.
2) Za korištenje pametnih ugovora neophodan je zaseban zakon kojim će se njihovo korištenje regulirati unutar državne legislative.
3) Pametni ugovori kao način izvršavanja i čuvanja ugovornih obveza mogu smanjiti poteškoće i prijevare koje se događaju u obveznom pravu.

Nadalje, rad će početi s teoretskim dijelom koji će obuhvatiti povijesni razvoj pametnih ugovora kako bi se zaključno mogao iznijeti pojam pametnih ugovora. Nakon toga će se prikazati odabrani slučajevi u kojima bi se moglo ili se već i koriste pametni ugovori u praksi. Time će se prikazati potencijal i mogućnosti pametnih ugovora. Nakon toga slijedi osvrt na opasnosti korištenja pametnih ugovora. U zadnjem dijelu rada prikazat će se relevantni dijelovi domaće regulative kako bi se mogao dovesti zaključak o pravnim pitanjima povezanim s korištenjem pametnih ugovora u Republici Hrvatskoj i potrebi njihovog reguliranja.

3. IZVORI PODATAKA I METODE

Kako bi se navedene hipoteze mogle potvrditi ili opovrgnuti, u ovom će se radu koristiti saznanja iz znanstvene literature iz različitih stručnih područja na teme *blockchaina*, Ethereuma i pametnih ugovora. Radi ostvarenja tog cilja u ovom će se radu koristiti sljedeće znanstvene metode:

- metoda analize
- metoda deskripcije
- metoda kompilacije
- metoda dokazivanja i opovrgavanja
- metoda sinteze
- metoda komparacije.

Prema tome, iz znanstvene literature sumirat će se povijesni razvoj pametnih ugovora. Pojasnit će se potrebno znanje povezano s *blockchain* tehnologijom. Uz to, prikazat će se Bitcoin i Ethereum sustavi kako bi se utvrdile razlike između njih. Analizirat će se mogućnosti i opasnosti pametnih ugovora na primjerima i idejama iz prakse. Također, bit će osvrt na moguće opasnosti zbog korištenja pametnih ugovora. Na kraju će se pomoću pregleda zakonske regulative dati zaključak o pravnim pitanjima postavljenim u radu.

4. TEORETSKI OKVIR

4.1 Povijesni razvoj pametnih ugovora

Ideja pametnih ugovora nije onoliko nova kao što se čini, već je ideja za takav način izvršenja obveza 1999. godine došla od kriptografa Nicka Szaboa. U njegovom konceptu koji je nazvao „Božji protokol“ dvjema ili više strana omogućeno je da posluju uz takozvano božanstvo koje regulira da svaka strana dobije točno one informacije koje su potrebne da bi poslovale. Uz to se iz izlaznih rezultata mogu lako zaključiti podaci koji su bili dani od obje strane što povećava transparentnost poslovanja[1].

Cilj zbog kojega su prvotno nastali pametni ugovori bio je decentralizirana razmjena dobara i usluga putem interneta odnosno elektroničke trgovine na siguran način bez korištenja centralnog tijela ili intermedijana. Želja je bila da se mehanizam odvija nepristrano te da osobe same unose potrebne podatke i informacije u sustav te kako da sustav temeljem toga sam izvrši transakciju. Zamišljena prednost bi bila da ugovorne strane ne moraju otkrivati informacije koje nisu potrebne za izvršenje transakcije[2].

Prema tome, pametni ugovori su postojali već i prije Ethereum platforme u kontekstu kriptovaluta i automatiziranih plaćanja. Međutim, za vrijeme razvijanja tih ideja još nije postojala tehnologija koja bi takve radnje podržavala. Tek razvoj Bitcoina odnosno *blockchain* tehnologije[3] na kojoj se ta kriptovaluta temelji pametnim je ugovorima omogućio iskorak iz teorije u praksu.

4.1.1 Bitcoin blockchain

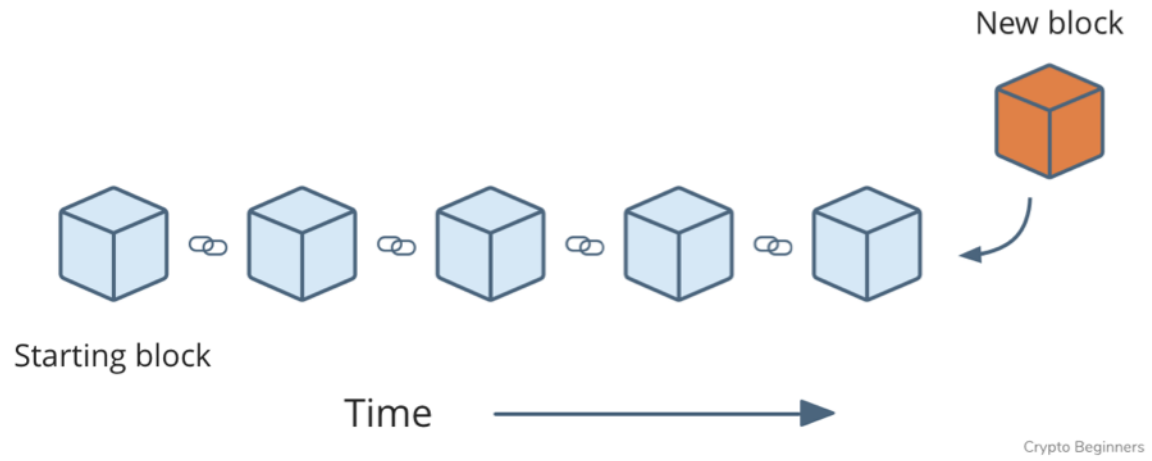
[1] Opširnije vidjeti pod: Blocher, W. (2016). The next big thing: blockchain–bitcoin–smart contracts. *Anwaltsblatt*, *66*(8), 9. Dostupno na: https://www.it-businesstalk.at/wp-content/uploads/AnwBl-2016-612_Blocher.pdf [Pristupljeno: 8. 6.]

[2] Perkušič, M. (2019): Pravna pitanja elektroničkog plaćanja. Sveučilište u Rijeci, pravni fakultet, str. 391-392.

[3] *Blockchain* tehnologija je decentraliziran način skladištenja podataka pri kojemu svako računalo koje je dio mreže ima uvid u podatke, mogućnost potvrđivanja i dodavanja novih podataka pri čemu su ti podaci lančano povezani i kriptirani.

Kako bismo analizirali pametne ugovore, prvo moramo pobliže pojasniti značenje termina *blockchain* tehnologije. Do njezinog razvoja došlo je nakon objave znanstvenog rada „Bitcoin: A Peer-to-peer electronic cash system“[4], čiji je cilj bio pružiti rješenje za takozvani „Double-spending problem“. Taj problem opisuje situaciju u kojoj dvije stranke ne mogu biti potpuno sigurne je li transakcija važeća u smislu je li isti novac već potrošen u drugoj transakciji. Zbog toga je potreban agent, kojeg najčešće utjelovljuju banke, klirinška društva i sl., kako bi se svaka transakcija mogla potvrditi kao valjana. To u praksi rezultira velikim, koncentriranim bazama podataka koje su primamljive za napade krađe podataka te iziskuju veliku razinu povjerenja od svojih korisnika zbog mogućih internih i vanjskih zloupotreba. Upravo zbog sve većeg nepovjerenja u te institucije te troškova koje svojim načinom poslovanja nameću korisnicima, ubrzalo se korištenje decentraliziranih sustava kao što je *blockchain*.

Princip rada valuta koje se temelje na takvom sustavu je da svaka transakcija u sebi sadrži podatke prethodne transakcije te da će se svaka iduća transakcija na nju nadovezati zbog čega su podaci takoreći lančano povezani. Ti su podaci posloženi u blokove čiju valjanost potvrđuju računala povezana s *blockchain* mrežom.

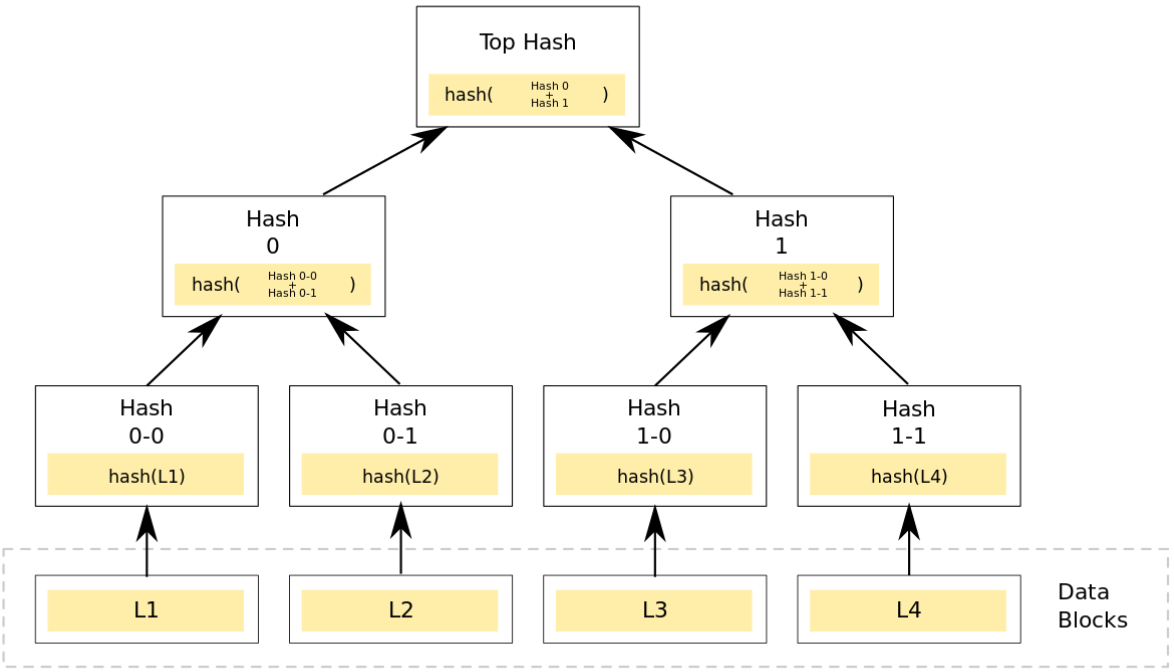


Slika 1. Prikaz *blockchain* lanca

Izvor: http://www.cs.colostate.edu/~cs481a3/#/

[4] Opširnije vidjeti pod: Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Dostupno na: https://bitcoin.org/bitcoin.pdf [Pristupljeno: 23. 5.]

Kako bi se transakcija zapisala kao valjana u lanac, mora biti potvrđena barem od većine mreže. Dakle, nijedna transakcija u sustavu ne bi smjela postojati ako je taj novac prethodno već potrošen. U odnosu na tradicionalne sustave plaćanja, pri Bitcoinu, i drugim kriptovalutama koje se temelje na istim principima, izostaje središnja točka u kojoj se sakupljaju podaci o transakcijama jer se podaci šalju direktno i to svakom članu mreže. Za razliku od bankovnih računa, kod kojih se strogo drži do bankovne tajne kako bi se sačuvala privatnost korisnika, kod *blokchaina* se sve transakcije objavljuju javno. Privatnost njezinih korisnika sačuvana je na način da se koriste pseudonimi. Prema tome se na *blockchain* sustav može gledati kao na svojevrsnu bazu podataka u kojoj svaki korisnik ima uvid u sve transakcije. Kako bi se podaci slagali, koristi se sustav Merkle Tree kojeg također nazivaju *hash*[5] stablom.



Slika 2. Shematski prikaz Merkle Tree sustava

Izvor: https://en.wikipedia.org/wiki/Merkle_tree

[5] *Hash* vrijednosti dobiju se koristeći *hash* algortitam koji radi na način da omogućuje pretvorbu relativno velike količine podataka u *hash* vrijednost određene dužine čiju točnost se lako može računalno provjeriti.

Nadalje, tri su primarna elementa od kojih se sastoji Bitcoin *blockchain*[6]:

1. The ledger – baza podataka
2. The network – mreža računala
3. The consensus – pravilnik.

Navedeni elementi u kombinaciji čine mehanizam koji ispunjava uvjete potrebne za povjerenje bez agenta odnosno takozvani *trustless trust* (hrv.: povjerenje bez povjerenja). Kao što je već pojašnjeno prethodno, *blockchain* je povezana baza podataka koju decentralizirano pohranjuje i nadopunjuje mreža računala zbog čega se procjenjuje da zajednički čine najsnažnije računalo na svijetu. Ipak, najveća inovacija te mreže je njezin pravilnik koji utjelovljuje rudarenje. Rudari su onaj dio računala iz mreže koji dodaju nove blokove u *blockchain* odnosno dodaju nove transakcije u sustav koje ostala računala iz mreže potvrđuju. Moguće je da se u lanac takoreći „ubace" dvije različite transakcije u isto vrijeme. U tom slučaju će se dogoditi rascjep lanca. Nakon nekog vremena odbacit će se ona transakcija koja ima manji broj sljedećih blokova jer u konačnici može samo opstati onaj blok i lanac koji potvrđuje većina računala u mreži odnosno većina procesorske snage mreže. Prema tome će napad na mrežu jedino biti uspješan ako napadač ima veću procesorsku snagu od ostalih računala u mreži jer će morati nanovo i nanovo dodati blokove na krivotvoren blok kako bi ostao najduži. Međutim, prema logici tvoraca Bitcoin *blockchaina* je vjerojatnost za takvu situaciju utoliko manja ukoliko postoje računala koja će biti iskrena i ne potvrđivati krive blokove. A zbog lančanosti podataka, lako se može utvrditi gdje greška ili prijevara počinje.

Pitanje koje se nameće je zašto bi osobe pomoću svojih računala potvrdile tuđe transakcije i time trošile svoje procesorske i energetske resurse. Odgovor na to pitanje upravo je proces rudarenja. Naime, kako bi potvrdili transakciju i dodali novi blok na lanac, rudari moraju riješiti zahtjevan zadatak „proof-of-work" pomoću *hash* vrijednosti. Specifičnost takvog zadatka jest jednosmjernost. Dakle, do rješenja zadatka ne može se doći konkretnom formulom nego nagađanjem te računalo koje brže uspije pogoditi rješenje uspjet će dodati novi blok u lanac. U suprotnom smjeru veoma se brzo može provjeriti točnost *hash* vrijednosti bloka što znači da ostala računala lako mogu provjeriti točnost komponenti lanca.

[6] Opširnije vidjeti pod: Werbach, K., & Cornell, N. (2017). Contracts ex machina. Duke LJ, 67, 313. Dostupno na: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj [Pristupljeno: 8. 6.]

