MOGUĆNOSTI KORIŠTENJA I PRAVNOG UREĐENJA TAKOZVANIH PAMETNIH UGOVORA U REPUBLICI HRVATSKOJ

Perkušić, Marko; Jozipović, Šime; Mamut, Jelena

Source / Izvornik: **Hrvatsko obvezno pravo u poredbenopravnom kontekstu: petnaest godina Zakona o obveznim odnosima, 2022, 665 - 694**

Book chapter / Poglavlje u knjizi

Publication status / Verzija rada: **Published version / Objavljena verzija rada (izdavačev PDF)**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:487796

POGLAVLJE 18.

MOGUĆNOSTI KORIŠTENJA I PRAVNOG UREĐENJA TAKOZVANIH PAMETNIH UGOVORA U REPUBLICI HRVATSKOJ

Doc. dr. sc. Marko Perkušić*
Doc. dr. sc. Šime Jozipović**
Jelena Mamut***

SAŽETAK

U poglavlju se analizira pojam i način funkcioniranja tzv. pametnih ugovora te se kroz primjere iz prakse prikazuju neka od područja u kojima bi se oni mogli koristiti. Posebno se objašnjava *blockchain* tehnologija budući da je ona omogućila širu primjenu pametnih ugovora te i dalje ostavlja prostora za njihov budući razvoj u kreditnom, građevinskom i drugim sektorima. Posebna pozornost posvećena je ključnim svojstvima i pravnoj kategorizaciji pametnih ugovora te pravnim pitanjima zlouporabe i grešaka u sustavu. Kako je razvoj tzv. pametnih ugovora tek u svojim začecima, mnogi problemi za predmetna pitanja i dalje nisu riješeni. Stoga poglavlje kritički analizira postojeći pravni okvir u Republici Hrvatskoj i daje konkretne sugestije za implementaciju pravne regulative pametnih ugovora u domaćem zakonodavstvu. Autori zaključuju da se pametni ugovori moraju regulirati u skladu s njihovom svrhom i oblikom. Pritom je izrazito bitno uzeti u obzir razliku između pametnih ugovora utemeljenih na javnom sustavu i onih utemeljenih na privatnom ili hibridnom sustavu. Također je bitno uzeti u obzir i pravnu kategorizaciju pametnih ugovora koji uglavnom predstavljaju sredstvo izvršenja ugovorne obveze, ali iznimno i determiniraju sam sadržaj ugovora.

KLJUČNE RIJEČI: pametni ugovor, *blockchain*, Ethereum, ugovor u elektroničkom obliku, *oracle*, *contractware*.

1. UVOD

Takozvani pametni ugovori (*smart contracts*) predstavljaju jedan od ključnih izazova današnjice za pravne sustave širom svijeta. Kao koncepti koji povezuju

* Dr. sc. Marko Perkušić, docent na Sveučilištu u Splitu, Sveučilišnom odjelu za forenzične znanosti. ORCID: https://orcid.org/0000-0002-5845-2961.

** Dr. sc. Šime Jozipović, docent na Ekonomskom fakultetu Sveučilišta u Splitu, Katedri za management. ORCID: https://orcid.org/0000-0000-0002-8050-5134.

*** Jelena Mamut, mag. oec., mag. forens., poslovni administrator u Adria Docks d.o.o. ORCID: https://orcid.org/0000-0002-8056-8653. Poglavlje se temelji na istraživanju koje je koautorica provela pri izradi diplomskog rada: Jelena Mamut, „Mogućnosti i opasnosti korištenja pametnih ugovora" (diplomski rad, Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti, 2019.).

informatičke sustave s pravnim učincima, pametni ugovori mogu imati dalekosežne učinke te nije moguće predvidjeti sve potencijalne oblike njihove primjene. U ovom će se poglavlju nastojati utvrditi način i smjer u kojemu bi se trebalo ići pri reguliranju pametnih ugovora. Pri tome će se prije svega utvrditi što su to pametni ugovori, kako su nastali i razvijali se, način na koji funkcioniraju, kao i mogućnosti te opasnosti njihove primjene u praksi. Na koncu, iz provedene analize, izvršit će se podjela pametnih ugovora prema različitim oblicima (sustavima) njihovog korištenja te će se ispitati mogućnosti primjene već postojećih zakonskih okvira na pametne ugovore, a sve u cilju izvođenja zaključka o smjeru i načinu na koji bi ih trebalo regulirati.

2. POVIJESNI RAZVOJ I NAČIN FUNKCIONIRANJA TAKOZVANIH PAMETNIH UGOVORA

2.1. POČETAK RAZVOJA TAKOZVANIH PAMETNIH UGOVORA

Sam koncept tzv. pametnih ugovora bitno je stariji od modernog pravnog diskursa i platformi poput Ethereuma.[1] Naime, već 1999. godine kriptograf Nick Szabo iznio je koncept tzv. Božjeg protokola kojim bi se dvjema ili više stranama omogućilo da posluju na način da u sustav unose isključivo one informacije koje su potrebne za konkretno poslovanje, dok bi se nakon izvršenja transakcije omogućio transparentan uvid u sve faktore koji su doveli do izvršenja protokola.[2] Pametni su ugovori dakle zamišljeni primarno kao sredstvo ostvarenja decentralizirane digitalne razmjene dobara i usluga koje omogućava informacijski minimalizam.[3] Iako koncept pametnih ugovora dakle već postoji preko dvadeset godina, tek je *bitcoin*, odnosno *blockchain* tehnologija[4] na kojoj se ta kriptovaluta temelji, pametnim ugovorima omogućio iskorak iz teorije u praksu.

---

1 Opširnije o tome v. pod 2.3.

2 Opširnije v. u Walter Blocher, „The next big thing: Blockchain – Bitcoin – Smart Contracts" (2016.) 66 *Anwaltsblatt* 612.

3 Pod informacijskim minimalizmom podrazumijeva se sustav u kojem se objavljuju samo one informacije koje su ključne za provedbu same transakcije. Detaljnije o načinu funkcioniranja ovoga sustava i unosu informacija v. Marko Perkušić, „Pravna pitanja elektroničkog plaćanja" (doktorska disertacija, Pravni fakultet Sveučilišta u Rijeci, 2019.), 394–399.

4 *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.

2.2. BITCOIN *BLOCKCHAIN*

Bitcoin kao kriptovaluta i *blockchain* tehnologija stvoreni su kako bi se riješio tzv. *double-spending problem*. Prvi znanstveni rad na ovu temu, „Bitcoin: A Peer-to-Peer Electronic Cash System",[5] opisuje predmetni problem kako slijedi. Kada određena osoba ima novčana sredstva u digitalnome obliku (primjerice novac na računu) i želi izvršiti transakciju drugoj osobi, druga osoba bez centralnog sustava ne može biti sigurna jesu li predmetna sredstva već iskorištena za drugu transakciju. Zbog toga u klasičnim digitalnim transakcijama u svrhu rješenja ovog problema nastupaju banke kao posrednici koji u svojim sustavima bilježe svaku pojedinačnu transakciju (brisanje sredstava s jednog računa i dodavanje predmetnih sredstava na drugi račun). Suprotno tome, *blockchain* tehnologija dopušta isključenje posrednika iz sustava u cijelosti. Naime, svaka transakcija u sustavu se bilježi kao javno dostupna dodatna karika u nizu (novi *block* u *chainu*) te sadrži podatke o prijenosu sredstava. Umjesto središnjeg sustava (baze podataka banaka), potvrdu o transakciji i postojanju sredstava mora dati većina decentraliziranog sustava mreže putem sustava Merkle Tree, odnosno *hasha*.[6] Iako su transakcije javne, pa korisnici *blockchaina* nemaju klasičnu razinu zaštite osobnih podataka u smislu bankovne tajne, kod svih transakcija isključivo je vidljiv javni ključ (kôd) računa s kojega je transakcija izvršenja (tzv. elektroničkog novčanika, odnosno *walleta*).[7] Time korisnici umjesto anonimnosti zapravo postižu pseudonimnost.

Za obavljanje transakcija u *blockchainu* potrebna su tri elementa koja zajednički osiguravaju sigurnost transakcija bez povjerenja u pojedinačne pripadnike sustava:[8] baza podataka (*ledger*), mreža računa (*network*) i pravilnik (*consensus*). Naime, pravilnikom je definirano da tzv. rudari – sudionici računalne mreže koji dodaju nove blokove u bazu podataka, moraju riješiti zahtjevan računski zadatak *proof-of-work* kako bi definirali *hash* vrijednosti. Specifičnost takvog zadatka jest u

---

5 Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin Project: White Paper*, 31. 10. 2008.) <https://bitcoin.org/bitcoin.pdf> (pristupljeno 21. 6. 2021.).

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

7 Elektronički novčanik kao novčanik uobičajeno označava softver koji u sebi čuva ključeve svog korisnika te mu dopušta provedbu raznih transakcija.