Težina tih izračuna mijenja se kroz vrijeme jer upravo rudar koji uspije dodati novi blok bit će nagrađen jedinicom dotične kriptovalute. To je razlog zašto je rudarima u interesu dodati što više transakcija. Uz to pošiljatelj uz transakciju može kao nagradu dodati iznos koji će dati rudaru. Time će se ubrzati potvrda te transakcije. U budućnosti će se više i više smanjiti nagrada rudarima za dodavanja novih blokova u lanac te se predviđa da će umjesto toga biti plaćeni dobrovoljnim naknadama korisnika kriptovaluta. Kako će se onda definirati cijena transakcije i kako će to utjecati na njihov protok, zasebno je pitanje. U smislu ovoga rada bitno je naglasiti pretpostavku da će napadač teško mijenjati blok u svoju korist te ako posjeduje nadmoć u procesorskoj snazi, radije će izdati točne nove blokove kako bi pridobio nagradu sustava za sebe.

Ukratko se funkcioniranje dodavanja novih blokova može zapisati na sljedeći način[7]:

1. Nova transakcija se proširi po svim računalima u mreži.
2. Svako računalo sakuplja nove transakcije u blokove.
3. Svako računalo radi na „proof-of-work“ zadatku.
4. Kada računalo pronađe rješenje zadatka, šalje novi blok svim ostalim računalima.
5. Druga računala će taj blok jedino potvrditi ako su sve transakcije u njemu valjane i nisu prethodno već potrošene.
6. Računala izražavaju potvrdu bloka na način da počinju raditi na sljedećem bloku koji će u sebi sadržavati *hash* potvrđenog bloka kao *hash* svog prethodnika.

Naposljetku, trebaju se također razmotriti i osnovne postavke sigurnosti privatnosti korisnika pri sustavu u kojemu su sve transakcije javne i lančano povezane. Iz tog razloga korisnici koriste jedinstvene pseudonime. Kako bi poslali iznos, korisnici ih adresiraju na nečiji javan ključ[8]. Kako bi korisnik pristupio svojim iznosima na elektroničkom novčaniku[9] mora koristiti privatan ključ[10] koji treba strogo držati za sebe.

[7] Nakamoto, S. (2008). o.c., str. 3.
[8] Javan ključ u slučaju Bitcoin *blockchaina* je adresa korisnika koja se koristi kako bi se provele transakcije, a sastoji se od 160-bit *hash* funkcije koji je dio cjelovite funkcije koja uključuje i javan i privatan ključ.
[9] Elektronički novčanik kao novčanik uobičajeno označava softver koji u sebi čuva ključeve svog korisnika te mu dopušta provedbu raznih transakcija.
[10] Privatan ključ predstavlja drugi dio cjelokupnog ključa te omogućuje korisniku korištenje sredstava naznačenih na adresi javnog ključa zbog čega se taj ključ treba držati tajnim. Pomoću privatnog ključa korisnik se potpisuje na transakciji, a drugi korisnik pomoću javnog ključa lako može provjeriti valjanost ključeva i transakcije.



Slika 3. Prikaz primjera Bitcoin javnog i privatnog ključa

Izvor: https://99bitcoins.com/how-to-safely-deposit-and-withdraw-bitcoins-from-a-paper-wallet/

Dakle, Bitcoin *blockchain* može se promatrati kao platforma na kojoj se mogu upotrijebiti jednostrani, jednostavni pametni ugovori odnosno transakcije koje sustav samostalno izvršava. Međutim, zbog svoje nezgrapnosti i ograničenosti, Bitcoin *blockchain* prvenstveno se koristi upravo zbog Bitcoina odnosno korištenja kriptovaluta za transakcije plaćanja.

4.1.2 Ethereum

Ethereum je odgovor na probleme pri pisanju pametnih ugovora pomoću Bitcoin programskog jezika te prema njegovom autoru čini nadograđenu verziju Blockchain sustava koji sadržava široku paletu značajki pogodnih za korištenje koncepta pametnih ugovora u okviru zasebne platforme[11]. Ethereum koristi vlastitu kriptovalutu po imenu *ether*. S obzirom na to što je u prethodnom dijelu pojašnjen *blockchain* sustav, na primjeru Bitcoina u ovom će se dijelu rada ukazati na razlike i poboljšanja u Ethereum *blockchain* koje ga čine pogodnim za pisanje i provedbu pametnih ugovora.

4.1.2.1 Programski jezik

Najznačajnija razlika je to što Ethereum koristi programski jezik koji omogućuje bilo kome pisanje pametnih ugovora i decentraliziranih aplikacija u kojima mogu odrediti pravila koja im odgovaraju u smislu vlasništva, transakcija i funkcija. To otvara vrata mnogim različitim idejama. Jedna od najvećih mana pri Bitcoinu je nedostatak petlji u kodu, ali je zbog uvođenja petlji bilo potrebno uvrstiti posebne sigurnosne mjere u Ethereum sustav. Također,

[11] Opširnije vidjeti pod: Buterin, V. (2013). Ethereum white paper. GitHub repository, 22-23. Dostupno na: https://eprint.iacr.org/2016/1007.pdf [Pristupljeno: 23. 5.]

Bitcoin je *value-blind* što znači da nije uvijek moguće odrediti točan iznos UTXO[12] koji će biti isplaćen. Uz to, u Ethereum sustavu ispravljen je nedostatak Lack of state koji je značio da vrijednost može biti jedino isplaćena ili neisplaćena što ne ostavlja mjesta za ugovore (ili transakcije) koji bi bili višeslojni. To je značilo da nije bilo mogućnosti za određivanje limita povlačenja vrijednosti, ali i da se pomoću Bitcoina teško implementiraju kompleksniji ugovori. Pomoću State awareness je Ethereum riješio te probleme[13].

4.1.2.2 Poruke, transakcije i naknade

Ethereum je pisan u *low-level*, *stackbased bytecode* programskom jeziku nazvanom „Ethereum virtual machine code" odnosno „EVM code" u kojemu svaki bajt predstavlja operaciju. U Ethereum sustavu koristi se princip Poruka koji je sličan Transakcijama u Bitcoinu s tri bitne razlike. Kao prvo, Ethereum Poruka može biti kreirana od vanjske strane ili ugovora što omogućuje *eskrow* pametne ugovore odnosno pametne ugovore koji se ponašaju kao skrbnički računi te npr. dok se pretpostavke ugovora ne ispune čuvaju određenu količinu novca[14]. Kao drugo, Ethereum Poruka može sadržavati podatke. Kao treće, primatelj Ethereum Poruke, ako se radi o *contract accountu*[15], ima mogućnost slanja povratne poruke. Nasuprot tome, izraz Transakcija u kontekstu Ethereuma označava potpisani, podatkovni paket s porukom koja dolazi od računa u eksternom vlasništvu. Transakcija sadržava primatelja, potpis pošiljatelja, količinu *ethera* te vrijednosti STARTGAS i GASPRICE[16]. STARTGAS označava limit, a GASPRICE naknadu koju rudar prima prema računalnim radnjama koje je proveo za inicijatora transakcije. Ako naknada koja je naznačena da će rudaru pripasti nakon izvršenja radnji nije dostatna za izvršenje svih potrebnih operacija, sve učinke će se vratiti u prethodno stanje osim već plaćenih naknada. Onaj dio koji je bio određen za naknade, a koji nije iskorišten, vraća se pošiljatelju. Jedan od mehanizama u

[12] Accr. Unspent transaction outputs – vrijednost koja je proizašla rudarenjem, ali još nije korištena za nijednu transakciju.
[13] Opširnije vidjeti pod: Buterin, V. (2013). o.c.
[14] Werbach, K., & Cornell, N. (2017). o.c., str. 32.
[15] *Contract account* je korisnički račun koji u biti pripada pametnom ugovoru koji onda može izvršavati određene radnje.
[16] Gas označava mjernu jedinicu koju se koristi kada korisnik treba platiti da mu se radnje obavljaju na Ethereum mreži. *Online* se može provjeriti cijena jedne Gas jedinice i potreban broj Gas jedinica za pojedini zadatak. Opširnije vidjeti pod: https://kb.myetherwallet.com/en/transactions/what-is-gas/ [Pristupljeno: 9. 9.]

Ethereum sustavu jest „first class citizen“ koji označava da će i sami pametni ugovori moći slati poruke i kreirati nove pametne ugovore[17].

Ukratko, koraci na koji se način transakcije odvijaju u Ethereumu mogu se zapisati kako slijedi[18]:

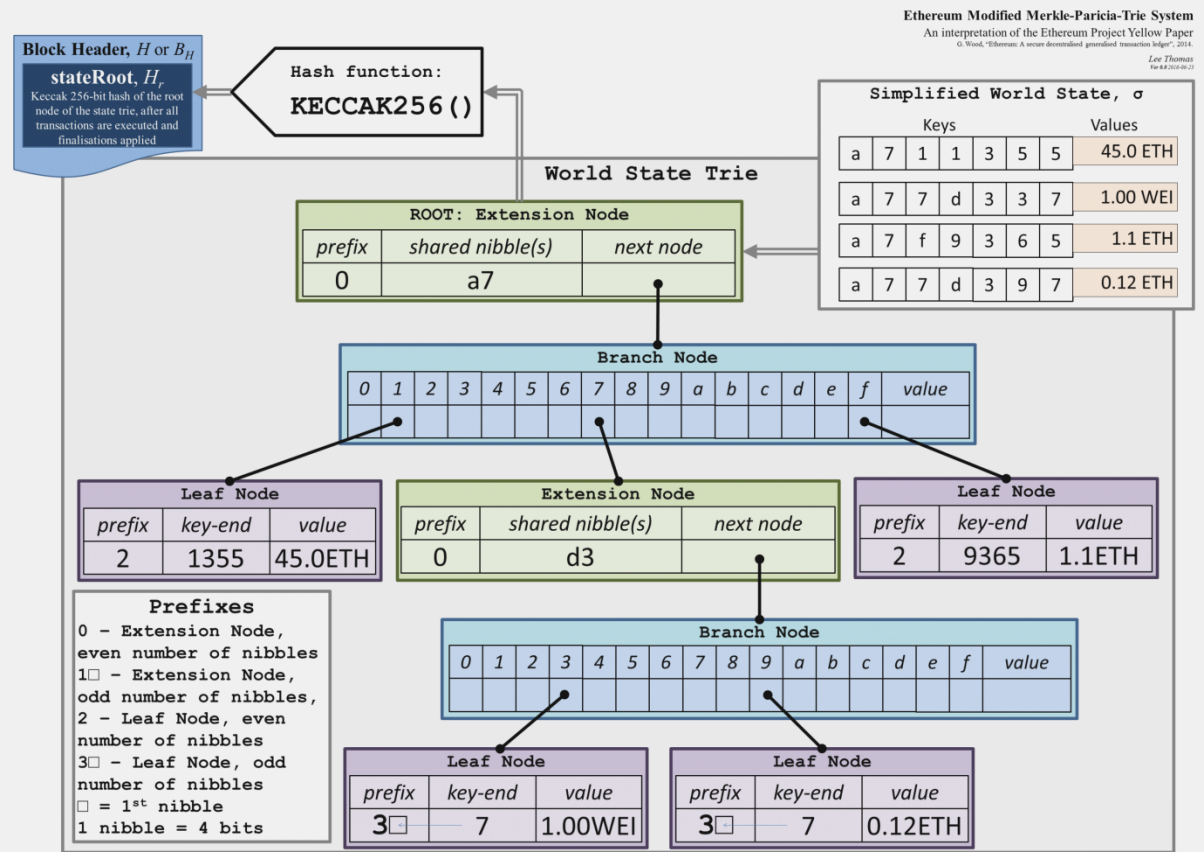
1. Provjera je li transakcija ispravno napisana, ima valjan potpis i da se podaci slažu s podacima pošiljateljevog računa. Ako ne, korisniku se vraća poruka s greškom.
2. Izračun naknade transakcije (STARTGAS*GASPRICE) i određivanje pošiljatelja prema potpisu. Oduzimanje naknade od pošiljateljevog računa i promjena pošiljateljevih podataka. Ako nema dovoljno sredstava na računu, korisniku se vraća poruka s greškom.
3. Inicijalizacija GAS = STARTGAS te oduzimanje određene količine gasa po bajtu da bi se platili bajtovi u transakciji.
4. Transferiranje vrijednosti transakcije od računa pošiljatelja na račun primatelja. Ako račun primatelja ne postoji, slijedi kreiranje tog računa. Ako je račun primatelja pametni ugovor, pokrenut će se kod tog ugovora do njegovog završetka ili kada više nema gasa.
5. Ako se transfer ne dovrši jer pošiljatelj nema dovoljno novca ili kod ostane bez gasa, sve promjene se vrate na stanje prije transfera osim plaćenih naknada koje se dodaju na račun rudara.
6. U suprotnom slijedi vraćanje naknada preostalog gasa pošiljatelju te se naknada za vraćanje tog gasa pripisuje rudaru.

4.1.2.3 Način skladištenja podataka

Iako su Ethereum i Bitcoin veoma slični u kontekstu arhitektura njihovog *blockchain* sustava, postoji velika razlika u smislu spremanja podataka. Nasuprot Merkle Tree koji Bitcoin *blockchain* koristi, Ethereum koristi Patricia Tree. U Ethereum sustavu blokovi sadrže kopiju liste transakcija i najnovije stanje. Grafički prikaz tog pristupa liči na stablo pri kojemu se mijenjaju zadnje karike pri svakoj transakciji. Kako bi se pristupilo upisanim podacima, koriste se pokazivači unutar stabla. U konačnici, kako je stanje zapisano u svakom zadnjem bloku, nema potreba zapisivanja cijele *blockchain* povijesti što u odnosu na Bitcoin štedi

[17] Opširnije vidjeti pod: Buterin, V. (2013). Ethereum white paper. GitHub repository, 22-23. Dostupno na: https://eprint.iacr.org/2016/1007.pdf [Pristupljeno: 23. 5.]
[18] Ibid., str. 15.

prostor na računalima. Za razliku od Bitcoinovog Merkle Treea, koji sačinjavaju *hash* podaci, kod Ethereumovog modificiranog sustava mogu se i dodavati i brisati zapisi[19,20].



Slika 4. Prikaz Ethereum modified Merkle-Paricia-trie sustava

Izvor: https://www.chartnumber.club/ten-awesome-things-you-can-learn-from-ethereum-transaction-chart-ethereum-transaction-chart/40880/

4.2 Pojam pametnih ugovora

Prije primjera gdje bi se pametni ugovori mogli koristiti mora se prvo definirati pojam pametnih ugovora. Iako je osnovni princip pametnih ugovora prilično jednostavan, u praksi ih je teško jedinstveno definirati. Zbog toga postoje razne definicije od kojih neke zauzimaju više tehnički, a neke više pravni položaj. Ovisno o kompleksnosti također bi se Bitcoin transakcije mogle nazvati jednostavnim pametnim ugovorima iako ih se trenutno ne bi

[19] https://medium.com/codechain/modified-merkle-patricia-trie-how-ethereum-saves-a-state-e6d7555078dd [Pristupljeno 12. 6.]
[20] Opširnije vidjeti pod: Buterin, V. (2013). o.c.

takvima smatrali. U današnjici se javlja cijeli niz pitanja pri pokušaju definiranja pametnih ugovora.

U najširem smislu su pametni ugovori niz linija računalnog kôda. Prirodno tome se kao prvo postavlja pitanje što ih razlikuje od uobičajenih računalnih programa, a da ih približava konceptu ugovora. Radi se o njihovoj namjeni. Pravno primjenjiv ugovor omogućuje strankama da koordiniraju svoje postupke i vjeruju da će obveze koje su preuzeli jedni prema drugima biti ispunjene[21].

Moguća definicija pametnih ugovora mogla bi glasiti: „Smatramo kako se s pravnog aspekta pametne ugovore može opisati kao svaki pravni posao koji se sklapa putem algoritma koji samostalno (neovisno od ugovornih strana) osigurava izvršenje jedne ili više činidbi ili utvrđuje ispunjenje određenih uvjeta temeljem unaprijed zadanih parametara.[22]“ Ono osnovno što pametne ugovore čini ugovorima su karakteristike kao što je činjenica da su od strane agenta generirani mehanizmi koji prebacuju prava i obveze. Prema tome se ugovori smatraju takoreći obećanjima ili sporazumom koji su zakonski provedivi. U tom smislu, pametni ugovor će biti ugovor sve dok predstavlja konkretne obveze[23].

Dodatno, možemo pametne ugovore klasificirati i na jake i slabe ugovore. Prema tome, jaki pametni ugovori bi bili oni koji će se izvršiti bez obzira na volju stranaka na način da se njihovo izvršenje ne može spriječiti ili bi bilo preskupo da se to učini. Suprotno tomu, na slabe pametne ugovore može se relativno lako vršiti pritisak voljom stranaka ili sudbene vlasti na njihovo neizvršenje iako su prema uvjetima ugovora bile ispunjene pretpostavke za njegovo izvršenje[24].

Za postojanje pametnih ugovora veže se i nekoliko dodatnih pojmova. Kao prvo, važan je pojam *contractware*. Time se misli na fizičku komponentu pametnog ugovora odnosno digitalno postojanje ugovornih odredbi koje su zapisane pomoću računalnog koda u

[21] Werbach, K., & Cornell, N. (2017). o.c., str. 18.
[22] Perkušič, M. (2019). o.c.
[23] Werbach, K., & Cornell, N. (2017). o.c., str. 26-31.
[24] Raskin, M. (2016). The law and legality of smart contracts, str. 6. Dostupno na: https://www.ilsa.org/ILW/2018/CLE/Panel%20%2311%20-%20THE%20LAW%20AND%20LEGALITY%20OF%20SMART%20CONTRACTS%201%20Georgetown%20Law%20Technology%20Rev.. .pdf [Pristupljeno: 11. 5.]

predefinirani softver koji je na određeni način povezan s onime na što se ugovor odnosi npr. stroj[25]. Usko povezan s korištenjem pametnih ugovora je također pojam „oracle“[26]. Budući da je po svojoj osnovi pametni ugovor ništa drugo negoli računalni kôd, teško može provjeriti ispunjenje pretpostavke čiji se podaci nalaze u njegovom sustavu. Zbog toga se koriste eksterne baze podataka nazvane *oracles* koje mogu biti dio sudbene vlasti, arbitrarne stranke ili odvojene baze podataka kojima obje strane ugovora vjeruju. Tako se na primjer za podatak o temperaturi u određenom mjestu može koristiti baza podataka određene *web*-stranice čijim podacima pametni ugovor ima pristup i koja će u tom smislu biti *oracle* za taj pametni ugovor. Još jedan pojam koji se sve više povezuje s domenom pametnih ugovora je „Internet of things“, koji se sastoji od mnogo fizičkih uređaja koji će kao središnju točku moći koristiti pametne ugovore koji će njima po unaprijed definiranim uvjetima i pravilima raspolagati[27].

Zaključno, pametne ugovore možemo definirati kao način izvršenja unaprijed definiranih kriterija i uvjeta na koje dvije ili više strana pristaje da bi se samostalno izvršili pomoću računalnog kôda koji se nalazi na decentraliziranoj *blockchain* mreži.

[25] Ibid., str. 3.
[26] Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *Available at SSRN 2580664*, str. 50. Dostupno na: https://poseidon01.ssrn.com/delivery.php?ID=670117070070069028074121019118080120031047031042055074081065125024121065069000085124049107118055103025009099114079106120083118028035061021010081089102065087095112112003008009002100098091084090102026123031099001073029100096010070079028112072116115029103&EXT=pdf [Pristupljeno: 8. 6.]
[27] Ibid., str. 14.

5. MOGUĆNOSTI PRIMJENE PAMETNIH UGOVORA

U ovom dijelu rada prikazat će se određeni primjeri na koji način bi se mogle iskoristiti prednosti pametnih ugovora za rješavanje nekih dosadašnjih problema ili za poboljšanje dosadašnjih rješenja.

5.1 Starter interrupt devices

Jednu od mogućih primjena pametnih ugovora u financijskom poslovanju možemo vidjeti u svijetu SID-ova („starter interrupt devices" – uređaj koji onemogućuje pokretanje auta) koji sve učestalije koriste kreditne institucije ili lizing društva pri prodaji automobila[28]. Pomoću takvih uređaja otvaraju se vrata ljudima koji prije nisu bili u mogućnosti na takav način financirati kupnju vozila. Međutim, istovremeno ti uređaju mogu predstavljati veliki rizik za sigurnost tih osoba zbog čega se predlaže korištenje pametnih ugovora.

S ekonomskog aspekta, SID-ovi omogućuju smanjivanje troškova institucija koje su vlasnici vozila jer se ne moraju oslanjati na službe za prisilno vraćanje imovine. Takvi procesi mogu biti skupi i dugotrajni te dovesti u opasnost osoblje tih službi. U SID uređajima je uobičajeno i uključen GPS-uređaj kako bi se mogla utvrditi točna lokacija vozila u trenutku gašenja ili već prije gašenja. Iz razloga što kreditori vozila ne moraju tražiti, ponekad i po različitim državama, te ih mogu isključiti kako bi onemogućili bijeg nakon prestanka otplate vozila, kreditori mogu nuditi takve vrste financiranja uz manje kamate. Uz to, kako kreditori bez velikih napora i troškova mogu vozilo vratiti u svoje vlasništvo, kreditori imaju inicijativu odobravanja kredita osobama s lošijim kreditnim rejtingom s kojima prethodno nisu bili voljni poslovati. Prema nekim procjenama ti su uređaji već postigli da plaćanja od strane korisnika budu redovitije[29].

Nažalost, uz koristi koje ti uređaji donose kako za kreditore, tako i za korisnike vozila, već su se dogodile razne situacije koje pokazuju zabrinjavajuće rizike koji potiču regulatore da se

[28] Opširnije vidjeti pod: Corkery, M., & Silver-Greenberg, J. (2014). Miss a Payment? Good Luck Moving That Car. *New York Times*. Dostupno na: https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/ [Pristupljeno 16. 6.]
[29] Ibid.

uključe u ovu tematiku. Samo je jedan od primjera da se korisnici financiranja osjećaju nesigurno jer nisu dovoljno detaljno obaviješteni o tome u kojem slučaju i roku se vozilo može na daljinu isključiti. Pri lošoj ugradnji postoji rizik da se vozilo i tijekom vožnje isključi. Također, neke osobe tvrde da kôd koji im je dan od kreditora kako bi vozilo ipak u hitnoj situaciji mogli koristiti nije uvijek bio ispravan. Neke osobe se u konačnici osjećaju izrabljeno te se nalaze u situaciji u kojoj moraju prihvatiti ugradnju takvog uređaja kako bi imale pristup financiranju te platiti troškove uređaja i njegove ugradnje. Bez obzira na pozitivan utjecaj na kamate zbog smanjenih rizika, troškovi financiranja su vrlo visoki uz malu toleranciju na kašnjenje plaćanja[30].

Konkretno, u Kanadi postoji velika zabrinutost glede zaštite privatnosti korisnika vozila. Kada su u vozilo ugrađeni SID uređaji koji imaju i GPS uređaj, kreditori imaju mogućnost stalnog praćenja kretanja vozila. Kreditori bi takve podatke mogli koristiti bez obzira na to je li rata uredno plaćena ili nije i time zadirati u osobni život korisnika vozila. Također, može se zamisliti mogućnost da se na temelju konstantnog sustavnog praćenja putanja vozila utvrdi je li vozilo ukradeno, ali je uspješnost takvih mjera upitna. Kreditori ističu kako su njihovi uređaji i načini njihovog korištenja u skladu s postojećim zakonima. Međutim, na primjeru Kanade i njihovih zakona za zaštitu privatnosti može se vidjeti da nisu spremni na takav razvoj tehnologije što korporacijama daje otvorene ruke u njihovome poslovanju i korištenju mjera s kojima se potrošači ne slažu najbolje[31].

Zbog svega navedenoga, već sada postoje određene preporuke kako bi odnos između kreditora i potrošača bio što skladniji, kao na primjer[32]:

1. Obavezno postojanje internog ili eksternog osoblja koje će pravilno ugraditi sve uređaje.
2. Davanje načina korištenja ugovora i dotične dokumentacije na pregled svom odvjetniku.
3. Provjera da je korisnik vozila dobio svu potrebnu dokumentaciju te da je upoznat s tim kako uređaj radi i koje radnje treba poduzeti u hitnim situacijama.

[30] Ibid.
[31] Colbert, Y. (2018): Privacy group wants better regulation for GPS starter interrupt devices. CBC News. Dostupno na: https://www.cbc.ca/news/canada/nova-scotia/gps-starter-interrupters-privacy-technology-laws-1.4780860 [Pristupljeno 16. 6.]
[32] Johnson, E., L. (2016): Starter interrupt and GPS devices: Best practices. Passtimegpssolutions. Dostupno na: https://passtimegps.com/starter-interrupt-and-gps-devices-best-practices/ [Pristupljeno: 16. 6.]

4. Provjera pravne utemeljenosti u državnoj legislativi.
5. Osiguravanje da ne bude utjecaja diskriminacije (npr. da uređaji budu isključivo u vozilima kojima upravljaju žene).
6. Sustavno prikupljanje i obrada reklamacija i prigovora.
7. Dubinska analiza poduzeća koje prodaje SID uređaje.
8. Upozorenje osiguratelju koji troškovi mogu proizaći zbog SID uređaja.

Iz iznesenoga se teško može vidjeti hoće li u ovom slučaju prevagnuti prednosti ili nedostaci SID uređaja. Najveći problem prvotno predstavlja nedostatak reguliranosti tog područja što stvara nesigurnost za njegove korisnike čija se vozila ponekad i bez najave više ne mogu koristiti. Drugi najveći problem je zaštita privatnosti korisnika te njihova zaštita od samovolje zaposlenika financijske institucije. Upravo zbog toga se u ovom području vidi potencijal pametnih ugovora. Bez obzira na detalje koji će biti uključeni u zakone o SID uređajima, sve buduće odredbe zakona će se moći prenijeti u pametni ugovor. Prema tome će korisnici vozila biti sigurni da će se pametni ugovor izvršiti točno onako kako je određeno ugovorom. Postoje načini da se pametni ugovor računalno napiše na način da u sebe može apsorbirati nove zakonske odredbe. Također, postoji mogućnost transparentnosti korištenja *blockchain* sustava te zaštite privatnosti kroz pseudonime i enkripciju podataka. Iako pametni ugovori neke poteškoće s lakoćom mogu riješiti, nedostaje ljudskost koja je često potrebna s obzirom na to što se u ovim slučajevima prvenstveno radi o osobama koje će s velikom vjerojatnošću kad-tad imati problem s pravovremenim plaćanjem. U takvim slučajevima je pitanje tko će moći vozilo dati na korištenje kada se radi o situaciji koja je možda opasna po život tih osoba. Zbog toga će se morati uvesti posebne sigurnosne mjere. Pitanje je kako objasniti računalnom kôdu hitnost situacije. Ako se uvede mjera da korisnik vozila pošalje zahtjev osoblju financijske institucije koja odobrava privremeno korištenje vozila, opet postoji mogućnost iskorištavanja moći od strane osoblja te pametni ugovor gubi na samostalnosti zbog koje je prvotno i uveden.

5.2 Know-your-customer

Još jedno područje u kojemu se mogu vidjeti velike prednosti korištenja pametnih ugovora jest koncept *know-your-customer* koji se primjenjuje u dubinskoj analizi. Prema Zakonu o sprječavanju pranja novca, dubinska analiza u kontekstu KYC-a je utvrđivanje identiteta

stranke i provjera njezina identiteta na osnovi dokumenata, podataka ili informacija dobivenih iz vjerodostojnoga, pouzdanoga i neovisnoga izvora, uključujući, ako ga stranka ima, kvalificirani certifikat za elektronički potpis ili elektronički pečat ili bilo koji drugi siguran, daljinski ili elektronički, postupak identifikacije koji su regulirala, priznala, odobrila ili prihvatila relevantna nacionalna tijela te utvrđivanje identiteta stvarnoga vlasnika stranke i poduzimanje odgovarajućih mjera za provjeru identiteta stvarnoga vlasnika stranke, uključujući poduzimanje mjera potrebnih za razumijevanje vlasničke i kontrolne strukture stranke kada je stranka trgovačko društvo, druga pravna osoba i s njome izjednačen subjekt ili *trust* i s njime izjednačen subjekt stranoga prava[33]. Korištenje pametnih ugovora pri dubinskoj analizi potencijalno bi moglo omogućiti da institucije i stranke mogu provesti mjere KYC bez zadiranja u privatnost stranaka te dodatno omogućuje financijskim institucijama koje su prema zakonskim odredbama prisiljene na vršenje mjera dubinske analize da mogu sudjelovati u korištenju *blockchain* tehnologije.

U nadi za rješenjem problema privatnosti, autori znanstvenog članka razvili su osnovne pretpostavke kako bi se mogao koristiti koncept pametnih ugovora u KYC radnjama na način da se sačuva privatnost stranaka nad kojima se te radnje izvršavaju. Prema mišljenju autora, kod digitalnog identiteta mora se moći provjeriti da je to taj korisnik te provjeriti ima li korisnik pravo na izvršenje radnje koju zahtijeva. Kao rješenje predlažu KYC davatelja kojeg utjelovljuje pametni ugovor temeljen na Ethereum sustavu. Davatelj je jedini koji ima pristup privatnim podacima te pomoću unutarnje, kriptirane baze podataka provjerava kvalificiranost korisnika. Na takav način, korisnici sigurno mogu koristiti iste digitalne račune na više različitih mjesta. Također, postoji prijedlog da se osnuje specifičan *blockchain* sustav npr. za banke. U tom slučaju bi prva banka spremila *hash* podatke dokumenata korisnika u pametan ugovor na taj *blockchain*, a svaka druga banka bi imala siguran pristup toj bazi zbog čega ne bi bilo potrebe za osnivanjem više baza podataka[34].