8 Opširnije v. u Kevin Werbach i Nicolas Cornell, „Contracts *ex machina*" (2017.) 67 *Duke Law Journal* 313.

tome da je kalkulacija rješenja izrazito složena, dok je provjera ispravnosti rješenja jednostavna. Ostatak mreže tako jednostavno može provjeriti ispravnost izračunate vrijednosti i potvrditi valjanost *blockchaina*. Za svaku valjanu transakciju, protokol automatski nagrađuje rudara u obliku dodjeljivanja određene jedinice kriptovalute kojom se vrše transakcije na predmetnom *blockchainu*.

Ukratko se funkcioniranje dodavanja novih blokova može zapisati na sljedeći način:[9]

- Svako računalo u sustavu ima pospremljen cijeli *blockchain*.
- U određenom trenutku računala dobiju obavijest o novoj transakciji.
- Svako računalo sakuplja nove transakcije u blokove.
- Svako računalo radi na *proof-of-work* zadatku.
- Kada neko računalo pronađe rješenje zadatka, šalje novi blok svim ostalim računalima.
- Druga računala taj će blok potvrditi jedino ako su sve transakcije u njemu valjane i nisu prethodno već potrošene.
- Računala izražavaju potvrdu bloka na način da počinju raditi na sljedećem bloku koji će u sebi sadržavati *hash* potvrđenog bloka kao *hash* svog prethodnika.

2.3. ETHEREUM

Ethereum je sustav koji je zamišljen kao nadogradnja Bitcoin *blockchain* sustava, na način da omogući svakome pisanje pametnih ugovora i decentraliziranih aplikacija.[10] Jedno od najvećih ograničenja Bitcoina je nedostatak petlji u kodu koje bi dopustile sustavno programiranje koda. Međutim, uvođenje petlji predstavlja sigurnosni rizik koji zahtijeva posebne sigurnosne mjere. Upravo Ethereum sustav uvodi petlje i odgovarajuće sigurnosne mjere uz nekoliko drugih inovacija. Naime, pored navedenog valja naglasiti da je Bitcoin *value-blind* što znači da nije uvijek moguće odrediti točan iznos UTXO-a[11] koji će biti isplaćen, dok Ethereum nema ovaj problem. Nadalje, u Ethereum sustavu uveden je tzv. *state awareness* kojim je ispravljen tzv. *lack of state* problem[12] koji je značio da određena

[9] Nakamoto (bilj. 5), 3.

[10] O tome opširnije v. u Vitalik Buterin, „Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform" (*Ethereum White Paper*, 2014.) <https://ethereum.org/en/whitepaper/> (pristupljeno 21. 6. 2021.).

[11] *Unspent transaction outputs* – vrijednost koja je proizašla rudarenjem, ali još nije korištena za nijednu transakciju.

[12] Buterin (bilj. 10), 12.

transakcijska vrijednost može biti jedino isplaćena ili neisplaćena, bez mogućnosti izvršenja višeslojnih transakcija.

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 *escrow* pametne ugovore, odnosno pametne ugovore koji se ponašaju kao skrbnički računi te npr. dok se pretpostavke ugovora ne ispune, čuvaju određenu količinu novca.[13] Kao drugo, Ethereum poruka može sadržavati podatke. Kao treće, primatelj Ethereum poruke, ako se radi o *contract accountu*,[14] 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.[15] 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, svi će se učinci 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 Ethereum sustavu jest *first class citizen* koji označava da će i sami pametni ugovori moći slati poruke i kreirati nove pametne ugovore.[16]

Ukratko, koraci odvijanja transakcije u Ethereumu mogu se zapisati kako slijedi:[17]

- Provjera ispravnosti transakcije, valjanosti potpisa i slaganja podataka s podacima pošiljateljevog računa. Ako provjera nekog od elemenata dobije negativan rezultat, korisniku se vraća poruka s greškom.
- Izračun naknade transakcije (STARTGAS*GASPRICE) i određivanje

13 Werbach i Cornell (bilj. 8), 344–345.

14 *Contract account* je korisnički račun koji u biti pripada pametnom ugovoru koji onda može izvršavati određene radnje.

15 *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 v. Brionne Lawson, „What is Gas: An overview of Gas and how it is used on the blockchain" (*MyEtherWallet*) <https://help.myetherwallet.com/en/articles/5878945-what-is-gas> (pristupljeno 21. 6. 2021.).

16 Opširnije v. u Buterin (bilj. 10), 22–23.

17 Ibid., 15.

pošiljatelja prema potpisu. Oduzimanje naknade od pošiljateljevog računa i promjena pošiljateljevih podataka. Ako nema dovoljno sredstava na računu, korisniku se vraća poruka s greškom.
- Inicijalizacija GAS = STARTGAS te oduzimanje određene količine *gasa* po bajtu da bi se platili bajtovi u transakciji.
- 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 kôd tog ugovora do njegovog završetka ili iscrpljenja *gasa*.
- Ako se transfer ne dovrši jer pošiljatelj nema dovoljno novca ili kôd ostane bez *gasa*, sve se promjene vrate na stanje prije transfera osim plaćenih naknada koje se dodaju na račun rudara.
- U suprotnom slijedi vraćanje naknada preostalog *gasa* pošiljatelju te se naknada za vraćanje tog *gasa* pripisuje rudaru.

Iako su Ethereum i Bitcoin veoma slični u kontekstu arhitektura njihovog *blockchain* sustava, postoji velika razlika u smislu spremanja podataka. Nasuprot sustavu Merkle Tree koji koristi Bitcoin *blockchain*, Ethereum koristi Patricia Tree. U Ethereum sustavu blokovi sadrže kopiju liste transakcija i najnovije stanje. Grafički prikaz tog pristupa izgleda kao stablo pri kojem se mijenjaju zadnje karike kod svake transakcije. Kako bi se pristupilo upisanim podacima, koriste se pokazivači unutar stabla. U konačnici, kako je stanje zapisano u svakom zadnjem bloku, nema potrebe zapisivanja cijele *blockchain* povijesti što u odnosu na Bitcoin štedi prostor na računalima. Za razliku od Bitcoinovog Merkle Treea, koji sačinjavaju *hash* podaci, kod Ethereumovog modificiranog sustava mogu se i dodavati i brisati zapisi.[18]

3. POJAM TAKOZVANIH PAMETNIH UGOVORA

Iako je osnovni koncept tzv. pametnih ugovora prilično jednostavan, u praksi ih je teško jedinstveno definirati. Predmetna problematika rezultat je izrazite raznolikosti oblika koje bi mogli poprimiti pametni ugovori, ali i dualne prirode pametnih ugovora koji imaju svoju pravnu, ali i tehničku dimenziju. Tako bi se primjerice moglo postaviti pitanje predstavljaju li već transakcije unutar Bitcoinovog *blockchaina* svojevrsne transakcije putem jednostavnih pametnih ugovora.

[18] Ibid., 9–10.

3.1. VOLJA UGOVORNIH STRANA KAO TEMELJNI KRITERIJ RAZGRANIČENJA POJMA PAMETNOG UGOVORA OD PRAVNOG POJMA UGOVORA

U tehničkom smislu pametni su ugovori niz linija računalnog koda koji su namijenjeni koordinaciji postupaka dviju ili više strana na način da se međusobno preuzete obveze ispune.[19] U pravnoj teoriji zastupljeno je i stajalište kako su pametni ugovori uistinu i pravno gledano ugovori jer predstavljaju sredstvo izvršenja pravno predvidivih i unaprijed definiranih prava i obveza, definirano od strane ugovornih strana.[20]

Konkretna pravna definicija pojma pametnog ugovora neupitno će ovisiti o shvaćanju pojma ugovora u nacionalnome zakonodavstvu pojedine države. Stoga je teško predodrediti pravni status pametnog ugovora kao pravno valjanog ugovora ili računalnog koda koji služi provedbi ugovora. Međutim, polazeći od hrvatske pravne tradicije, ugovor predstavlja usuglašenje volja ugovornih strana oko postizanja dopuštenih pravnih učinaka. Dakle, sadržaj ugovora je ono oko čega ugovorne strane postignu sporazum, a za očekivati je da će sporazum postići upravo oko shvaćanja onoga što će određeni kôd izvršiti (primjerice, transfer određene kriptovalute između dva računa ako se ostvare određeni preduvjeti), a ne oko samog sadržaja teksta koda. Stoga zaključno, iz svega navedenog smatramo kako pametni ugovori prvenstveno nisu ugovor ili oblik ugovora, već način provedbe ugovora, pa stoga pametne ugovore možemo definirati kao način izvršenja unaprijed definiranih kriterija i uvjeta na koje dvije ili više strana pristaju kako bi se samostalno izvršili pomoću računalnog koda koji se nalazi na *blockchain* mreži.

Bitno je naglasiti da predmetna razlika nije isključivo teoretske prirode. Naime, za očekivati je da pametni ugovori kao svi oblici računalnog koda mogu imati grešku (tzv. *bug*), temeljem koje dolazi do različitog ishoda od onoga koji je prethodno bio zamišljen od ugovornih strana (primjerice, preuranjeno ispunjenje ili neispunjenje). Kako je ugovor između strana međutim „sporazum oko očekivanih učinaka koda", a ne „pristanak na bilo koje učinke koje bi kôd mogao imati", takva transakcija, iako bi se provela, ne bi bila izvršena na temelju ugovora te bi oštećenoj strani pripadao pravni zahtjev za povratom danoga temeljem odredbi o stjecanju bez osnove.