Jedan od primjera načina provođenja KYC mjera pomoću *blockchaina* koja uključuje ne samo identificiranje stranke nego i praćenje poslovanja uvođen je od strane revizora Deloitte.

[33] Zakon o sprječavanju pranja novca i financiranju terorizma (NN 108/17, 39/19). Dostupno na: https://www.zakon.hr/z/117/Zakon-o-sprje%C4%8Davanju-pranja-novca-i-financiranju-terorizma [Pristupljeno: 19. 6.]

[34] Opširnije vidjeti pod: Biryukov, A., Khovratovich, D., & Tikhomirov, S. (2018). Privacy-preserving KYC on Ethereum. Dostupno na: https://pdfs.semanticscholar.org/8aa3/5a333495bda6fca2e75cbae6d7a3ffc62b7f.pdf [Pristupljeno: 16. 6.]

Taj pristup je reguliran te omogućuje smanjenje troškova dodavanja novih korisnika na različite platforme i institucije. U tom sustavu korisnici imaju točan uvid u osobne podatke spremljene na *blockchain* sustavu. Na taj način korisnici imaju sve veću razinu zaštite svojih podataka, ali i veću razinu sigurnosti pri prijavljivanju na različite platforme ili stupanjem u odnos s različitim institucijama te također institucije mogu uštedjeti značajnu količinu vremena i resursa pomoću automatizacije i olakšavanja tog procesa[35].

5.3 e-Residency

Jedno od novih područja primjene pametnih ugovora jest projekt „e-Residency“ (e-rezidentnost) u Estoniji[36]. Ono se zasniva na suradnji s organizacijom Bitnation koja je time prvotno napravila iskorak kako bi se pomoglo izbjeglicama koje su masovno došle u Europsku uniju i slične probleme. Zbog toga Bitnation radi na tome da njihovi dokumenti budu u skladu sa smjernicama Ujedinjenih naroda za hitne putne dokumente. Nasuprot tome, Estonija je u ovoj suradnji napravila iskorak prema dugoročnim rješenjima. Osobe mogu bez obzira na svoju nacionalnost dobiti e-rezidentnost koja označava identitet ne na području Estonije, već na području Blockchaina. U sklopu e-rezidentnosti nalazi se program infrastrukture za javne ključeve koju je započela estonska vlada. Korisnici dobiju „smart card“ (pametnu karticu) takozvanu Digi-ID koja u sebi sadržava digitalne certifikate koji potvrđuju osobne podatke vlasnika kartice. Na karticu su povezane Ethereum adrese koje su tako povezane s osobnim podacima te se pomoću te kartice mogu pokrenuti i primiti transferi s novčanikom temeljenom na pametnom ugovoru. Pametni ugovori potrebni su za verifikaciju podataka te se izgubljena kartica može poništiti te izdati nova[37].

Korisnici takvog sustava mogu dobiti potpise na *blockchainu* za koje im inače treba javni bilježnik (npr. za ženidbe, rodni listovi, trgovački ugovori i slično)[38]. Zbog toga je Bitnation

[35] https://www.finextra.com/pressarticle/69173/deloitte-develops-blockchain-proof-of-concept-to-mutualise-kyc-checksleft [Pristupljeno: 19. 6.]
[36] https://blog.oraclize.it/identity-on-the-blockchain-chapter-3-585bc5c7e2c7?fbclid=IwAR0jUlELSQiiKeolvlZWsoP5IuzQz_EM4De0ayiP4CaYoQOfSDqvAvUorhQ [Pristupljeno: 19. 6.]
[37] https://cointelegraph.com/news/bitnation-registers-first-refugees-on-the-blockchain?fbclid=IwAR3eRj7s-OaIQmuRRtz33hD0t2Jj1ymTphQACLgAXfknreNM66_9hdipvcA [Pristupljeno: 19. 6.]
[38] https://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923?fbclid=IwAR2k3Z82G1kZ54jIAv8zIG5qplG2VYeJP-vnYsl92fuqSsRHlsRIgJVX1CU [Pristupljeno: 19. 6.]

takoreći prva virtualna država. To znači da e-Rezidenti koji se na taj način vjenčaju nisu vjenčani u jurisdikciji Estonije, već na *blockchainu* koji predstavlja pravnu obvezu o postojanju i integritetu ugovornih sporazuma. Na taj način pokušava se građanima dati izbor za usluge koje inače isključivo nude države[39]. Korisnicima programa je omogućeno otvaranje poduzeća, iako nemaju fizičku rezidentnost u Estoniji. Također, korisnici imaju mogućnost digitalno potpisati, verificirati i šifrirati dokumente i ugovore. Međutim, Estonija je odredila određene sigurnosne mjere, kao npr. ako osoba želi otvoriti bankovni račun u Estoniji, mora doći barem prvi put osobno u banku. Što se tiče pravne utemeljenosti, mora se uzeti u obzir regulativa države u kojoj se osoba nalazi. Npr. u Ujedinjenom Kraljevstvu zemljišta se ne mogu prodavati bez pisanog ugovora. Prema tome, valjanost radnji će uvelike ovisiti o regulaciji elektroničkih potpisa, obveznosti pisanosti ugovora i slično[40].

Iz iznesenoga se može zaključiti kako pomoću pametnih ugovora možemo dovoljno kontrolirati *blockchain* sustav da bismo omogućili njihovo korištenje širim masama uz istovremeno postojanje države i njezine legislative.

5.4 Osiguranje

Osiguranje je područje koje u sebi sadržava mnogo mjesta u kojima se mogu iskoristiti značajke pametnih ugovora i *blockchain* tehnologije. Veliki su učinci na ubrzavanje i automatizaciju rutinskih procesa što povećava efikasnost i snižava troškove poslovanja. Osiguravajuća društva također mogu koristiti KYC aplikacije koje rade pomoću sustava temeljenih na pametnim ugovorima[41].

U neka od područja osiguranja kojima će pametni ugovori pridonijeti mogu se ubrojiti područje rizika od više sile. Osiguratelj može ugradnjom termometara i sličnih uređaja ili koristeći treće stranke za podatke automatizirati proces isplate odštete na način da npr. ako temperatura doseže ili padne pod određenu razinu, aktivira se pametni ugovor. Na taj se način

[39] https://bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offer-blockchain-notarization-services-to-e-residents-1448915243?fbclid=IwAR3uwOBPjFJ3Dji5kBaZzU8cmberTXVmQsYqOnDEpz7gGY9ojQs0lYMyuwY
[Pristupljeno: 19. 6.]
[40] https://cointelegraph.com/news/estonian-e-residency-and-bitnation-launch-new-public-notary-in-blockchain-jurisdiction?fbclid=IwAR10lQrT2Afq5aJtGzNClOL20Pu_TxA1guPUQrXxebQVIjzYUvqTep5z98g
[Pristupljeno: 19. 6.]
[41] Opširnije pod poglavljem rada: 5.3.

poljoprivrednici mogu osigurati za slučaj lošeg uroda bez da moraju dugo čekati odštetu. Na sličan način mogu se riješiti štete na autu pomoću mjerila krupe[42]. Još jedno područje u kojem pametni ugovori mogu činiti veliku pozitivnu razliku jest transportno osiguranje. Zbog čestih promjena osiguratelji imaju poteškoća stići mijenjati uslugu korisnika osiguranja zbog čega su korisnici često previše ili premalo osigurani. Pomoću pametnih ugovora će korisnik osiguranja sam moći u sustav unijeti promijenjene značajke te dobiti promjenu usluga trenutno. Još jedan primjer bio bi povezivanje s ovlaštenim mehaničarima kako bi se isplata odštete za popravak automobila automatizirano mogla isplatiti[43].

Ako bi se dodatno iskoristile prednosti virtualnih valuta, otvara se mogućnost mikroosiguranja. Tako bi automobil mogao biti osiguran samo onoliko dugo koliko se koristi ili bi osoba plaćala za putno osiguranje automatski kada prijeđe granicu sve dok se ne vrati nazad. U modernom izdanju života korisnika osiguranja, moglo bi se putem pametnih satova mjeriti koliko je osoba zdrava kako bi se premija osiguranja preračunala. Neke značajke *blockchain* tehnologije čak koriste za P2P[44] način kako bi se međusobno osigurali bez financijske institucije[45].

Prema iznesenome može se zaključiti kako je razvoj pametnih ugovora za industriju osiguranja tek pri svom početku te uvelike ovisi o povezivanju pametnih ugovora s mjerilima u stvarnome svijetu. Pri tome će i osiguranici i osiguratelji morati biti pažljivi pri odluci na koji način će se stvarni događaji mjeriti kako bi bili sigurni u valjanost odluka o odštetama koje se prema tim podacima isplaćuju. Također, osiguratelji će se morati brinuti o načinu kako korisnik osiguranja dodaje značajke u sustav osiguratelja kako ne bi odmah u početku osiguranja došlo do prijevare.

[42] Möhlenkamp, M., Wessel, T. (2018): Smart Contracts in der Versicherung – Chancen und rechtliche Herausforderungen. Wilhelm Rechtsanwälte. Dostupno na: https://www.wilhelm-rae.de/sites/default/files/pdf/versicherungspraxis_-_smart_contracts_in_der_versicherung_-_mai_2018.pdf [Pristupljeno: 8. 6.]

[43] Opširnije vidjeti pod: Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough?. *Future Internet*, *10*(2), 20. Dostupno na: https://scholar.google.hr/scholar?hl=hr&as_sdt=0%2C5&q=Blockchain+and+Smart+Contracts+for+Insurance%3A+Is+the+Technology+Mature+Enough%3France_Is_the_Technology_Mature_Enough&btnG= [Pristupljeno: 9. 6.]

[44] *Peer to peer* izraz se koristi kada se transfer vrši direktno od osobe do osobe bez korištenja intermediara.

[45] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). o.c.

5.5 Građevinska industrija

Građevinska industrija je karakteristična po velikim iznosima uloženih sredstava tijekom gradnje koja se vraćaju naknadno kroz najam ili trenutno kroz prodaju nekretnine. Radi se o veoma tradicionalnoj industriji s kojom se susrećemo u svakoj državi. Autori znanstvenog članka iz Rumunjske su problematici koja je uočena u njihovoj državi povezanoj s građevinskim sektorom pristupili rješenjem koje uključuje pametne ugovore. Nacionalna istraživanja provedena u toj državi pokazala su kako uzrok najvećih poteškoća te stečaja građevinskih poduzeća kod njih leži u poremećajima plaćanja tijekom gradnje. Prečesto se dogodi da novac nije dostupan kada je potreban te dolazi do stečaja manjih poduzeća uključenih u gradnju ili kašnjenja zbog nemogućnosti kupnje materijala. Među zakonskim prijedlozima je bio i plan takozvanog građevinskog *trusta* koji bi bio zadužen na nadzor i plaćanja među sudionicima gradnje. Međutim, ideja za takvo tijelo nije provedena u praksi. Zbog toga autori predlažu pametne ugovore koji će moći u sebe implementirati da novac za plaćanje „stoji na čekanju" sve dok radnici ne potvrde u sustavu ispunjenje zahtijevanih kriterija. Također, može se implementirati provizijsko plaćanje za određene dijelove ispunjenja. Uz to, mogu se različiti pametni ugovori povezati kako bi se dobila mreža koja uključuje sve sudionike i dijelove gradnje[46]. Ukratko se prednosti korištenja pametnih ugovora mogu svesti na sljedeće točke[47]:

1. Postoji jamstvo da su uplaćena sredstva te su kroz cijeli vremenski proces gradnje dostupna za plaćanje.
2. Zaštita izvođaču radova, svih podizvođača te dobavljača na način da nisu moguća kašnjenja u plaćanjima ili eventualno neplaćanje.
3. Zaštita različitih sudionika od insolventnosti drugog sudionika.

Kako bi dobili dojam o vjerojatnosti implementacije pametnih ugovora u građevinsku industriju u Velikoj Britaniji je provedeno anketno istraživanje na temelju odgovora osoba koje rade u industrijama povezanim s građevinom odnosno pravnici, konzultanti, projekt-menadžeri i slično. Iako su prema prvim odgovorima te osobe bile veoma optimistične i

[46] Opširnije vidjeti pod: Cardeira, H. (2015). Smart contracts and their applications in the construction industry. Dostupno na: https://heldercardeira.com/1503P.pdf [Pristupljeno: 15. 6.]
[47] Ibid., str. 5.

uvjerene da se radi o modernoj industriji koja je spremna prihvatiti nove tehnologije, ostali odgovori bili su manje entuzijastični. Kao prvo, nisu bili upoznati ni s pojmom ni s praksom korištenja pametnih ugovora. Kao drugo, smatraju da bi novu tehnologiju tek implementirali kada postoji dovoljno drugih osoba i industrija u kojima se već raširila[48]. Prema tome, može se primijetiti kako usprkos velikim prednostima, industrije koje nisu prvenstveno tehničke naravi, teško prihvaćaju nove tehnologije kao inovatori.

5.6 Internet stvari

Jedno od apstraktnijih polja je takozvani internet stvari. Neki pod tim nazivom podrazumijevaju mrežu, neki paradigmu i tako dalje. U poveznici s pametnim ugovorima možemo ga zamisliti kao način upravljanja najrazličitijim uređajima na automatiziran i unaprijed definiran način koji se sastoji od linija računalnog kôda spremljenih na *blockchain* mreži. Kako bismo pobliže definirali koji su to uređaji možemo koristiti sljedeće karakteristike[49]:

- uređaj mora imati svrhu
- može se povezivati bez potrebe da mora stalno biti povezan (povezivanje se može postići putem *etherneta*, verbalne ili fizičke ljudske interakcije)
- ima oblik ili unutar sebe ima postavljen set struktura koje imaju oblik
- postoji mogućnost lociranja uređaja pomoću unaprijed definiranih mehanizama kao npr. GPS
- postoji mogućnost komuniciranja od strane uređaja, prema uređaju ili oboje
- postojanje korisničkog sučelja ili drugog načina za komunikaciju
- postojanje fizičkog ili logičkog oblika
- može biti živuće ili neživuće
- može se identificirati
- ima određeni kapacitet za samostalno djelovanje
- može biti materijalno ili nematerijalno

[48] Opširnije vidjeti pod: Mason, J., & Escott, H. (2018). Smart contracts in construction: views and perceptions of stakeholders. In Proceedings of FIG Conference, Istanbul May 2018. FIG. Dostupno na: http://eprints.uwe.ac.uk/35123/ [Pristupljeno: 15. 6.]

[49] Opširnije vidjeti pod: Oriwoh, E., & Conrad, M. (2015). 'Things' in the Internet of Things: towards a definition. International Journal of Internet of Things, 4(1), 1-5. Dostupno na: http://article.sapub.org/10.5923.j.ijit.20150401.01.html [Pristupljeno: 16. 6.]

- može biti autonomno, djelomično autonomno ili neautonomno.

Iako se radi o podosta apstraktnom pojmu, lako se mogu naći uređaji iz svakodnevnog života koji bi se mogli povezati s takvom tehnologijom. Tako npr. senzori na automobilu automatski bi mogli prijaviti kvar i naručiti dijelove za popravak vozila[50]. Slični načini korištenja lako se mogu zamisliti i za druge uređaje, strojeve i slično. Granica je mašta njihovih korisnika.

Povezivanje pametnih ugovora s *blockchain* tehnologijom kod korištenja interneta stvari pridonosi na sljedeće načine[51]:

- distribuiran sustav zapisa koji omogućuje dijeljenje podataka na mreži čiji su članovi ključni sudionici
- uvjeti poslovanja i pravila automatizacije interakcije sudionika u sustavu ugrađeni su u sam sustav
- sigurnost se bazira na *hash* tehnologiji, verifikaciji identiteta i podrijetlu autentičnosti
- postoje pravilnici i suglasnost za modele na koji način će se detektirati loši igrači i ublažiti rizike
- smanjivanje troškova.

Također, koristeći pametne ugovore, mogu se riješiti neki problemi s kojima se susreću tradicionalna poduzeća[52]:

- analitično praćenje podataka
- sigurna ažuriranja softvera
- plaćanja i mikroplaćanja.

Iako pametni ugovori pružaju odgovor na mnogo pitanja i problema s kojima se poduzeća te kućanstva susreću, tehnička rješenja još uvijek imaju dug put ispred sebe prije nego što će moći udovoljiti zahtjevima svojih potencijalnih korisnika. Tomu pridonosi što Ethereum (u trenutku pisanja članka) tek može obrađivati 25 transakcija u sekundi, a pretpostavlja se da bi za veću primjenu morao biti spreman obrađivati 1000 transakcija u sekundi. Daljnji tijek

[50] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018), o.c., str. 7.
[51] https://medium.com/smartz-blog/how-blockchain-and-smart-contracts-can-impact-iot-f9e77ebe02ab [Pristupljeno: 22. 6.]
[52] https://medium.com/smartz-blog/how-blockchain-and-smart-contracts-can-impact-iot-f9e77ebe02ab [Pristupljeno: 22. 6.]

razvoja i šire primjene tih tehnologija će dakle ovisiti o brzini razvoja tehničkog dijela te tehnologije[53].

5.7 Društva temeljena na pametnim ugovorima

Zbog mogućnosti ugrađivanja određenih pravila, povezivanja ugovora te stavljanja novca na raspolaganje, zagovornici pametnih ugovora opisuju načine kako cijele organizacije i poduzeća temeljiti na pametnim ugovorima koji će biti dio *blockchain* sustava. Prema tome, moguće je takva društva definirati kao „organizaciju koja se pokreće pomoću pravila koja su programirana u računalne programe nazvane pametnim ugovorima"[54].

Primjeri takvih poduzeća se već mogu naći u praksi kao što su Dash governance, The DAO i Digix.io. Neki smatraju kako bi bilo poželjno strukturirati poduzeća na takav način da posluju bez ikakvog ljudskog uplitanja. U praksi takva poduzeća su zapravo kontrolirana od osoba koji glasaju posredovanjem sustava na *blockchainu* uz pomoć pametnih ugovora. Međutim, mora se pažljivo razmatrati pravna osnovanost takvog poduzeća kako se ne bi kršio zakon. Npr. u SAD-u su slična društva bila smatrana neregistriranim poduzećima koja ilegalno posluju. Trenutna alternativa bi bila poduzeće s neograničenom odgovornošću, što dosadašnjim korisnicima nije prihvatljiv izbor. Još jedan značajan problem odnosi se na velike poteškoće ispravljanja grešaka. Dosadašnje rješenje bi bilo prebacivanje svih sredstava na novi sustav s ispravljenim kôdom što stvara dodatnu kompleksnost[55].

Iako se ideja o decentraliziranim, autonomnim organizacijama ili poduzećima lako može iskoristiti za iskusne poduzetnike, također otvara vrata malim poduzetnicima i poduzetnicima koji su početnici koji bi mogli s manjim troškovima i s manjom količinom rizika otvoriti poduzeće. Ne smije se pritom zaboraviti kako će se te osobe susresti s povećanim rizicima kinetičkog kriminala te će biti pitanje hoće li se usprkos takvim rizicima i troškovima i dalje isplatiti koristiti takve tehnologije[56]. U budućnosti se očekuje sve veća aktivnost na tom

[53] https://medium.com/smartz-blog/how-blockchain-and-smart-contracts-can-impact-iot-f9e77ebe02ab [Pristupljeno: 22. 6.]

[54] Chohan, U. W. (2017). The decentralized autonomous organization and governance issues. Available at SSRN 3082055, str. 1. Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055 [Pristupljeno: 22. 6.]

[55] Opširnije vidjeti pod: Ibid.

[56] Opširnije vidjeti pod: Norta, A. (2016, November). Designing a smart-contract application layer for transacting decentralized autonomous organizations. In International Conference on Advances in Computing

području te jedan od pojmova koji pridobiva sve veću pažnju je Defi[57]. Aragon[58], makerDao[59], humanitydao[60], molochdao[61], compound.finance[62] su samo neki od važnih primjera koji se u praksi zalažu za decentralizirano rješavanje problema i napredak bez potrebe države.

5.8 Ostale mogućnosti korištenja pametnih ugovora

Kao što se iz prethodno iznesenih primjera može vidjeti, moguća primjena pametnih ugovora je veoma raznolika te se primjenjuje uz prisustvo raznih uređaja, strojeva ili baza podataka. Također, može se primijetiti kako koristi koje pametni ugovori mogu pružati nisu ograničene na poduzeća, već ih mogu iskoristiti i države i pojedinci.

Neka druga polja u kojima bi se pametni ugovori mogli iskoristiti bi npr. mogli biti[63,64,65]:

- prijavljivanje poreza
- prodaja nekretnina i prijepis vlasništva
- *online* kockanje
- autorstvo i intelektualno vlasništvo
- vrijednosnice (npr. derivati)
- trgovinsko poslovanje
- stambeni krediti

---

and Data Sciences (pp. 595-604). Springer, Singapore. Dostupno na: https://link.springer.com/chapter/10.1007/978-981-10-5427-3_61 [Pristupljeno: 22. 6.]

[57] Decentralized finance se odnosi na široku paletu projekata koji se zalažu za decentralizaciju financija što npr. uključuje kreditiranje.

[58] Aragon je open-source software projekt koji omogućava stvaranje i vođenje decentraliziranih organizacija. Opširnije vidjeti pod: https://breakermag.com/can-aragon-make-decentralized-autonomous-governance-work/ [Pristupljeno: 9. 9.]

[59] Cilj makerDao projekta su transparentne i održive financije. MakerDao uključuje kredite uz kolateral i upravljanje od strane zajednice. Opširnije vidjeti pod: https://makerdao.com/en/ [Pristupljeno: 9. 9.]

[60] HumanityDAO projekt uspostavlja standard za jedinstvene identitete na Ethereumu. Humanity registar može poslužiti kao temelj različitih radnji kao što su npr. krediti, glasanje itd. Opširnije vidjeti pod: https://www.stateofthedapps.com/dapps/humanitydao [Pristupljeno: 9. 9.]

[61] Molochdao je poseban po svojoj organizacijskoj strukturi koja djeluje slično poput inkubatora. Organizacija je potpuno demokratska te povezana pomoću pametnih ugovora. U središnjici se nalazi pametan ugovor koji zamjenjuje banku u koji članovi mogu alocirati resurse i izvlačiti ih ponovno. https://decrypt.co/5206/fixing-ethereum [Pristupljeno: 9. 9.]

[62] Compound.finance je otvoreni, autonomni protokol namijenjen programerima kako bi mogli stvarati nove aplikacije za financije. https://compound.finance/ [Pristupljeno: 9. 9.]

[63] https://ambisafe.com/blog/smart-contracts-10-use-cases-business/[Pristupljeno: 22. 6.]

[64] https://www.ccn.com/smart-contracts-12-use-cases-for-business-and-beyond/[Pristupljeno: 22. 6.]

[65] https://disruptionhub.com/smart-contract-uses/ [Pristupljeno: 22. 6.]

- ugovori o radu i slično.

Koji konkretni primjeri će se uistinu koristiti u praksi ovisit će o stupnju spremnosti poduzeća, država te pojedinačnih korisnika. Također, veliki utjecaj će imati brzina kojom se ta tehnologija razvija, postaje brža i jednostavnija za korištenje širim masama.

6. OPASNOSTI PRI KORIŠTENJU PAMETNIH UGOVORA

Iako pametni ugovori pružaju mnoge prednosti, ne smiju se zaboraviti opasnosti kojima se njihovi korisnici izlažu. Kako bi korisnici bili što spremniji za izbjegavanje ili sprječavanje tih opasnosti, pažljivo moraju razmotriti u kakvim se oblicima mogu pojaviti. Prema tome će se ukratko obraditi pametni ugovori koji po svome sadržaju nisu dopušteni, napadi na pametne ugovore te pametne ugovore u kojima je računalni kôd manjkav.

6.1 Mogućnosti prijevara uz korištenje pametnih ugovora

Prijevare se ne moraju isključivo dogoditi na tehničkoj sferi pametnih ugovora, već je moguće da problem leži u samom sadržaju ugovora. Prema tome mogu se razlikovati sljedeće kategorije kriminala za koje se ta tehnologija koristi[66]:

- krađa podataka i prodaja tajnih podataka
- krađa privatnih ključeva
- plaćanje za kriminalna djela koja se fizički izvršavaju u realnom svijetu (plaćena ubojstva, podmetanje požara i sl.).

Karakteristike zbog kojih bi kriminalne osobe mogle preferirati pametne ugovore su prvenstveno[67]:

- *Fair exchange* – ugovaratelji će biti sigurni da će se ugovor izvršiti zbog čega se manje moraju oslanjati na reputaciju druge strane što onemogućuje varanje te otežava državnu intervenciju u sprječavanju ugovora.
- *Minimalna interakcija* – dodatno otežava sprječavanje kriminala. Osoba je u mogućnosti da nakon pokretanja kriminalnog ugovora više nema potrebe intervenirati niti stupati u kontakt s drugim osobama koje bi potencijalno prijavile slučaj.
- *Mogućnost korištenja vanjskih podataka* – kao što je već objašnjeno u teoretskom dijelu[68] rada pametni ugovor može imati mogućnost provjere stanja izvršenja

[66] Juels, A., Kosba, A., & Shi, E. (2016, October). The ring of gyges: Investigating the future of criminal smart contracts. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 283-295). ACM, str. 2. Dostupno na: https://dl.acm.org/citation.cfm?id=2978362 [Pristupljeno: 11. 5.]
[67] Ibid., str. 4.
[68] Opširnije pod poglavljem rada: 4.2.

zahtijevanih kriterija zapisanih u ugovoru van svog sustava, što omogućuje provjeru i isplatu naknade za kaznena dijela.

Važno je dakle osvijestiti postojanje takvih ugovora kako bi se tražilo rješenje koje će ih otkloniti ili spriječiti. Nažalost, u ovom se kontekstu kriptovalute ističu zbog korištenja pseudonima kao novog načina pranja novca. Jedno moguće rješenje bi moglo biti označavanje jedinica određene kriptovalute za koju se zna da je povezana s kriminalnim radnjama[69] kako bi ih druge osobe aktivno mogle izbjegavati. Također, predlaže se mogućnost poništavanja takvih ugovora i njihovog brisanja s *blockchaina* uz uvjet većine glasova pri kojemu bi sudionici ostali anonimni ili odlukom određene autoritarne strane[70].

6.2 Napadi na pametne ugovore

Iako bi se pretpostavilo da napadi na takve sustave nisu mogući, postoji niz detalja koji bi se mogli iskoristiti kako bi se nepravedno uskratila sredstva drugoj osobi ili drugom računu. Zbog toga su važna ažuriranja sustava bilo da se radi o Ethereumu ili nekom drugom *blockchain* sustavu. Svakodnevno se mogu otkriti nove ranjivosti. Neki od primjera napada na pametne ugovore uključuju kašnjenje transakcija ili njihov pomak u redoslijedu u kojemu se zapisuju u *blockchain* mrežu. Kao problem se ističe što su dokumentacije o otkrivenim ranjivostima najčešće raspršene među mnogo izvora te korisnici pametnih ugovora najčešće zbog nedovoljnog znanja nisu niti svjesni napada koji se dogodio[71].

6.3 Manjkav kôd pametnih ugovora

Jedan od problema koji zahvaća osobe koji nisu programerskog obrazovanja ili nemaju dovoljno iskustva na tom polju su manjkavosti koje se događaju pri samom pisanju računalnog kôda pametnih ugovora. Dakle, ne radi se o prijevari jer ne dolazi do svjesne manipulacije kôdom.

[69] To znači da se direktno iskorištava svojstvo lančanosti transakcija pri čemu jedinice kriptovalute ne mogu biti odvojene od prošlih transakcija u kojima ih se koristilo.
[70] Opširnije vidjeti pod: Juels, A., Kosba, A., & Shi, E. (2016). o.c.
[71] Opširnije vidjeti pod: Atzei, N., Bartoletti, M., & Cimoli, T. (2016). A survey of attacks on Ethereum smart contracts. IACR Cryptology ePrint Archive, 2016, 1007. Dostupno na: http://kddlab.zjgsu.edu.cn:7200/research/blockchain/A%20Survey%20of%20Attacks%20on%20Ethereum%20Smart%20Contracts.pdf [Pristupljeno: 11. 5.]

Prema znanstvenom istraživanju u kojemu su istraženi računalni kodovi većeg broja pametnih ugovora, razlozi zašto bi pametni ugovor trošio više korisnikovog novca nego je potrebno mogu se podijeliti na kôd koji se nikad neće iskoristiti i manjkavi kôd povezan s petljama[72]. Nadalje, situacije s petljama koje čine pametan ugovor nepotrebno skupljim ponovno se mogu podijeliti na sljedeće[73]:

- skupe operacije su stavljene u petlju te svakim ponavljanjem nepotrebno poskupljuju izvršenje ugovora
- postojanje petlje za izračun bez obzira na to što će rezultat uvijek biti isti
- petlje koje se mogu spojiti u jednu su odvojene
- uspoređivanje rezultata unutar petlje kada je to suvišno.