---

19 Werbach i Cornell (bilj. 8), 330.

20 Ibid., 338–343.

Upravo u navedenome kontekstu valja spomenuti postojanje razlike između tzv. jakih i slabih pametnih ugovora. Naime, jaki pametni ugovori izvršit će se bez obzira na volju strana jer se njihovo izvršenje ne može spriječiti ili bi sprječavanje bilo neekonomično. Dakle, greška u kodu ne može se ispraviti za vrijeme odvijanja pametnog ugovora. Suprotno tomu, na izvršenje slabih pametnih ugovora, ugovorne strane ili javna vlast mogu utjecati na način da postignu ishod koji može biti različit od onoga ovisnog o kodom definiranih pretpostavki za njegovo izvršenje.[21] Iako bi upravo opcija odbijanja mogućnosti naknadnog utjecaja na kôd mogla biti indikator za to da su ugovorne strane zapravo pristale na „bilo koje učinke koje bi kôd mogao imati", do ovakvog zaključka ipak se ne može doći. Naime, enormna većina ugovornih strana nije u stanju razumjeti sve učinke nekog računalnog koda, već će redovito umjesto samostalne izrade pametnog ugovora koristiti tzv. *contractware*, dakle softver sa sadržajem pametnog ugovora izrađen od strane trećega.[22] Stoga će ugovorne strane već pri sklapanju ugovora imati zamisao o tome što će određeni kôd (pametni ugovor) izvršiti. Drugim riječima, nije želja ugovornih strana da pravne učinke podrede pametnome ugovoru, već da pametni ugovor služi provedbi zamišljenih pravnih učinaka. Dakle, nije za očekivati da određena ugovorna strana izvrši ozbiljnu transakciju s ciljem pristanka na rizik ishoda koji nije unaprijed mogla očekivati. Stoga sklapanje jakog pametnog ugovora zapravo samo indicira volju ugovornih strana za nesmetanom provedbom, ali ne isključuje pravo strana na pravnu zaštitu u slučaju nastupa neočekivanih učinaka pametnog ugovora.

Od gore navedenog valja upozoriti i na jednu iznimku, odnosno slučaj u kojemu se u praksi može pokazati da je pametni ugovor (dakle sami kôd) jednak sadržaju ugovora u pravnome smislu. Drugim riječima, ugovorne strane su složne oko toga da se pristupi isključivo provedbi koda te da faktički učinci koda budu ujedno i željeni pravni učinci. Kao što je već naglašeno, da bi se to moglo ostvariti, obje bi ugovorne strane morale pristati „na bilo koje učinke koje bi kôd mogao imati". Dakle, sami kôd, uključujući moguće *bugove*, definirao bi sadržaj ugovora, a činjenica da ugovorna strana nije proučila upravo taj kôd bila bi izjednačena sa slučajem u kojemu ugovorna strana nije pročitala sadržaj nekog pisanog ugovora. Osim više teoretskog slučaja u kojemu bi ugovorne strane zajednički pristupile

[21] Max Raskin, „The Law and Legality of Smart Contracts" (2017.) 1 *Georgetown Law Technology Review* 305, 310.

[22] Ibid., 307.

pisanju koda kao što inače pristupaju pisanju ugovora, postoji međutim i jedna u praksi relevantna situacija u kojoj može doći do ovog scenarija.

Naime, samo je potrebno zamisliti decentralizirani sustav temeljen na *blockchainu* u kojemu ugovorne strane nemaju direktnu komunikaciju, već nastupaju isključivo pseudonimno, kroz interakciju putem pametnog ugovora, ali ne i izravno. Primjerice, zamislimo burzu virtualnih valuta utemeljenu na decentraliziranome pametnome ugovoru. Nazovimo predmetni pametni ugovor *x-contract*. Taj *x-contract* radi po principu da bilo koja osoba može unijeti u decentralizirani sustav određeni broj X *coinova* te navesti javni ključ digitalnog novčanika i iznos druge virtualne valute koju želi primiti u predmetni digitalni novčanik. Primjerice, osoba 1 pseudonimno unese 10 x *coinova* u *x-contract* i navede da traži da se prebaci 0.1 *bitcoin* u digitalni novčanik pod brojem 1111111. Sada bilo koja druga osoba koja sudjeluje u decentraliziranome sustavu *x-contracta* može zatražiti priliku za ispunjenjem predmetnoga ugovora, odnosno prihvatiti predmetnu ponudu i to na način da u *blockchain* unese broj svog digitalnog novčanika u sustavu *x-contracta* i digitalnog novčanika s kojega će prenijeti 0.1 *bitcoin*. Ako osoba 2 pseudonimno ispuni transakciju 0.1 *bitcoina* u digitalni novčanik 1111111, *x-contract* će automatski izvršiti transakciju 10 x *coinova* na digitalni novčanik osobe 2.

Osoba 1 i 2 se međusobno ne poznaju te je gotovo pa isključeno da jedna osoba može saznati identitet druge osobe. Osobe su u sustav isključivo unijele digitalne podatke (kriptovalute i javne ključeve), ne navodeći željene pravne učinke. Sustav je decentraliziran te nema niti jedne konkretne osobe odgovorne za izvršenje transakcije. Osoba 1 i 2 nisu nikako drugačije usuglasile svoje volje, osim što su obje pristale sudjelovati u sustavu *x-contracta*.

U navedenome slučaju, ugovorne strane se nisu složile oko apstraktnog koncepta transakcije, već oko toga da učinak transakcije u cijelosti „daju u ruke“ pametnome ugovoru jer znaju da bilo koja greška sustava ne može naknadno biti ispravljena, niti će naknadno moći zatražiti učinkovitu pravnu zaštitu zbog pseudonimne prirode sustava. Dakle, ugovorne strane pristaju svjesno na sve očekivane i neočekivane učinke ugovora. Time je sadržaj ugovora „izvršenje kôda“, odnosno drugim riječima, pametni ugovor je jednak sadržaju ugovora u pravnome smislu.

3.2. VANJSKE BAZE PODATAKA I PAMETNI UGOVORI

Usko povezan s korištenjem pametnih ugovora je također pojam *oracle*.[23] Pod ovim pojmom podrazumijevaju se eksterne baze podataka koje mogu sadržavati podatke u vezi sa sudskim ili arbitražnim odlukama, stanjem na određenim tržištima kapitala ili robe, ili druge podatke kojima obje strane ugovora vjeruju. Tako se na primjer za podatak o temperaturi u određenom mjestu može koristiti baza podataka određene mrežne 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.[24]

4. MOGUĆNOSTI PRIMJENE PAMETNIH UGOVORA

Sam način funkcioniranja pametnih ugovora objasnili smo pomoći kriptovaluta *bitcoin* i *ether*.[25] Međutim, iako je sama tehnologija i ideja za uspješno korištenje pametnih ugovora nastala kao način efikasnijeg korištenja kriptovaluta, pametni ugovori počinju se sve više koristiti i izvan sfere kriptovaluta. Tako se pametni ugovori koriste, ili se njihova upotreba razmatra:

- kod uređaja koji onemogućuju pokretanje motornih vozila[26]
- pri različitim konceptima dubinskih analiza[27]

---

[23] Aaron Wright i Primavera De Filippi, „Decentralized Blockchain Technology and the Rise of Lex Cryptographia“ (2015.), 50 <https://ssrn.com/abstract=2580664> (pristupljeno 21. 6. 2021.).

[24] Ibid., 14.

[25] V. odjeljke 2.2. i 2.3.

[26] V. odjeljak 4.1.

[27] Sukladno čl. 15. st. 1. Zakona o sprječavanju pranja novca i financiranju terorizma, NN 108/2017. i 39/2019. (dalje u tekstu: ZSPNFT), dubinska analiza između ostalog obuhvaća utvrđivanje identiteta stranke i provjeru 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. U znanstvenoj

- kod razvoja e-rezidentnosti[28]
- u sektoru osiguranja[29]
- u građevinskoj industriji[30]
- kao način upravljanja najrazličitijim uređajima na automatiziran i unaprijed definiran način koji se sastoje od linija računalnog kôda spremljenih na *blockchain* mreži[31]
- kod trgovačkih društava temeljenih na pametnim ugovorima[32]
- u brojnim drugim područjima.[33]

Stoga ćemo u ovom dijelu poglavlja prikazati određene primjere i načine na koje bi se mogle iskoristiti prednosti pametnih ugovora za rješavanje nekih dosadašnjih problema ili za poboljšanje trenutnih rješenja.