Bilo da se radi o prijevari, neznanju ili slučajnosti, postoji mnogo mjesta za poteškoće pri korištenju pametnih ugovora. Zbog toga je važno pri njihovu pribavljanju pažljivo razmotriti izvore te stalno ažurirati softver koji se koristi kako bi se smanjio rizik povećanih troškova.

[72] U kontekstu programiranja petlje se koriste kako bi se smanjio obujam računalnog kôda. Umjesto da se linije ponavljaju, određene funkcije izvršavanje usmjere na takav način da se već napisane linije kôda iskoriste ponovno.

[73] Opširnije vidjeti pod: Chen, T., Li, X., Luo, X., & Zhang, X. (2017, February). Under-optimized smart contracts devour your money. In 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 442-446). IEEE. Dostupno na: https://www4.comp.polyu.edu.hk/~csxluo/Gasper.pdf [Pristupljeno: 11. 5.]

7. PRAVNO UREĐENJE PAMETNIH UGOVORA U REPUBLICI HRVATSKOJ

S obzirom na široku moguću primjenu i veliku apstraktnost koja se javlja vezano za pametne ugovore, postoji mnogo poteškoća i pitanja o tome kako kvalitetno regulirati pametne ugovore. Pri tome se može uzeti u obzir rješenje da se izdvoji poseban zakon koji bi regulirao isključivo pametne ugovore ili da se pametni ugovori dodaju u već postojeći zakon. Neke države su već poduzele određene mjere u regulaciji pametnih ugovora. Međutim, većina država još nema odredbi kojima bi ih regulirali, niti konkretne planove za njihovo uvođenje.

7.1 Regulacija pametnih ugovora

Primjer gdje možemo pametne ugovore naći u zakonu je država Nevada. U toj državi se zakonski priznaje *blockchain* tehnologija kao elektronički zapisnik podataka. Također, određeno je da su aktivnosti korištenja *blockchain* tehnologije neoporezive te da za to nije potreban ni certifikat ni ispunjenje bilo kakvih drugih uvjeta[74]. Pametan ugovor se također podrazumijeva pod elektroničkim zapisom koji se nalazi u *blockchainu* te se ne smije odbiti pravni učinak pametnog ugovora iz razloga što je *blockchain* korišten kako bi se taj ugovor kreirao, spremio, potvrdio pametni ugovor, njegov zapis ili potpis[75].

Na razini Europske unije i dalje ne postoji regulativa koja se bavi *blockchain* tehnologijom i pametnim ugovorima. U tijeku je projekt koji pokreće Europska komisija kojem je cilj postaviti okvire regulacije koje bi pomogle regulirati cjelokupnu Europsku uniju ili da se daju smjernice pojedinim zemljama članicama. Kako će se situacija razviti bez sustavnog rada na

[74] Vidjeti opširnije pod: Hyman, G. M., & Digesti, M. P. (2017). New Nevada legislation recognizes blockchain and smart contract technologies. Nev. Law., 25, 13-14. Dostupno na: https://www.nvbar.org/wp-content/uploads/NevadaLawyer_Aug2017_Blockchain-1.pdf?fbclid=IwAR32RvjI1h4nC5t02KyDmrmDL9baEPgFC95aETOS4KjgB2KOYfBYYw-9WzY [Pristupljeno: 22. 6.]

[75] https://bravenewcoin.com/insights/nevada-now-protects-blockchains-and-smart-contracts-from-government-taxes-licenses-and-certifications[Pristupljeno: 29. 6.]

razini Europske unije, kakvi zakoni bi se trebali predložiti i kako riješiti zakonsku nadležnost, samo su neka od pitanja na koja Europska komisija tim projektom želi naći odgovor[76]. Nadalje, u Republici Hrvatskoj ne postoji zakonsko rješenje za pitanja povezana s *blockchain* tehnologijom i pametnim ugovorima.

7.2 Pametni ugovori i ugovori u elektroničkom obliku

Kako bismo mogli dovesti pametne ugovore u vezu s pravnom regulativom Republike Hrvatske, moramo se osvrnuti na postojeće zakone koji reguliraju korištenje ugovora u elektroničkom obliku, te će se iz tog osvrta izvući zaključak je li za reguliranje pametnih ugovora u Republici Hrvatskoj potreban zaseban zakon ili se pametni ugovori mogu regulirati s već postojećim zakonima. Stoga će se prije svega razmotriti Zakon o obveznim odnosima[77] (u daljnjem tekstu ZOO) kao *lex generalis* Zakon kojim se uređuje sklapanje ugovora u elektroničkom obliku, te Zakon o elektroničkom potpisu[78] (u daljnjem tekstu ZEP), Zakon o elektroničkoj ispravi[79] i Zakon o elektroničkoj trgovini[80] (u daljnjem tekstu ZET) kao *lex specialis* zakoni koji se mogu primijeniti kod ugovora u elektroničkom obliku.

ZOO određuje da se ugovor može sklopiti u bilo kojem obliku, osim kada propisuje točan oblik ugovora[81]. Dodatno, prema ZOO-u za sklapanje ugovora u elektroničkom obliku vrijedi slijedeće:
(1) Ugovor je sklopljen elektroničkim putem kad su se strane suglasile o bitnim sastojcima.

[76] https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects [Pristupljeno: 29. 6.]
[77] Zakon o obveznim odnosima (NN 35/05, 41/08, 125/11, 78/15, 29/18). Dostupno na: https://www.zakon.hr/z/75/Zakon-o-obveznim-odnosima [Pristupljeno: 30. 6.] U daljnjem tekstu ZOO.
[78] Zakon o elektroničkom potpisu više nije na snazi. Zamijenjen je Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/17). Dostupno na: https://www.zakon.hr/z/923/Zakon-o-provedbi-Uredbe-%28EU%29-br.-910-2014-Europskog-parlamenta-i-Vije%C4%87a-od-23.-srpnja-2014.-o-elektroni%C4%8Dkoj-identifikaciji-i-uslugama-povjerenja-za-elektroni%C4%8Dke-transakcije-na-unutarnjem-tr%C5%BEi%C5%A1tu-i-stavljanju-izvan-snage-Direktive-1999-93-EZ [Pristupljeno: 30. 6.]
[79] Zakon o elektroničkoj ispravi (NN 150/05). Dostupno na: https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi [Pristupljeno: 30. 6.]
[80] Zakon o elektroničkoj trgovini (NN 173/03, 67/08, 36/09, 130/11, 30/14, 32/19). Dostupno na: https://www.zakon.hr/z/199/Zakon-o-elektroni%C4%8Dkoj-trgovini [Pristupljeno: 30. 6.] U daljnjem tekstu ZET.
[81] Oblik ugovora posebno je reguliran odredbama čl. 286. – 294. ZOO-a. O tome opširnije vidjeti Perkušič, M. (2019). o.c., str. 106.

(2) Ponuda učinjena elektroničkim putem smatra se ponudom nazočnoj osobi, ako se u konkretnom slučaju može na izjavu odmah dati protuizjava.
(3) Uporaba elektroničkog potpisa prilikom sklapanja ugovora uređuje se posebnim propisima[82].
Nadalje, ZOO uređuje osnovne obveznih odnosa u svojem općem dijelu i ugovorne i izvanugovorne odnose u svojem posebnom dijelu. Određena pravila koja su povezana s elektroničkim ugovorima se nalaze u zakonima koje slijede.

Kod pametnih ugovora ne može se govoriti o nijednoj postojećoj vrsti ugovora koju opisuje ZOO jer taj pojam sam po sebi nema sadržaj koji bi se mogao podvest pod vrstu ugovora u tom smislu. Također, kako pametan ugovor nema oblikovanu formu, ne može se ni prema tome razvrstati na neku određenu vrstu ugovora. Trenutno su pametni ugovori najsličniji ugovorima u elektroničkom obliku.

Izdvojeno iz ZOO-a se u ZET-u nalaze pravila u vezi sa sklapanjem ugovora u elektroničkom obliku i obveze društva koje ih koriste. Ugovori u elektroničkom obliku su ugovori što ih pravne i fizičke osobe u cijelosti ili djelomično sklapaju, šalju, primaju, raskidaju, otkazuju, pristupaju i prikazuju elektroničkim putem koristeći elektronička, optička ili slična sredstva, uključujući, ali ne ograničavajući se na prijenos internetom[83]. Ugovori u elektroničkom obliku se ne mogu primijeniti na sljedeće ugovore:
– imovinske, predbračne, odnosno bračne ugovore i druge ugovore koje uređuje Obiteljski zakon,
– ugovore o opterećenju i otuđenju imovine za koje je potrebno odobrenje centra za socijalnu skrb,
– ugovore o ustupu i raspodjeli imovine za života, ugovore o doživotnom uzdržavanju, ugovore o dosmrtnom uzdržavanju i sporazume u vezi s nasljeđivanjem, ugovore o odricanju od nasljedstva, ugovore o prijenosu nasljednog dijela prije diobe, oporučne poslove i druge ugovore koje uređuje Zakon o nasljeđivanju,
– darovne ugovore,
– ugovore o prijenosu prava vlasništva na nekretninama ili druge pravne poslove kojima se uređuju stvarna prava na nekretninama, osim ugovora o najmu i zakupu nekretnina,

[82] Čl. 293. st. 1 – 3. ZOO-a.
[83] Čl. 2. st. 6. ZET-a.

– druge ugovore za koje je posebnim zakonom propisano da se sastavljaju u obliku javnobilježničkog akta, odnosno isprave,
– ugovore i očitovanja volje jamaca, ako je jamac osoba koja djeluje izvan svoje trgovačke, poslovne ili profesionalne djelatnosti[84].

U ZET-u se slično kao u zakonu države Nevade dopušta pravnim subjektima korištenje elektroničkih ugovora bez licence[85]. Međutim, pri poslovanju uz ugovore u elektroničkom obliku se traže određene radnje koje mora obavljati informacijsko društvo. Od velike je važnosti da je informacijsko društvo posredno ili neposredno uvijek dostupno[86] te da obavlja nadzor nad sustavom i informacijama koje ulaze u sustav[87].

U ZET-u se nalaze ograničenja prema sadržaju kojeg bi pametni ugovori ukoliko se koriste kao ugovori u elektroničkom obliku imale. Uz to, problem se javlja pri obvezi nadzora informacijskog društva. Prednost pametnog ugovora bi trebala biti što u idealnom slučaju nema potreba skladištenja ni provjere informacija koje se u njima nalaze. Međutim, kako bi se spriječile prijevare i nedopuštene radnje, zakon traži nadzor podataka koje ulaze u sustav što se krši sa željom za privatnošću koju korisnici pametnih ugovora i *blockchain* sustava žele.

Zakonom o elektroničkoj ispravi uređuje pravo fizičkih i pravnih osoba na uporabu elektroničke isprave u svim poslovnim radnjama i djelatnostima te u postupcima koji se vode pred tijelima javne vlasti u kojima se elektronička oprema i programi mogu primjenjivati u izradi, prijenosu, pohrani i čuvanju informacija u elektroničkom obliku, pravna valjanost elektroničke isprave te uporaba i promet elektroničkih isprava[88]. Prema tome, elektronička isprava – jednoznačno povezan cjelovit skup podataka koji su elektronički oblikovani (izrađeni pomoću računala i drugih elektroničkih uređaja), poslani, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju, i koji sadrži svojstva kojima se utvrđuje izvor (stvaratelj), utvrđuje vjerodostojnost sadržaja te dokazuje postojanost sadržaja u vremenu. Sadržaj elektroničke isprave uključuje sve oblike pisanog teksta, podatke, slike i

[84] Čl. 9. st. 4. ZET-a.
[85] Čl. 5. st. 2. ZET-a.
[86] Čl. 6. st. 1. ZET-a.
[87] Čl. 21. st. 2. ZET-a.
[88] Čl. 1. st.1. ZEI-a.

crteže, karte, zvuk, glazbu i govor[89]. Elektronička isprava mora u svim radnjama uključenim u dokumentacijski ciklus osigurati:
– jednoznačno obilježje kojim se nedvojbeno utvrđuje pojedinačna elektronička isprava,
– jednoznačno obilježje kojim se nedvojbeno utvrđuje pojedinačni stvaratelj elektroničke isprave,
– informacijsku cjelovitost i nepovredivost elektroničke isprave,
– pristup sadržaju elektroničke isprave kroz cijelo vrijeme dokumentacijskog ciklusa,
– oblik zapisa koji čitatelju omogućuje jednostavno čitanje sadržaja[90].

Građa elektroničke isprave sastoji se obvezno od dva neodvojiva dijela:
– općeg dijela kojeg čini predmetni sadržaj (informacije u elektroničkom obliku) isprave. Uključuje i naslov primatelja ako je elektronička isprava namijenjena otpremi imenovanom primatelju,
– posebnog djela kojeg čine jedan ili više ugrađenih elektroničkih potpisa i podaci o vremenu nastajanja (završetka izrade) elektroničke isprave, kao i druga dokumentacijska svojstva[91].

Važno je da se svaka radnja s elektroničkom ispravom unutar dokumentacijskog sustava označi jedinstvenom oznakom i svojstvima koji se moraju ugraditi u elektroničku ispravu te koja osigurava izravnu povezanost prethodne i sljedeće radnje s elektroničkom ispravom[92].

Postavlja se pitanje gdje se kod pametnih ugovora mogu primijeniti pravila za elektroničke isprave. Iz razloga što pametan ugovor sam po sebi nije dokument, ne može se vidjeti kao isprava. Korištenjem *blockchain* sustava koji bi bio *online* u svakom trenutku bi se moglo udovoljiti nekima od traženih uvjeta. Također, podatke iz građe elektroničke isprave bi se trebale izvući iz *blockchain* zapisa na kojemu se pametan ugovor nalazi te bi *blockchain* sustav pružio uvid u povezanost isprava. Naposljetku je u ovom dijelu bitno naglasiti jednu dilemu. Ako je temeljna pretpostavka da nitko nema posebne ovlasti direktnog utjecaja na način rada i podatke koje se nalaze na *blockchainu* kako riješiti zahtjev da upravo mora postojati osoba koja bi mogla u situaciji greške ili prijevare zauzeti mjesto s posebnim ovlastima nad sustavom.

[89] Čl. 4. st. 1. ZEI-a.
[90] Čl. 6. ZEI-a.
[91] Čl. 7. ZEI-a.
[92] Čl. 14. st. 1.-2. ZEI-a.

Prema novom zakonu o elektroničkom potpisu određeno je za nadležno tijelo državna uprava nadležna za poslove e-Hrvatske[93,94] koja obavlja sljedeće poslove:
1. prijavljivanje i uklanjanje nacionalnih sustava za elektroničku identifikaciju Europskoj komisiji radi njihove objave u Službenom listu Europske unije
2. suradnja s tijelima za zaštitu osobnih podataka[95].

Dosada se prioritet e-Hrvatske odnosi na informatizaciju kojom se treba osigurati povezivanje informacijskih sustava tijela javne uprave iz svih sektora na način da se građanima pruži što veći broj kompleksnih e-usluga i smanji opterećenje građana u interakciji s javnom upravom[96].

Inspekcijski nadzor nad radom pružatelja usluga povjerenja i kvalificiranih pružatelja usluga povjerenja te nacionalnih sustava elektroničkih identifikacija u području prikupljanja, uporabe i zaštite osobnih podataka potpisnika provode inspektori i drugi državni službenici ovlašteni za provedbu nadzora određeni zakonom i drugim propisima kojima se uređuje zaštita osobnih podataka, u skladu s propisanim djelokrugom[97].

Prema ZEP-u svaki pružatelj usluga povjerenja ima obvezu:
1. omogućiti svakoj zainteresiranoj osobi uvid u identifikacijske podatke pružatelja usluga povjerenja
2. čuvati sve podatke i dokumentaciju o izdanim certifikatima najmanje deset godina od dana izdavanja, pri čemu podaci i prateća dokumentacija mogu biti i u elektroničkom obliku
3. primjenjivati odredbe zakona i drugih propisa kojima je uređena zaštita osobnih podataka[98].

U ovom dijelu rada postavlja se pitanje, tko bi mogao i kojim sredstvima pružiti uslugu povjerenja te kako bi se u pogledu pametnih ugovora mogla verificirati točnost podataka.

[93] Čl. 1. st. 1. ZEP-a.
[94] O e-Hrvatskoj se može opširnije vidjeti pod: https://uprava.gov.hr/o-ministarstvu/ustrojstvo/4-uprava-za-e-hrvatsku-1080/1080 [Pristupljeno: 28. 8.]
[95] Čl. 1. st. 2. ZEP-a.
[96] https://uprava.gov.hr/strategija-e-hrvatska-2020/14630 [Pristupljeno: 28. 8.]
[97] Čl. 7. st. 3. ZEP-a.
[98] Čl. 13. ZEP-a.

Korisnici blockchain sustava smatraju kako sami korisnici verificiraju podatke na način da nastave rudariti pomoću postojećih podataka. Međutim, Zakon traži verifikaciju pri objavljivanju podataka, a u ovom slučaju se podaci smatraju verificiranim sve dok ih netko ne opozove ili više ne obrađuje. Uz to, nema neposredne osobe ili društva koje bi moglo jamčiti odnosno preuzimati odgovornost za podatke koji su objavljeni. Za ova pitanja nisu samo odlučujući zakoni i odluke koje će donijeti Republika Hrvatska, već su od utjecaja mišljenja Europske komisije s kojima se moramo uskladiti.

Sumirajući, razlika između tradicionalnih i elektroničkih ugovora leži u mogućnostima digitalizacije koje se dopuštaju pri izradi i drugim radnjama. Međutim, ne propisuje se drugačiji oblik samog ugovora, već taj ostaje isti bez obzira je li ugovor sastavljen ili predan fizičkim ili elektronskim putem. Prividno se može dogoditi da forma izgleda skraćeno, ali u izvoru obvezujućeg dogovora se mora nalaziti pisani ugovor zakonski određene forme. Pametni ugovor na drugoj strani, nije napisan u obliku ugovora, već kao računarski kôd te kao takav ne može poslužiti kao ugovor. Pametni ugovor kao takav isključivo određuje način na koji će se izvršit ugovor, ali uz njega mora biti priložen pisani ugovor koji će biti dostupan svim stranama te biti prikazan pri davanju suglasnosti. U praksi se cijeli sadržaj ugovora može nalaziti i na drugom mjestu s naglaskom da mora postojati i u svakom trenu biti dostupan[99]. Tako se primjerice kod mikroosiguranja korisniku može prikazati na ekranu skraćeni prikaz dogovora, u pozadini se nalazi pametan ugovor koji će izvršiti dotični dogovor, a na klik korisnika mora biti dostupan ugovor pisan zakonski određenom formom koji predstavlja pravnu osnovu radnje osiguranja[100].

Iz svega navedenoga se može zaključiti kako bez obzira na prividnu sličnost pametnih ugovora i ugovora u elektroničkom obliku postojeći zakoni koji reguliraju ugovore nisu prikladni za reguliranje korištenja pametnih ugovora.

[99] Matić, T. (2008). Formularni ugovori u elektroničkom obliku (Sklapanje ugovora klikom miša-elektroničkim očitovanjem volje putem Interneta na web stranici–click wrap i browse wrap ugovori). Zbornik Pravnog fakulteta u Zagrebu, 58(3), str. 789. https://hrcak.srce.hr/22007 [Pristupljeno: 30. 6.]
[100] Vidi opširnije pod 5.4.

8. REZULTATI

1) *Pametni ugovori mogu se uspješno koristiti i u djelatnostima nevezanim za financije.*

U petom poglavlju rada pokazalo se da se pametni ugovori mogu koristiti u veoma različitim djelatnostima. Doseg ponajviše ovisi o potrebama osoba koje ih žele koristiti i zakonskoj regulativi države. Tako se pametnim ugovorima čak mogu rješavati poslovi koji spadaju u domenu država[101]. Najpoznatiji primjeri u praksi se odnose na financijsku djelatnost, ali u biti se radi o kupoprodajnim ugovorima koji se lako mogu oslikati na trgovanje bilo kakvim sredstvima ili imovinom. Također, pametni ugovori koji prate stanje financijskih tržišta kako bi automatski inicirali kupnju ili prodaju vrijednosnica su u biti veoma slični pametnim ugovorima koji npr. reguliraju rad stroja[102]. Uz regulaciju se trebaju razviti *oraclei* koji bi bili vjerodostojni, ostalo ovisi o mašti korisnika pametnih ugovora[103].

2) *Za korištenje pametnih ugovora je neophodan zaseban zakon kojim će se njihovo korištenje regulirati unutar državne legislative.*

Usprkos prividnom dojmu noviteta koji naziv *pametan ugovor* nosi, ne radi se o novom obliku ugovora, već o automatiziranom načinu izvršenja iza kojega se krije standardizirani tip ugovora koji je već definiran postojećim zakonima. Prema tome, nema potrebe sastavljanja posebnog zakona koji bi regulirao pametne ugovore, već bi trebalo definiciju pametnog ugovora kao načina izvršenja te definiciju *blockchain* tehnologije kao informacijskog sustava za pohranu i prijenos pametnih ugovora dodati u odgovarajući zakon. Dodavanje tih pojmova bi se preporučilo u ZOO-u s odgovarajućom referencom na ZET kao što je učinjeno s ugovorima u elektroničkom obliku. Dakle, moglo bi se u ZET dodati definicije pametnih ugovora i *blockchain* tehnologije. Također bi se kao npr. u Nevadi[104] trebalo priznati *blockchain* sustav kao valjan davatelj elektroničkih potpisa što se mora dodati u odgovarajući zakon. Uz to se i podaci s *blockchain* sustava trebaju priznati kao legitimni podaci koji imaju svoju snagu kako u svojstvu informacije pa sve do dokazne snage u sudskom postupku. Ako se nadležna tijela slože na dopuštenje korištenja pametnih ugovora u djelatnostima na koje se

[101] Opširnije pod poglavljem rada: 5.3.
[102] Opširnije pod poglavljem rada: 5.6.
[103] Opširnije pod poglavljem rada: 4.2.
[104] Opširnije pod poglavljem rada: 7.1.

odredbe ugovora u elektroničkom obliku izričito ne odnose (kao što je npr. građevinska industrija u kojoj postoji veliki potencijal za pametne ugovore), može se svaka pojedinačna djelatnost dodatno regulirati u posebnom zakonu. Na taj način se nova tehnologija može dio po dio prenijeti u djelatnosti koje su i prethodno posebno regulirane što se tiče elektroničkog ugovaranja.

3) *Pametni ugovori kao način izvršavanja i čuvanja ugovornih obveza mogu smanjiti poteškoće i prijevare koje se događaju u obveznom pravu.*

Usprkos tome što mnogi kriptovalute smatraju samo još jednim novim sredstvom za lakše izvršavanje i plaćanje kriminalnih radnji[105], postoje mnoge prednosti pametnih ugovora te *blockchain* tehnologije na kojima se temelji koje bi mogle imati veći pozitivan od negativnog utjecaja. Problem manjkavog kôda[106] te napada na pametne ugovore[107] prirodno će se riješiti napretkom tehnologije te sve veće standardiziranosti u kôdu pametnih ugovora. Zbog toga se treba staviti veći naglasak na napredak koji te tehnologije donose. A već prijelazom s Bitcoin *blockchaina* na Ethereum[108] mogu se primijetiti znatna poboljšanja koja pridonose snazi i sigurnosti korištenja pametnih ugovora. Pomoću *blockchain* tehnologije već sada postoji mogućnost za sasvim novu razinu transparentnosti i nemogućnost falsificiranja podataka[109]. Koristeći te značajke, razina prijevara može se znatno smanjiti, pogotovo ako se tehnologija koristi sustavno i na što široj razini.

[105] Opširnije pod poglavljem rada: 6.1.
[106] Opširnije pod poglavljem rada: 6.3.
[107] Opširnije pod poglavljem rada: 6.2.
[108] Opširnije pod poglavljem rada: 4.1.2.
[109] Opširnije pod poglavljem rada: 4.1.1.

9. ZAKLJUČAK

Pametni ugovor je način na koji fizička ili javna osoba može izvršiti ugovorne odredbe automatizirano, držeći sve podatke na distribuiranoj bazi podataka zvanoj *blockchain*. Za razliku od ugovora u elektroničkom obliku, ne radi se o vrsti ugovora, već o načinu izvršenja ugovora koji se mora zasebno sklopiti. Samim time dolazi se do zaključka da nije potreban poseban zakon koji bi uredio pametne ugovore jer bi se njihovo dodavanje u regulativu Republike Hrvatske u svojoj biti nadovezalo na Zakon o obveznim odnosima, Zakon o elektroničkoj trgovini, Zakon o elektroničkoj ispravi i naslijeđe Zakona o elektronskom pečatu.

S obzirom na činjenicu da se pametni ugovori koriste u raznim djelatnostima koje uključuju također građevinu, osiguranje, tržište kapitala i slično koje su izuzete od odredbi Zakona o elektronskoj trgovini, treba se razmotriti dodavanje posebnih odredbi u pojedinačne zakone kako bi se omogućilo korištenje pametnih ugovora u tim djelatnostima. Naravno, takvo nadopunjavanje zakona morat će se izvršiti nakon prethodne procjene državnih tijela odgovornih za e-Hrvatsku jer bi nesrazmjer u napretku tehnologije u odnosu na sigurnosne mjere doveo do prenagle i visoke razine opasnosti za njezine građane.

Međutim, ako se promjene dogode s dovoljno pažnje i vremena za prilagodbu, pametni ugovori donose mnogo prednosti. Transparentnost podataka i nepromjenjivost unesenoga čine ih načinom izvršenja obveza koji sadrži nepovredivo jamstvo. Time se može stvoriti okvir za djelovanje ne samo fizičkih i pravnih osoba, već i djelovanje države na sustavnoj razini koja omogućuje transparentniju i efikasniju državu koja ulijeva povjerenje.

10. LITERATURA

Znanstveni članci:

1. Atzei, N., Bartoletti, M., & Cimoli, T. (2016). A survey of attacks on Ethereum smart contracts. IACR Cryptology ePrint Archive, 2016, 1007. Dostupno na: http://kddlab.zjgsu.edu.cn:7200/research/blockchain/A%20Survey%20of%20Attacks%20on%20Ethereum%20Smart%20Contracts.pdf [Pristupljeno: 11. 5.]
2. Biryukov, A., Khovratovich, D., & Tikhomirov, S. (2018). Privacy-preserving KYC on Ethereum. Dostupno na: https://pdfs.semanticscholar.org/8aa3/5a333495bda6fca2e75cbae6d7a3ffc62b7f.pdf [Pristupljeno: 16.06.]
3. Blocher, W. (2016). The next big thing: blockchain–bitcoin–smart contracts. *Anwaltsblatt*, *66*(8), 9. Dostupno na: https://www.it-businesstalk.at/wp-content/uploads/AnwBl-2016-612_Blocher.pdf [Pristupljeno: 8. 6.]
4. Buterin, V. (2013). Ethereum white paper. GitHub repository, 22-23. Dostupno na: https://eprint.iacr.org/2016/1007.pdf [Pristupljeno: 23. 5.]
5. Cardeira, H. (2015). Smart contracts and their applications in the construction industry. Dostupno na: https://heldercardeira.com/1503P.pdf [Pristupljeno: 15. 6.]
6. Chen, T., Li, X., Luo, X., & Zhang, X. (2017, February). Under-optimized smart contracts devour your money. In 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 442-446). IEEE. Dostupno na: https://www4.comp.polyu.edu.hk/~csxluo/Gasper.pdf [Pristupljeno: 11. 5.]
7. Chohan, U. W. (2017). The decentralized autonomous organization and governance issues. Available at SSRN 3082055. Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055 [Pristupljeno: 22. 6.]
8. Corkery, M., & Silver-Greenberg, J. (2014). Miss a Payment? Good Luck Moving That Car. *New York Times*. Dostupno na: https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/ [Pristupljeno 16. 6.]
9. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough?. *Future Internet*, *10*(2), 20. Dostupno na: https://scholar.google.hr/scholar?hl=hr&as_sdt=0%2C5&q=Blockchain+and+Smart+

Contracts+for+Insurance%3A+Is+the+Technology+Mature+Enough%3France_Is_the_Technology_Mature_Enough&btnG= [Pristupljeno: 9. 6.]