---

literaturi ističe se kako bi korištenje pametnih ugovora potencijalno moglo omogućiti da se dubinska analiza može provesti bez zadiranja u privatnost osoba nad kojima se ta dubinska analiza provodi. O tome opširnije v. u Alex Biryukov, Dmitry Khovratovich i Sergei Tikhomirov, „Privacy-preserving KYC on Ethereum" (2018.) 2 (12) *Reports of the European Society for Socially Embedded Technologies* <https://dl.eusset.eu/handle/ 20.500.12015/3165> (pristupljeno 21. 6. 2021.).

28 E-rezidentnost (*e-Residency*) je projekt koji je nastao u Estoniji, a zasniva se na suradnji s organizacijom Bitnation. Cilj projekta je omogućiti osobama (bez obzira na njihovu nacionalnost) dobivanje e-rezidentnosti koja ne označava identitet na području Estonije, već na području Bitnationa. U sklopu e-rezidentnosti nalazi se program infrastrukture za javne ključeve koji je započela estonska vlada. Korisnici dobiju pametnu karticu, takozvanu Digi-ID koja u sebi sadržava digitalne certifikate koji potvrđuju osobne podatke vlasnika kartice. Pametne kartice povezane su s Ethereum adresama koje se povezuju i s osobnim podacima osoba koje ih koriste. Navedene pametne kartice omogućuju osobama i pokretanje ili primanje transfera, a sve to je temeljeno na pametnim ugovorima koji su potrebni za verifikaciju podataka te se izgubljena kartica može poništiti i izdati nova. O projektu e-rezidentnosti v. Jelena Mamut, „Mogućnosti i opasnosti korištenja pametnih ugovora" (diplomski rad, Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti, 2019.), 20–21.

29 V. odjeljak 4.2.

30 V. odjeljak 4.3.

31 Radi se o dosta apstraktnom pojmu koji se spominje u znanstvenoj literaturi, a kao primjer njegovog korištenja mogu se navesti senzori na vozilu koji bi automatski mogli prijaviti kvar te tako aktivirati naručivanje dijelova za popravak vozila. O tome opširnije v. Edewede Oriwoh i Marc Conrad, „'Things' in the Internet of Things: Towards a Definition" (2015.) 4 (1) *International Journal of Internet of Things* 1; Valentina Gatteschi i dr., „Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?" (2018.) 10 (2) *Future Internet* 1, 7.

32 V. odjeljak 4.4.

33 V. odjeljak 4.5.

4.1. UREĐAJI KOJI ONEMOGUĆUJU POKRETANJE MOTORNIH VOZILA

Jedan od mogućih oblika primjene pametnih ugovora (u financijskom poslovanju) može se naći kod SID-ova (*starter interrupt device* – uređaj koji onemogućuje pokretanje motornog vozila) koje sve učestalije koriste kreditne institucije ili *leasing* društva pri prodaji motornih vozila.[34] Pomoću takvih uređaja omogućuje se osobama koje inače nemaju pristup kreditnom ili drugom financiranju kupnje motornih vozila (visoko rizičnim dužnicima) pristup potrebnim sredstvima, uz istovremeno umanjenje rizika davatelja kredita odnosno *leasinga*.

S ekonomskog aspekta, SID-ovi omogućuju smanjivanje troškova institucijama koje su vlasnici vozila jer se ne moraju oslanjati na službe za prisilni povrat objekta *leasinga*. Takvi procesi mogu biti skupi i dugotrajni te dovesti u opasnost osoblje tih službi. U SID uređajima uobičajeno je ugrađen i GPS uređaj kako bi se mogla utvrditi točna lokacija vozila u trenutku gašenja ili već prije gašenja. Iz razloga što kreditori vozila imaju bitno manje troškove pronalaska i povrata vozila, mogu nuditi takve vrste financiranja uz manje kamate. U pogledu na praktičnu primjenu valja naglasiti da prve analize primjene predmetnih sustava već indiciraju da primjena SID uređaja dovodi do urednijeg plaćanja od strane dužnika.[35]

Pored navedenih pozitivnih učinaka SID-ova, postoje međutim i negativne strane primjene ovih uređaja. Tako nedovoljna obaviještenost o točnim uvjetima i rokovima u kojima će se primijeniti blokada putem SID-ova izaziva nelagodu i nesigurnost na strani dužnika. Nadalje, u slučaju loše ugradnje postoji rizik da se vozilo i tijekom vožnje isključi. Također, neki su od dužnika naveli da kôd koji im je dan od kreditora kako bi vozilo ipak u hitnoj situaciji mogli koristiti nije uvijek bio ispravan. Valja naglasiti da unatoč smanjenom riziku troškovi financiranja i dalje mogu biti izrazito visoki u odnosu na druge oblike kreditiranja.[36] Nadalje, valja naglasiti rizike vezane za zaštitu privatnosti korisnika vozila. Kada su u vozilo ugrađeni SID uređaji koji sadrže i GPS uređaj, kreditori imaju mogućnost stalnog praćenja kretanja vozila. Stoga postoji opasnost da kreditori takve podatke koriste bez obzira na temeljnu svrhu njihova prikupljanja.[37]

---

34 V. Michael Corkery i Jessica Silver-Greenberg, „Miss a Payment? Good Luck Moving That Car" (*The New York Times*, 24. 9. 2014.) <https://archive.nytimes.com/dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/> (pristupljeno 21. 6. 2021.).

35 Ibid.

36 Ibid.

37 Yvonne Colbert, „Privacy group wants better regulation for GPS starter interrupt

Zbog svega navedenoga, već sada se u literaturi javljaju određene preporuke vezane za odnos između kreditora i korisnika kredita osiguranog SID-om, i to:[38]

- obavezno postojanje internog ili eksternog osoblja koje će pravilno ugraditi sve uređaje
- preporuka da ugovornu dokumentaciju prije sklapanja ugovora pregleda stručna osoba – odvjetnik korisnika kredita
- uspostava sustava provjere kojim se utvrđuje je li korisnik vozila dobio svu potrebnu dokumentaciju te je li upoznat s time kako uređaj radi i koje radnje treba poduzeti u hitnim situacijama
- provjera pravne utemeljenosti u državnoj legislativi
- sustav zaštite od diskriminacije pri odlučivanju o potrebi ugradnje SID-a
- sustavno prikupljanje i obrada reklamacija i prigovora
- dubinska analiza društava koja prodaju SID uređaje
- upozorenje osiguratelju koji troškovi mogu proizaći temeljem korištenja SID uređaja.

Iz iznesenoga se teško može predvidjeti hoće li u konačnici prevagnuti prednosti ili nedostaci SID uređaja. Najveći problem prvotno predstavlja nedostatak regulacije tog područja što stvara nesigurnost za njegove korisnike čija se vozila ponekad i bez najave više ne mogu koristiti. Drugi 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 moći će se prenijeti u pametni ugovor. Prema tome će korisnici vozila biti sigurni da će se pametni ugovor izvršiti točno onako kako je određeno ugovorom. Primjenom *blockchain* sustava mogla bi se osigurati zaštita privatnosti kroz pseudonime i enkripciju podataka, a moderni pametni ugovori mogu se stvoriti u takvome obliku da budu „slabi" u odnosu na organe državne vlasti u slučaju promjena zakonske regulative. Pitanje koje će se međutim morati riješiti je definicija sustava hitnog odobrenja upravljanja blokiranim vozilom. Naime, poseban će biti izazov odrediti kriterije hitnosti i pretočiti ih u funkcionalan pametni ugovor. Naime, ako se jednostavno definira odredba prema kojoj korisnik vozila mora uputiti zahtjev osoblju financijske institucije koja odobrava

devices" (*CBC News*, 13. 8. 2018.) <www.cbc.ca/news/canada/nova-scotia/gps-starter-interrupters-privacy-technology-laws-1.4780860> (pristupljeno 21. 6. 2021.).

[38] Eric L. Johnson i Corinne Kirkendall, „Starter Interrupt and GPS Devices: Best Practices" (*PassTime Blog*, 14. 1. 2016.) <https://passtimegps.com/blog/starter-interrupt-and-gps-devices-best-practices/> (pristupljeno 21. 6. 2021.).

privremeno korištenje vozila, i dalje postoji opasnost od iskorištavanja moći od strane osoblja, a time pametni ugovor gubi na samostalnosti zbog koje je prvotno i uveden.

4.2. OSIGURANJE

Sektor osiguranja predstavlja jedno od područja s najvećim potencijalom za uključivanje pametnih ugovora i *blockchain* tehnologije. Tako, primjerice, osiguravajuća društva već mogu koristiti KYC[39] pri aplikacijama koje rade pomoću sustava temeljenih na pametnim ugovorima. U neka od područja osiguranja kojima će pametni ugovori pridonijeti može se ubrojiti područje rizika od više sile. Osiguratelj može ugradnjom senzora za mjerenje temperature i sličnih uređaja ili koristeći treće strane za podatke automatizirati proces isplate odštete na način da npr. ako temperatura doseže ili padne pod određenu razinu, dođe do aktivacije ugovora. Na taj se način poljoprivrednici mogu osigurati za slučaj lošeg uroda bez potreba postavljanja posebnog odštetnog zahtjeva. Na sličan način mogu se riješiti štete na autu pomoću uređaja za mjerenje padalina (krupe).[40] Još jedno područje u kojem pametni ugovori mogu postići pozitivne učinke je transportno osiguranje. Zbog učestalih promjena u okolnostima slučaja, osiguratelji imaju poteškoća u ostvarenju pravovremenih izmjena opsega usluga korisniku osiguranja. Posljedica toga je da su korisnici često previše ili premalo osigurani. Pomoću pametnih ugovora korisnik osiguranja sam može u sustav unijeti promijenjene značajke te dobiti promjenu usluga trenutno. Još jedan primjer bilo bi povezivanje s ovlaštenim mehaničarima kako bi se isplata odštete za popravak motornog vozila automatizirano mogla isplatiti.[41]

Ako bi se dodatno iskoristile prednosti kriptovaluta, otvara se mogućnost mikroosiguranja. Tako bi motorno vozilo moglo biti osigurano samo onoliko dugo koliko se koristi ili bi osoba plaćala za putno osiguranje automatski kada prijeđe granicu pa sve do povratka u tuzemstvo. Nadalje bi se korištenjem pametne odjeće (*smartweara*) poput pametnih satova mogle mjeriti biološke značajke pojedinca te vršiti preračunavanje premija osiguranja putem pametnih

[39] Radi se konceptu *know-your-customer* koji se primjenjuje pri dubinskoj analizi.

[40] Magdalena Möhlenkamp i Tobias Wessel, „Smart Contracts in der Versicherung – Chancen und rechtliche Herausforderungen“ (*Wilhelm Rechtsanwälte*, 7. 5. 2018.) <www.wilhelm-rae.de/de/aktuelles/smart-contracts-in-der-versicherung-chancen-und-rechtliche-herausforderungen> (pristupljeno 21. 6. 2021.).

[41] Opširnije v. u Gatteschi i dr. (bilj. 31).

ugovora. Postoji također mogućnost da se *blockchain* tehnologija koristi za P2P[42] način međusobnog osiguranja bez uključivanja financijske institucije (osiguravajućeg društva) u transakciju.[43]

Temeljem svih iznesenih potencijalnih oblika primjene, može se zaključiti kako je razvoj pametnih ugovora za sektor osiguranja tek u nastanku te uvelike ovisi o povezivanju pametnih ugovora s materijalnim mjernim sustavima. 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 posebno morati brinuti o potencijalnim opasnostima prijave pri unošenju podataka u sustav pametnog ugovora.

4.3. GRAĐEVINSKA INDUSTRIJA

Građevinska industrija je karakteristična po svom financijskom ciklusu koji zahtijeva velika početna ulaganja u fazi izgradnje koja se nadomještaju naknadno kroz najam ili prodaju nekretnine. Pitanja primjene pametnih ugovora u ovome sektoru obrađena su u znanstvenoj literaturi na slučaju rumunjskog građevnog sektora. Nacionalna istraživanja provedena u ovoj državi pokazala su kako uzrok najvećih poteškoća te stečaja građevinara leži u poremećajima plaćanja tijekom gradnje. Tako je učestala pojava nedostupnost novčanih sredstava u trenutku kada su potrebni za dovršetak zgrade te tada dolazi do stečaja manjih društava uključenih u gradnju ili kašnjenja zbog nemogućnosti kupnje materijala. Kako ovaj problem značajno opterećuje cijeli sektor, među zakonskim prijedlozima našao se i plan tzv. građevinskog *trusta* koji bi bio zadužen za nadzor i plaćanje među sudionicima gradnje. Međutim, ideja za takvo tijelo nije provedena u praksi. Zbog toga autori predlažu pametne ugovore koji bi osigurali da novac za izgradnju ostane u pripravnosti, sve dok radnici ne potvrde u sustavu ispunjenje zahtijevanih kriterija. Naročito bi se ovim putem moglo povezati niz ugovora u svrhu stvaranja mreže koja uključuje sve sudionike i dijelove gradnje.[44]

---

[42] Izraz *peer to peer* koristi se kada se transfer vrši direktno od osobe do osobe bez korištenja intermedijara.

[43] Opširnije v. u Gatteschi i dr. (bilj. 31).

[44] Opširnije v. u Helder Cardeira, „Smart contracts and possible applications to the construction industry" (2015.) 1 (1) *Romanian Construction Law Review* 35.

Ukratko se prednosti korištenja pametnih ugovora mogu svesti na sljedeće:[45]

- postoji jamstvo da su sredstva uplaćena te su ona kroz cijeli vremenski proces gradnje dostupna za plaćanje
- zaštita izvođača radova, svih podizvođača te dobavljača na način da nisu moguća kašnjenja u plaćanjima ili eventualno neplaćanje
- zaštita različitih sudionika od insolventnosti drugog sudionika.

U svrhu proučavanja vjerojatnosti implementacije pametnih ugovora u građevinsku industriju u Velikoj Britaniji, provedeno je anketno istraživanje na temelju odgovora osoba koje rade u industrijama povezanim sa sektorom građevine: pravnicima, konzultantima, projekt-menadžerima i sl. Iako su prema prvim odgovorima te osobe bile veoma optimistične i uvjerene da se radi o modernoj industriji koja je spremna prihvatiti nove tehnologije, iz ostalih anketnih pitanja proizašao je jasan manjak znanja o pojmu i praksi korištenja pametnih ugovora. Nadalje, anketirane osobe ne vide građevinski sektor kao predvodnika ove tehnologije, već smatraju da se primjena pametnih ugovora treba tek razmatrati kada se oni dokažu u praksi u drugim sektorima.[46] Stoga nije za očekivati da industrije koje nisu utemeljene na digitalizaciji poslovanja, bez obzira na prednosti, budu među prvima pri implementaciji pametnih ugovora.

4.4. DRUŠTVA TEMELJENA NA PAMETNIM UGOVORIMA

Zbog mogućnosti ugrađivanja određenih pravila, povezivanja ugovora te stavljanja novca na raspolaganje, zagovornici pametnih ugovora opisuju načine kako bi se cijela društva mogla temeljiti na pametnim ugovorima koji bi bili 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".[47]

Primjeri začetaka takvih društava već se mogu naći u praksi, primjerice Dash Governance, The DAO i Digix.io. Međutim, pravni status takvih društava upitan je u nizu država, prije svega zbog temeljnog načela *numerus clausus* – a i kogentnih zakonskih propisa koji definiraju društvene oblike u pojedinim državama. Tako su u SAD-u slična društva bila smatrana neregistriranim društvima koja

[45] Ibid., 38.

[46] Jim Mason i Hollie Escott, „Smart contracts in construction: Views and perceptions of stakeholders" (FIG Congress 2018, Istanbul, 6. – 11. 5. 2018.) <http://eprints.uwe.ac.uk/35123/> (pristupljeno 21. 6. 2021.).

[47] Usman W. Chohan, „The Decentralized Autonomous Organization and Governance Issues" (2017.), 1 <https://ssrn.com/abstract=3082055> (pristupljeno 21. 6. 2021.).

ilegalno posluju. Još jedan značajan problem odnosi se na velike poteškoće ispravljanja grešaka. Dosadašnje rješenje bilo bi prebacivanje svih sredstava na novi sustav s ispravljenim kôdom što stvara dodatnu kompleksnost.[48]

Iako društvo utemeljeno na pametnim ugovorima u teoriji svakako može pružati neke prednosti, upitna je isplativost ovakvog sustava kada se uzmu u obzir moguće štete od grešaka u kodu i opasnost od računalnog kriminaliteta.[49] Za očekivati je sve veću aktivnost na ovome području i potrebu za odgovarajućom regulacijom u budućnosti. U tom kontekstu valja spomenuti upravo projekte kao Aragon,[50] MakerDAO,[51] HumanityDAO,[52] MolochDAO[53] i Compound[54] koji predstavljaju samo neke od važnijih primjera tehničkih rješenja namijenjenih decentraliziranim upravljanjem sustavima. Ovi tzv. DeFi[55] sustavi okosnica su daljnjeg razvoja, ali i okosnica buduće regulacije.

---

48 Ibid.

49 Opširnije v. u Alex Norta, „Designing a Smart-Contract Application Layer for Transacting Decentralized Autonomous Organizations", u: Mayank Singh i dr. (ur.), *Advances in Computing and Data Sciences* (Springer, 2017.), 595–604.

50 Aragon je *open-source* softver projekt koji omogućava stvaranje i vođenje decentraliziranih organizacija. Opširnije v. u Andrew Leonard, „Can Aragon Build an Unstoppable Robotic Government?" (*BreakerMag*, 20. 2. 2019.) <http://18.207.229.55/can-aragon-make-decentralized-autonomous-governance-work/> (pristupljeno 21. 6. 2021.).

51 Cilj MakerDAO projekta su transparentne i održive financije. MakerDAO uključuje kredite uz kolateral i upravljanje od strane zajednice. Opširnije v. na MakerDAO <https://makerdao.com/en/> (pristupljeno 21. 6. 2021.).