10. Hyman, G. M., & Digesti, M. P. (2017). New Nevada legislation recognizes blockchain and smart contract technologies. Nev. Law., 25, 13-14. Dostupno na: https://www.nvbar.org/wp-content/uploads/NevadaLawyer_Aug2017_Blockchain-1.pdf?fbclid=IwAR32RvjI1h4nC5t02KyDmrmDL9baEPgFC95aETOS4KjgB2KOYfBYYw-9WzY [Pristupljeno: 22. 6.]
11. Juels, A., Kosba, A., & Shi, E. (2016, October). The ring of gyges: Investigating the future of criminal smart contracts. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 283-295). ACM. Dostupno na: https://dl.acm.org/citation.cfm?id=2978362 [Pristupljeno: 11. 5.]
12. Mason, J., & Escott, H. (2018). Smart contracts in construction: views and perceptions of stakeholders. In Proceedings of FIG Conference, Istanbul May 2018. FIG. Dostupno na: http://eprints.uwe.ac.uk/35123/ [Pristupljeno: 15. 6.]
13. Matić, T. (2008). Formularni ugovori u elektroničkom obliku (Sklapanje ugovora klikom miša-elektroničkim očitovanjem volje putem Interneta na web stranici–click wrap i browse wrap ugovori). Zbornik Pravnog fakulteta u Zagrebu, 58(3), 779-803. Dostupno na: https://scholar.google.hr/scholar?hl=hr&as_sdt=0%2C5&q=Formularni+ugovori+u+elektroni%C4%8Dkom+obliku+%28Sklapanje+ugovora+klikom+mi%C5%A1a+-+elektroni%C4%8Dkim+o%C4%8Ditovanjem+volje+putem+Interneta+na+web+stranici+%E2%80%93+click+wrap+i+browse+wrap+ugovori%29&btnG=#d=gs_cit&u=%2Fscholar%3Fq%3Dinfo%3AcOxSqSYutYAJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Dhr [Pristupljeno: 30. 6.]
14. Möhlenkamp, M., Wessel, T. (2018): Smart Contracts in der Versicherung – Chancen und rechtliche Herausforderungen. Wilhelm Rechtsanwälte. Dostupno na: https://www.wilhelm-rae.de/sites/default/files/pdf/versicherungspraxis_-_smart_contracts_in_der_versicherung_-_mai_2018.pdf [Pristupljeno: 8. 6.]
15. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Dostupno na: https://bitcoin.org/bitcoin.pdf [Pristupljeno: 23. 5.]
16. Norta, A. (2016, November). Designing a smart-contract application layer for transacting decentralized autonomous organizations. In International Conference on Advances in Computing and Data Sciences (pp. 595-604). Springer, Singapore.

Dostupno na: https://link.springer.com/chapter/10.1007/978-981-10-5427-3_61 [Pristupljeno: 22. 6.]

17. Oriwoh, E., & Conrad, M. (2015). 'Things' in the Internet of Things: towards a definition. International Journal of Internet of Things, 4(1), 1-5. Dostupno na: http://article.sapub.org/10.5923.j.ijit.20150401.01.html [Pristupljeno: 16. 6.]
18. Perkušič, M.(2019): Pravna pitanja elektroničkog plaćanja. Sveučilište u Rijeci, pravni fakultet.
19. Raskin, M. (2016). The law and legality of smart contracts. Dostupno na: https://www.ilsa.org/ILW/2018/CLE/Panel%20%2311%20-%20THE%20LAW%20AND%20LEGALITY%20OF%20SMART%20CONTRACTS%201%20Georgetown%20Law%20Technology%20Rev.._.pdf [Pristupljeno: 11. 5.]
20. Werbach, K., & Cornell, N. (2017). Contracts ex machina. Duke LJ, 67, 313. Dostupno na: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj [Pristupljeno: 8. 6.]
21. Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *Available at SSRN 2580664*. Dostupno na: https://poseidon01.ssrn.com/delivery.php?ID=670117070070069028074121019118080120031047031042055074081065125024121065069000085124049107118055103025009099114079106120083118028035061021010081089102065087095112112003008009002100098091084090102026123031099001073029100096010070079028112072116115029103&EXT=pdf [Pristupljeno: 8. 6.]
22. Matić, T. (2008). Formularni ugovori u elektroničkom obliku (Sklapanje ugovora klikom miša-elektroničkim očitovanjem volje putem Interneta na web stranici–click wrap i browse wrap ugovori). Zbornik Pravnog fakulteta u Zagrebu, 58(3), 779-803. https://hrcak.srce.hr/22007 [Pristupljeno: 30. 6.]

Internetske stranice:

1. https://ambisafe.com/blog/smart-contracts-10-use-cases-business/[Pristupljeno: 22. 6.]
2. https://bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offer-blockchain-notarization-services-to-e-residents-1448915243?fbclid=IwAR3uwOBPjFJ3Dji5kBaZzU8cmberTXVmQsYqOnDEpz7gGY9ojQs0lYMyuwY [Pristupljeno: 19. 6.]

3. https://blog.oraclize.it/identity-on-the-blockchain-chapter-3-585bc5c7e2c7?fbclid=IwAR0jUlELSQiiKeolvlZWsoP5IuzQz_EM4De0ayiP4CaYoQOfSDqvAvUorhQ [Pristupljeno: 19. 6.]
4. https://bravenewcoin.com/insights/nevada-now-protects-blockchains-and-smart-contracts-from-government-taxes-licenses-and-certifications[Pristupljeno: 29. 6.]
5. https://cointelegraph.com/news/bitnation-registers-first-refugees-on-the-blockchain?fbclid=IwAR3eRj7s-OaIQmuRRtz33hD0t2Jj1ymTphQACLgAXfknreNM66_9hdipvcA [Pristupljeno: 19. 6.]
6. https://cointelegraph.com/news/estonian-e-residency-and-bitnation-launch-new-public-notary-in-blockchain-jurisdiction?fbclid=IwAR10lQrT2Afq5aJtGzNClOL20Pu_TxA1guPUQrXxebQVIjzYUvqTep5z98g [Pristupljeno: 19. 6.]
7. https://disruptionhub.com/smart-contract-uses/ [Pristupljeno: 22. 6.]
8. https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects[Pristupljeno: 29. 6.]
9. https://medium.com/codechain/modified-merkle-patricia-trie-how-ethereum-saves-a-state-e6d7555078dd [Pristupljeno 12. 6.]
10. https://medium.com/smartz-blog/how-blockchain-and-smart-contracts-can-impact-iot-f9e77ebe02ab [Pristupljeno: 22. 6.]
11. https://www.ccn.com/smart-contracts-12-use-cases-for-business-and-beyond/[Pristupljeno: 22. 6.]
12. https://www.finextra.com/pressarticle/69173/deloitte-develops-blockchain-proof-of-concept-to-mutualise-kyc-checksleft [Pristupljeno: 19. 6.]
13. https://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923?fbclid=IwAR2k3Z82G1kZ54jIAv8zIG5qplG2VYeJP-vnYsl92fuqSsRHlsRIgJVX1CU [Pristupljeno: 19. 6.]
14. https://uprava.gov.hr/o-ministarstvu/ustrojstvo/4-uprava-za-e-hrvatsku-1080/1080 [Pristupljeno: 28. 8.]
15. https://uprava.gov.hr/strategija-e-hrvatska-2020/14630 [Pristupljeno: 28. 8.]

Zakoni:

1. Zakon o elektroničkoj ispravi (NN 150/05). Dostupno na: https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi [Pristupljeno: 30. 6.]
2. Zakon o elektroničkoj trgovini (NN 173/03, 67/08, 36/09, 130/11, 30/14, 32/19). Dostupno na: https://www.zakon.hr/z/199/Zakon-o-elektroni%C4%8Dkoj-trgovini [Pristupljeno: 30. 6.]
3. Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/17). Dostupno na: https://www.zakon.hr/z/923/Zakon-o-provedbi-Uredbe-%28EU%29-br.-910-2014-Europskog-parlamenta-i-Vije%C4%87a-od-23.-srpnja-2014.-o-elektroni%C4%8Dkoj-identifikaciji-i-uslugama-povjerenja-za-elektroni%C4%8Dke-transakcije-na-unutarnjem-tr%C5%BEi%C5%A1tu-i-stavljanju-izvan-snage-Direktive-1999-93-EZ [Pristupljeno: 30. 6.]
4. Zakon o sprječavanju pranja novca i financiranju terorizma (NN 108/17, 39/19). Dostupno na: https://www.zakon.hr/z/117/Zakon-o-sprje%C4%8Davanju-pranja-novca-i-financiranju-terorizma [Pristupljeno: 19. 6.]
5. Zakon o obveznim odnosima (NN 35/05, 41/08, 125/11, 78/15, 29/18). Dostupno na: https://www.zakon.hr/z/75/Zakon-o-obveznim-odnosima [Pristupljeno: 30. 6.]

11. SAŽETAK

Mogućnosti i opasnosti korištenja pametnih ugovora

U radu je ukratko prikazana povijest pametnih ugovora. Kako bi njihov način rada bio jasniji, prikazani su Bitcoin *blockchain* te novosti koje je donio Ethereum, jedan od *blockchain* sustava koji se najčešće koristi kao temelj pametnih ugovora. Također, uz primjere iz prakse prikazana su neka od područja u kojima bi se pametni ugovori mogli koristiti. Potom se rad osvrnuo na moguće opasnosti i zloupotrebe koje pametni ugovori omogućuju. Kao zaključni dio rada obrađena je usporedba pametnih ugovora i ugovora u elektroničkom obliku kako bi se dao zaključak o kompatibilnosti načina rada pametnih ugovora sa zakonodavstvom Republike Hrvatske.

ključne riječi: *blockchain*, Ethereum, pametni ugovori, ugovori u elektroničkom obliku

12. SUMMARY

Possibilities and dangers of using smart contracts

This paper presents a brief overview of the history of smart contracts. In order to make the way smart contracts work clearer, the Bitcoin blockchain is presented, as well as the new features brought by Ethereum, one of the blockchain systems most commonly used basis for smart contracts. Also, with some examples of real-world practices, some of the areas where smart contracts could be used are shown. Then the paper reviewed possible dangers and frauds that smart contracts allow. As a concluding part of the paper, a comparison of smart contracts and electronic contracts is made to provide a conclusion on the compatibility of smart contract practices with the legislation of the Republic of Croatia.

Keywords: blockchain, Ethereum, smart contracts, electronic contracts

13. ŽIVOTOPIS

OSOBNE INFORMACIJE Mamut, Jelena

Put Mulina 33, 21220 Trogir (Hrvatska)

+385 21 884 865 +385 91 512 1199

jelena.mamut1994@gmail.com

www.linkedin.com/in/jelena-mamut-b48555176

Datum i mjesto rođenja: 29. 3. 1994. Köln (Njemačka)

RADNO ISKUSTVO

02/09/2019 – Danas — Analitičar u Odjelu revizije
Deloitte d.o.o., Zagreb (Hrvatska)

11/03/2019 – 15/03/2019 — Stručna praksa
Porezna uprava, Područni ured Split, Split (Hrvatska)
- odjel za plan i analizu
- odjel za porez na dobit
- odjel za suzbijanje poreznih prijevara
- odjel za ovrhu

22/05/2017 – 18/09/2018 — Referent za njemačko tržište
Adriagate d.o.o., Split (Hrvatska)
- rad u odjelu prodaje
- rad u odjelu korisničke službe i reklamacija
- telefonska komunikacija i komunikacija elektroničkom poštom na hrvatskom, njemačkom i engleskom jeziku s klijentima i B2B partnerima

01/03/2017 – 31/03/2017 — Stručna praksa
AD Plastik d.d., Solin (Hrvatska)
- računovodstvo u proizvodnom sektoru
- prijava poreza na dobit i PDV
- proces konsolidacije financijskih izvještaja i revizije

01/10/2016 – 25/11/2016 — Agentica u pozivnom centru
Euroherc osiguranje d.d., Split (Hrvatska)
- telefonska prodaja

- priprema obračuna cijene osiguranja obveznog automobilskog osiguranja
- davanje informacija o proizvodima

OBRAZOVANJE I OSPOSOBLJAVANJE

02/10/2017 – Danas

Magistar forenzike (smjer: Financijsko-računovodstvena forenzika)

Sveučilišni odjel za forenzične znanosti, Split (Hrvatska)

- gospodarski kriminalitet i kazneno pravo
- pisanje znanstvenih radova
- forenzično računovodstvo
- porezni sustav i politika

01/10/2015 – 16/10/2017

Magistar ekonomije (smjer: Financijski menadžment)

Ekonomski fakultet Split, Split (Hrvatska)

- znanje o financijskim tržištima i investicijama
- engleski za računovodstvo i financije
- korištenje statističkog programa SPSS

Naziv diplomskog rada: „Utjecaj strukture kapitala na profitabilnost poduzeća”

01/10/2012 – 31/09/2015

Prvostupnica ekonomije (smjer: Financijski menadžment)

Ekonomski fakultet Split, Split (Hrvatska)

- osnove ekonomije i računovodstva
- matematika i statistika u ekonomiji
- poslovni njemački

OSOBNE VJEŠTINE

Materinski jezik: njemački, hrvatski

Strani jezici

	RAZUMIJEVANJE		GOVOR		PISANJE
	Slušanje	Čitanje	Govorna interakcija	Govorna produkcija	
engleski	B1	B2	B1	B1	B1
francuski	A2	B1	A2	A2	A2

Stupnjevi: A1 i A2: Početnik - B1 i B2: Samostalni korisnik - C1 i C2: Iskusni korisnik

Zajednički europski referentni okvir za jezike

Komunikacijske vještine

- dobre sposobnosti engleskog jezika zbog volontiranja na konferenciji Blocksplit (27. – 28. 4. 2018.)

Organizacijske / rukovoditeljske vještine

- član Studentskog zbora, sastavnice Sveučilišnog odjela za forenzične znanosti
- tajnica studentske udruge IMEF i voditeljica tima za financije

Digitalne vještine

SAMOPROCJENA				
Obrada informacija	Komunikacija	Stvaranje sadržaja	Sigurnost	Rješavanje problema
Samostalni korisnik	Temeljni korisnik	Temeljni korisnik	Samostalni korisnik	Temeljni korisnik

Digitalne vještine – tablica za samoprocjenu

- dobro znanje korištenja programa Microsoft Office (Word, Excel, Outlook, OneNote)

Vozačka dozvola

B

DODATNE INFORMACIJE

Priznanja i nagrade

Rektorova nagrada Sveučilišta u Splitu za izvrsnost u akademskoj godini 2017./2018.

Tečajevi

Sprječavanje pranja novca i financiranje terorizma u financijskom sektoru – održan na akademiji Zagrebačke burze 12. 2. 2019.

Prezentacije

„Računovodstveni skandal Parmalat" u sklopu događaja Otvoreni dani forenzike kao studentska predstavnica prve godine smjera Financijsko-računvodstvene forenzike na Sveučilišnom odjelu za forenzične znanosti

Certifikati

Jezična diploma njemačkog jezika Goethe instituta za razinu C2

14. IZJAVA O AKADEMSKOJ ČESTITOSTI

SVEUČILIŠTE U SPLITU

Sveučilišni odjel za forenzične znanosti

Izjava o akademskoj čestitosti

Ja, Jelena Mamut, izjavljujem da je moj diplomski rad (zaokružite odgovarajuće) pod naslovom Mogućnosti i opasnosti korištenja pametnih ugovora

rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ičija autorska prava.

Izjavljujem da nijedan dio ovoga rada nije iskorišten u ijednom drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Split, 13.9.2019

Potpis studenta/studentice: Jelena Mamut

15. POPIS SLIKA

Slika 1. Prikaz *blockchain* lanca 6
Slika 2. Shematski prikaz Merkle Tree sustava 7
Slika 3. Prikaz primjera Bitcoin javnog i privatnog ključa 10
Slika 4. Prikaz Ethereum modified Merkle-Paricia-trie sustava 13