52 HumanityDAO projekt uspostavlja standard za jedinstvene identitete na Ethereumu. Humanity registar može poslužiti kao temelj različitih radnji kao što su npr. krediti, glasanje itd. V. na HumanityDAO <https://medium.com/marbleorg/introducing-humanity-90ddf9ead235> (pristupljeno 21. 6. 2021.).

53 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. V. Ben Munster, „Inside Moloch: A new DAO aims to fix Ethereum" (*Decrypt*, 15. 2. 2019.) <https://decrypt.co/5206/fixing-ethereum> (pristupljeno 21. 6. 2021.).

54 Compound je otvoreni, autonomni protokol namijenjen programerima kako bi mogli stvarati nove aplikacije za financije. V. Compound <https://compound.finance/> (pristupljeno 21. 6. 2021.).

55 Pojam *decentralized finance* (DeFi) odnosi se na široku paletu projekata koji se zalažu za decentralizaciju financija što npr. uključuje kreditiranje.

4.5. OSTALE MOGUĆNOSTI KORIŠTENJA PAMETNIH UGOVORA

Kao što se iz prethodno iznesenih primjera može vidjeti, postoje raznolika područja aktualne i buduće primjene pametnih ugovora uz prisustvo raznih uređaja, strojeva ili baza podataka. Također se može primijetiti kako koristi koje pametni ugovori mogu pružati nisu ograničene na gospodarske subjekte, već ih mogu iskoristiti i javna tijela i pojedinci.

Neka druga polja u kojima bi se pametni ugovori mogli iskoristiti, primjerice, mogla bi biti: prijavljivanje poreza, prodaja nekretnina i prijepis vlasništva, *online* kockanje, autorsko i intelektualno vlasništvo, vrijednosnice (npr. derivati), trgovinsko poslovanje, stambeni krediti, ugovori o radu i sl.[56]

Koji od danih primjera će (u cijelosti) zaživjeti u praksi, ovisit će o stupnju spremnosti gospodarskih subjekata, država te pojedinačnih korisnika. Pri tome će posebno velik utjecaj imati brzina kojom tehnološka rješenja vezana za pametne ugovore postaju primjenjivija, sigurnija i jednostavnija za korištenje širim masama.

5. OPASNOSTI PRI KORIŠTENJU PAMETNIH UGOVORA

Iako pametni ugovori imaju znatan potencijal u pogledu na brzo i učinkovito izvršenje digitalnih transakcija, ne smiju se zanemariti opasnosti kojima se njihovi korisnici izlažu. Stoga će se u nastavku ukratko obraditi pametni ugovori koji po svome sadržaju nisu dopušteni, napadi na pametne ugovore te pametni ugovori u kojima je računalni kôd manjkav.

5.1. PAMETNI UGOVORI I ILEGALNE AKTIVNOSTI

Prijevare se ne moraju isključivo dogoditi u 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:[57] krađa podataka i prodaja tajnih podataka, krađa privatnih ključeva, plaćanje za

[56] V. više na „Smart Contracts: 10 Use Cases for Business" (*Ambisafe*) <https://ambisafe.com/blog/smart-contracts-10-use-cases-business/> (pristupljeno 21. 6. 2021.); Lester Coleman, „Smart Contracts: 12 Use Cases For Business And Beyond" (*CCN*, 10. 12. 2016.) <www.ccn.com/smart-contracts-12-use-cases-for-business-and-beyond/> (pristupljeno 21. 6. 2021.); Laura Cox, „5 Applications of Smart Contracts" (*Disruption Hub*, 4. 1. 2018.) <https://disruptionhub.com/smart-contract-uses/> (pristupljeno 21. 6. 2021.).

[57] Ari Juels, Ahmed Kosba i Elaine Shi, „The Ring of Gyges: Investigating the Future of Criminal Smart Contracts", u: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications* (Association for Computing Machinery, 2016.), 284.

kriminalna djela koja se fizički izvršavaju u realnom svijetu (plaćanja ilegalnih supstanci, naručivanje ubojstava, podmetanje požara i sl.).

Karakteristike zbog kojih bi se pametni ugovori mogli koristiti u sferi kriminalnih aktivnosti su prvenstveno:[58]

- *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 poglavlja,[59] pametni ugovor može imati mogućnost provjere stanja izvršenja zahtijevanih kriterija zapisanih u ugovoru van svog sustava, što omogućuje provjeru i isplatu naknade za kaznena djela).

Pri bilo kakvoj regulaciji pametnih ugovora, bitno je upozoriti na postojanje interesa kriminalnih skupina i pojedinaca u korištenju pametnih ugovora za ilegalne aktivnosti. Upravo u ovom se kontekstu kriptovalute pokazuju problematične za državna tijela jer korištenje pseudonima bitno otežava praćenje transakcija, a time otvara vrata sustavima pranja novca. Jedno moguće rješenje moglo bi biti označavanje jedinica određene kriptovalute za koju se zna da je povezana s kriminalnim radnjama,[60] kako bi ih druge osobe aktivno mogle izbjegavati. Također, predlaže se mogućnost poništavanja takvih ugovora i njihovog brisanja s *blockchaina* odukom većine glasova pri čemu bi sudionici ostali anonimni ili odlukom određene autoritarne strane.[61]

5.2. NAPADI NA PAMETNE UGOVORE

Iako su *blockchain* sustavi zbog već opisanog sustava naočigled sigurni, postoji niz karakteristika sustava koje bi se mogle 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. Neki od primjera

58 Ibid., 286.

59 V. opširnije u odjeljku 2.

60 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.

61 Opširnije v. u Juels, Kosba i Shi (bilj. 57).

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.[62]

5.3. MANJKAV KÔD PAMETNIH UGOVORA

Jedan od problema koji zahvaća osobe koje nisu programerskog obrazovanja ili nemaju dovoljno iskustva na tom polju su manjkavosti koje nastaju pri samom pisanju računalnog kôda pametnih ugovora. Kada se pri programiranju pametnog ugovora zbog nepažnje programera (ljudski faktor) dogodi da određeni dio kôda ne čini upravo ono čemu je namijenjen, ne radi se o prijevari jer ne dolazi do svjesne manipulacije kôdom.

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.[63] Nadalje, situacije s petljama koje čine pametan ugovor nepotrebno skupljim ponovno se mogu podijeliti na sljedeće:[64]

- skupe operacije stavljene su 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 prostora za nastanak poteškoća 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.

---

[62] Opširnije v. u Nicola Atzei, Massimo Batoletti i Tiziana Cimoli, „A Survey of Attacks on Ethereum Smart Contracts (SoK)“, u: Matteo Maffei i Mark Ryan (ur.), *Principles of Security and Trust* (Springer, 2017.), 164–186.

[63] 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.

[64] Opširnije v. u Ting Chen i dr., „Under-Optimized Smart Contracts Devour Your Money“, u: Martin Pinzger, Gabriele Bavota i Andrian Marcus (ur.), *SANER 2017: 24th IEEE International Conference on Software Analysis, Evolution and Reengineering* (IEEE, 2017.), 442–446.

6. PAMETNI UGOVORI PREMA VRSTAMA *BLOCKCHAIN* SUSTAVA

Nakon što smo utvrdili što su to pametni ugovori, kako su nastali, kako funkcioniraju, gdje se sve koriste ili bi se mogli koristiti, te koje su opasnosti pri njihovoj primjeni, smatramo bitnim istaknuti i podjelu *blockchain* sustava koja je nastala u znanstvenoj literaturi. Naime, već na samom početku poglavlja istaknuli smo kako se pametni ugovori temelje na *blockchain* sustavima[65] te smatramo da se podjela *blockchain* sustava može primijeniti i na podjelu pametnih ugovora koja bi nam pomogla za opredjeljenje prema smjeru u kojem bi trebalo ići s reguliranjem pametnih ugovora.

Tako se u literaturi ističe da se *blockchain* sustavi mogu podijeliti na:

- potpuno javne sustave (javni *blockchain*/DLT)
- potpuno privatne sustave (privatni *blockchain*/DLT)
- hibridne ili konzorcijske sustave (hibridni *blockchain*/DLT).[66]

Temeljem potpuno javnog sustava funkcioniraju najpoznatije kriptovalute na svijetu, glavne karakteristike tog sustava možemo izvući iz primjera *bitcoina* i *ethera* koje smo ranije u ovom poglavlju objašnjavali.[67] Tako je za potpuno javne sustave karakteristično da su decentralizirani (nema odgovorne osobe), svima dostupni, da bilo tko može sudjelovati u njihovom radu putem rudarenja te da se kao nagradu za rudarenje dobiva naknada u obliku određene kriptovalute. Iz toga proizlazi kako je korištenje pametnih ugovora putem potpuno javnih sustava povezano i uz određenu kriptovalutu ili tokene[68] koji se koriste na tom potpuno javnom sustavu te da ne postoji središnje tijelo koje bi bilo odgovorno za funkcioniranje tog sustava.

---

65 V. odjeljak 2.

66 V. Mislav Mostarac, „Primjena 'blockchain' tehnologije u međunarodnim plaćanjima – poslovanje rambursnih banaka" (diplomski rad, Ekonomski fakultet Sveučilišta u Splitu, 2019.), 18; Vitalik Buterin, „On Public and Private Blockchains" (*Ethereum Blog*, 7. 8. 2015.) <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> (pristupljeno 21. 6. 2021.).

67 V. odjeljke 2.2. i 2.3.

68 Token u kontekstu pametnih ugovora „podrazumijeva svojevrsnu obveznicu u elektroničkom obliku pohranjenu unutar sustava *blockchaina*. Naime, token (u tom smislu) predstavlja ne samo računsku jedinicu, već i svojevrstan investicijski odnosno obvezнички certifikat". Perkušić (bilj. 3), 401.

Potpuno privatni sustavi koriste privatni *blockchain* koji kontrolira središnje tijelo. Stoga se takav sustav ne mora povezivati uz određenu kriptovalutu ili tokene, jer nije potreban takav tip rudarenja koji bi osiguravao decentraliziranost sustava, pa stoga središnje tijelo samo određuje tko će i na koji način spremati podatke na *blockchain*. Koncept pametnih ugovora temeljenih na potpuno privatnim sustavima koristit će se najčešće u slučajevima kao što su primjena uređaja koji onemogućuju pokretanje vozila,[69] pri području osiguranja[70] te u građevinskoj industriji.[71] Stoga kao ključne razlike između potpuno javnog sustava i potpuno privatnog sustava treba istaknuti činjenice da potpuno privatni sustav ne mora biti povezan uz određenu kriptovalutu ili tokene te kod njega postoji središnje odgovorno tijelo koje je odgovorno za funkcioniranje tog sustava. Navedene ključne razlike posebno su bitne s pravnog aspekta jer iz njih proizlazi kako u praksi mogu postojati pametni ugovori koji se:

- temelje na zakonskom sredstvu plaćanja te postoji odgovorna osoba za njihovo funkcioniranje
- temelje na alternativnim načinima plaćanja (kriptovalute, tokeni) te ne postoji odgovorna osoba za njihovo funkcioniranje
- temelje na kombinaciji prve dvije mogućnosti jer trenutno ništa ne sprječava da središnje tijelo u potpuno privatnom sustavu poveže funkcioniranje pametnih ugovora s npr. određenom kriptovalutom.

Kod hibridnih sustava „proces validacije konsenzusa mreže kontrolira se od strane unaprijed odabranih pojedinaca ili organizacija, kao što je konzorcij fin. institucija ili klijenata tvrtke".[72] Pritom se može raditi o različitim stupnjevima decentraliziranosti, odnosno centraliziranosti sustava, ali bez obzira na razinu tog stupnja, kod hibridnih sustava uvijek će postojati središnje tijelo koje to kontrolira. S pravnog aspekta to je ključna karakteristika zbog koje ćemo hibridne sustave analizirati skupa s potpuno privatnim sustavima.

7. PRAVNO UREĐENJE PAMETNIH UGOVORA U REPUBLICI HRVATSKOJ

Pametni ugovori nisu regulirani propisima Europske unije, kao ni propisima Republike Hrvatske. Kao jedan od rijetkih primjera možemo istaknuti *Senate Bill*

69 V. odjeljak 4.1.

70 V. odjeljak 4.2.

71 V. odjeljak 4.3.

72 Mostarac (bilj. 66).

398 iz 2017. godine[73] kojim je uvedeno uređenje pametnih ugovora u zakonodavstvo savezne države Nevade.[74] Njime se u Nevadi prvenstveno uređuje *blockchain* tehnologija koja se određuje kao elektronički zapisnik podataka čije korištenje je neoporezivo i pritom nije potreban određeni certifikat ili ispunjenje nekih drugih uvjeta kako bi se *blockchain* tehnologija mogla koristiti.[75] Za pametne ugovore se ističe kako i oni predstavljaju elektronički zapis koji se nalazi na *blockchainu*, te da 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. Iako je savezna država Nevada odredila što smatra *blockchain* tehnologijom i pametnim ugovorima te je odobrila njihovo korištenje, predmetno zakonsko rješenje se tek može smatrati začećem pravnog uređenja pametnih ugovora. Naime, trenutnim rješenjem tek je konkretno legalizirano korištenje *blockchain* tehnologije i pametnih ugovora kao sredstava provedbe ugovora. Međutim, zakonom nisu ni približno regulirane sve vrste i načini korištenja pametnih ugovora te sadašnje rješenje nije dovoljno da bi se zaštitilo korisnike u redovitoj primjeni pametnih ugovora.

Budući da pametni ugovori nisu uređeni u Republici Hrvatskoj, smatramo kako je potrebno utvrditi može li se određeno, već postojeće zakonsko uređenje primijeniti i na pametne ugovore. Osim toga, smatramo kako je potrebno utvrditi mogućnosti pravnog uređenja pametnih ugovora prema vrsti sustava[76] pomoću koje se ti određeni pametni ugovori koriste.

7.1. MOGUĆNOST PRIMJENE POSTOJEĆEG ZAKONSKOG UREĐENJA NA PAMETNE UGOVORE

Analizirajući pojam pametnih ugovora[77] i postojeće zakonsko uređenje u Republici Hrvatskoj, može se utvrditi da pametni ugovori predstavljaju novu kategoriju koja se ne može u cijelosti poistovjetiti s postojećim institutima. Neke se sličnosti na prvi pogled mogu uočiti između njih i ugovora u elektroničkom obliku. Naime, ugovori u elektroničkom obliku su ugovori što ih pravne i fizičke osobe u cijelosti ili djelomično sklapaju, šalju, primaju, raskidaju, otkazuju,

---

73 Njime je uređenje pametnih ugovora uvedeno u NRS § 719.045 i d.

74 Perkušić (bilj. 3), 392.

75 V. opširnije u Gayle M. Hyman i Matthew P. Digesti, „New Nevada Legislation Recognizes Blockchain and Smart Contract Technologies" (2017.) 25 (8) *Nevada Lawyer* 13, 13–14.

76 V. odjeljak 6.

77 V. odjeljak 3.

pristupaju i prikazuju elektroničkim putem koristeći elektronička, optička ili slična sredstva, uključujući, ali ne ograničavajući se na prijenos internetom.[78] Uspoređujući predmetne karakteristike s pojmom pametnog ugovora, mogu se kao zajedničke crte uočiti: a) da se ne radi o posebnoj vrsti ugovora; b) da barem djelomično moraju postojati u elektroničkom obliku.

Međutim, iako su im navedene karakteristike donekle zajedničke, detaljnim razmatranjem može se uočiti da se ove dvije kategorije ne preklapaju, ali se pod određenim uvjetima mogu nadopunjavati. Naime, ugovori u elektroničkom obliku su prvenstveno ugovori, dok su pametni ugovori prvenstveno način provedbe ugovora koji se izvršava s unaprijed definiranim kriterijima i uvjetima na koje dvije ili više strana pristaju. Stoga se može i zaključiti da su sličnosti ovih dvaju kategorija prije svega prividne. Naime, ugovori u elektroničkom obliku nisu posebna vrsta ugovora već oblik (digitalni) koji poprima određeni ugovor određene vrste. S druge strane, pametni ugovor redovito nije vezan za sami oblik ugovora, već za način provedbe ugovora. U tom pogledu se i druga prividno zajednička karakteristika, elektronički oblik, može objasniti. Naime, kod ugovora u elektroničkom obliku, digitalna struktura vezana je za način prikazivanja sadržaja ugovora, dok je digitalni oblik kod pametnih ugovora vezan za provedbu ugovora.

Stoga dolazimo do zaključka da se zakonske odredbe koje uređuju ugovore u elektroničkom obliku ne mogu primjenjivati na pametne ugovore. Međutim, kako medij sklapanja i medij provedbe ugovora predstavljaju dva komplementarna obveznopravna elementa, izgledno je da će pametni ugovori u budućnosti redovito služiti kao sredstvo provedbe ugovora u elektroničkom obliku. Stoga će se u takvim slučajevima na pametne ugovore moći primijeniti one odredbe o ugovorima u elektroničkom obliku koje se vežu za njihovu provedbu.

Stoga u konačnici pravna pitanja vezana za samu bit pametnog ugovora (njegova provedba pomoću računalnog kôda koji se nalazi na *blockchain* mreži) nisu obuhvaćena ni predviđena zakonskim odredbama koje uređuju ugovore u elektroničkom obliku. Štoviše, uređenje pametnih ugovora predstavljat će značajan izazov za zakonodavca. Budući da su pametni ugovori zbog potrebe za kodiranjem i korištenjem *blockchain* mreže znatno složeniji i opsežniji od klasičnih sustava digitalnih transakcija, njihovo uređenje iziskivat će značajne napore koji se ne mogu ni usporediti s pitanjima uređenja ugovora u elektroničkom obliku.

[78] Čl. 2. st. 6. Zakona o elektroničkoj trgovini, NN 173/2003., 67/2008., 36/2009., 130/2011., 30/2014. i 32/2019.

7.2. PRAVNO UREĐENJE PAMETNIH UGOVORA PREMA VRSTI SUSTAVA

Kao što je izloženo, pametni ugovori predstavljaju zajednički naziv za niz sustava provedbe ugovora. Kako bi se moglo predložiti učinkovito uređenje ovog izrazito širokog spektra, nužno je grupirati pametne ugovore prema njihovim meritornim značajkama. Upravo u podjeli pametnih ugovora prema sustavima unutar kojih djeluju, možemo naći takvu podjelu. Naime, izrazito su velike razlike između potpuno javnog te potpuno privatnog i hibridnog sustava[79] te smatramo kako ih je s pravnog aspekta potrebno odvojeno analizirati i tako utvrditi smjer njihove buduće regulacije.

7.2.1. Pravno uređenje pametnih ugovora temeljenih na javnim sustavima

Prilikom analiziranja pametnih ugovora temeljenih na potpuno javnim sustavima ustanovili smo kako je korištenje pametnih ugovora putem potpuno javnih sustava povezano i uz određenu kriptovalutu ili tokene koji se koriste na tom sustavu te da ne postoji središnje tijelo koje bi bilo odgovorno za funkcioniranje tog sustava. Stoga se kod takvih pametnih ugovora otvara problem sredstva plaćanja i odgovornosti za njihovo funkcioniranje.

Naime, takvi pametni ugovori povezani su uz kriptovalute koje su podskupina virtualnih valuta,[80] a koje se u Republici Hrvatskoj definiraju kao digitalni prikaz vrijednosti koji nije izdala i za koji ne jamči središnja banka ni javno tijelo, koji nije nužno povezan sa zakonski uspostavljenom valutom te nema pravni status valute ili novca, ali ga fizičke ili pravne osobe prihvaćaju kao sredstvo razmjene i može se prenositi, pohranjivati te se njime može trgovati elektroničkim putem.[81] Virtualne valute (pa tako ni kriptovalute) nisu dalje regulirane propisima u Republici Hrvatskoj, pa iz toga proizlazi kako su pametni ugovori (temeljeni na potpuno javnom sustavu) povezani uz sredstvo plaćanja za koje ne jamči ni jedno javno tijelo i koja su znatno nepredvidljivija opcija za pohranu vrijednosti zbog velike volatilnosti tečaja koja je znatno veća nego kod drugih valuta ili zlata.[82]

Kao drugi problem naveli smo problem odgovornosti za funkcioniranje sustava. Naime, budući da se radi o decentraliziranom tijelu iza kojeg ne stoji nijedna osoba, u slučaju greške na sustavu nitko ne odgovara korisnicima za štetu koja je

---

79 V. odjeljak 6.

80 Opširnije o tome v. Perkušić (bilj. 3), 371.

81 Čl. 4. st. 49. ZSPNFT-a.

82 David Yermack, „Is Bitcoin a Real Currency? An economic appraisal" (2013.) *NBER Working Paper* 19747, 14 <www.nber.org/papers/w19747> (pristupljeno 21. 6. 2021.).

nastala zbog izostanka provedbe ili krive provedbe pametnog ugovora koji se nalazio na tom sustavu. Budući da nema odgovorne osobe, javlja se i problem kontrole sadržaja koji bi ti pametni ugovori imali jer je prednost korištenja takve vrste pametnih ugovora anonimnost ugovornih strana te nedostatak potrebe za skladištenjem i provjerom informacija koje se u njima nalaze. Međutim, kako bi se spriječile prijevare i nedopuštene radnje, zakonodavac je skloniji traženju nadzora podataka koji ulaze u sustav (kao što je slučaj s bankama i informacijskim društvima), pa je i to jedan od problema koji prati pametne ugovore u javnim sustavima.

Iz navedenog proizlazi kako nema smisla krenuti s reguliranjem pametnih ugovora koji se koriste na potpuno javnim sustavima prije nego što se reguliraju kriptovalute i javni *blockchain* sustavi koji se koriste za te kriptovalute i pametne ugovore. Do tada smatramo kako za takvu vrstu pametnih ugovora može vrijediti isto upozorenje koje je Hrvatska narodna banka izdala za kriptovalute.[83]

7.2.2. Pravno uređenje pametnih ugovora temeljenih na privatnim i hibridnim sustavima

Za razliku od pametnih ugovora temeljenih na potpuno javnim sustavima, pametni ugovori temeljeni na privatnim i hibridnim sustavima ne moraju biti povezani s određenom kriptovalutom ili tokenima te kod njih postoji središnje tijelo, tj. odgovorna osoba za taj sustav na kojem se nalazi pametni ugovor. Budući da kod pametnih ugovora temeljenih na potpuno javnim sustavima nema problema (sredstvo plaćanja, decentraliziranost) koji sprječavaju reguliranje pametnih ugovora temeljenih na javnim sustavima, smatramo da je to smjer u kojem treba ići s reguliranjem pametnih ugovora. Pogotovo stoga što je trenutno glavni problem takve vrste pametnih ugovora nedostatak povjerenja u osobu koja kontrolira sustav, kao i u osobu koja sastavlja (kodira) takvu vrstu pametnog ugovora. Zakonodavac stoga mora odrediti tko može pokrenuti takvu vrstu privatnog ili hibridnog sustava za pametne ugovore, tko smije nuditi usluge kodiranja pametnih ugovora, što u slučaju greške na kodu pametnog ugovora ili sustavu na kojem je taj pametni ugovor te tko će vršiti kontrolu nad osobama koja nude usluge sustava i kodiranja pametnih ugovora.

[83] Opširnije o tome v. „Što su virtualne valute?“ (*Hrvatska narodna banka*, 9. 2. 2018.) <www.hnb.hr/-/sto-su-virtualne-valute-> (pristupljeno 21. 6. 2021.).

8. ZAKLJUČAK

Iz gornjih navoda vidljivo je da koncept pametnog ugovora nije samo složen u pogledu na njegove tehnološke značajke, već i u pogledu na njegove pravne značajke. Iako su danas digitalne transakcije postale redovita pojava, pametni ugovori redovito u bitnome odstupaju od onoga što podrazumijevamo pod ugovorom u elektroničkom obliku. Primarna svrha pametnih ugovora nije u tome da se njima definira volja ugovornih strana, već da se njima provede volja ugovornih strana. Stoga oni uglavnom neće predstavljati ugovor u pravnome smislu, a u skladu s time se i odredbe o ugovorima o elektroničkom obliku neće primijeniti na njih, unatoč tome što oni uistinu postoje u elektroničkom obliku. Međutim, u ovim slučajevima pametni ugovori i ugovori u elektroničkom obliku mogu predstavljati dva komplementarna elementa obveznopravnog odnosa (sadržaj i ispunjenje) kada su pametni ugovori, čija je svrha ispunjenje ugovorne volje strana, vezani za ugovor u elektroničkom obliku koji sadrži upravo tu volju ugovornih strana. U ovim slučajevima dolazi u obzir primjena zakonskih odredbi vezanih za ugovore u elektroničkom obliku koje se tiču ispunjenja na pametne ugovore. Od navedenoga postoji jedna bitna iznimka. Naime, u slučajevima kada ugovorne strane posredstvom tzv. jakog pametnog ugovora vezanog za pseudonimni, decentralizirani *blockchain* sustav stupaju u ugovorni odnos, zbog posebnih okolnosti slučaja, može se poći od toga da je volja ugovornih strana da sadržaj koda pametnog ugovora predstavlja ujedno i sadržaj njihovog ugovora. Tada takav pametni ugovor ujedno postaje ugovor u pravnome smislu te riječi, a s obzirom na svoj elektronički oblik, predstavlja i ugovor u elektroničkom obliku. Temeljem svega navedenog, dolazimo do zaključka da nije moguće jednako regulirati centralizirane (privatne) i hibridne sustave s jedne strane i decentralizirane sustave s druge strane. Stoga završno predlažemo da se prije bilo koje vrste regulacije pametnih ugovora temeljenih na javnim sustavima prvo reguliraju kriptovalute i *blockchain*. Nasuprot tome, nema pravne prepreke regulaciji privatnih i hibridnih sustava. Štoviše, u pogledu na ove sustave, ključno je regulirati što prije pravo njihova osnivanja i upravljanja, kako bi se moglo zaštititi korisnike sustava u odnosu na osobe koje kontroliraju takve sustave. Završno valja naglasiti da će značaj pametnih ugovora nesporno rasti s razvojem tehnologije. Stoga je zadatak zakonodavca pratiti ove razvojne procese odgovarajućom regulacijom, kako u interesu zaštite potrošača i gospodarskih subjekata, tako i u svrhu stvaranja povjerenja i sigurnosti u pravnome prometu.

BIBLIOGRAFIJA

— „Smart Contracts: 10 Use Cases for Business“ (*Ambisafe*) <https://ambisafe.com/blog/smart-contracts-10-use-cases-business/> (pristupljeno 21. 6. 2021.)

— „Što su virtualne valute?“ (*Hrvatska narodna banka*, 9. 2. 2018.) <www.hnb.hr/-/sto-su-virtualne-valute-> (pristupljeno 21. 6. 2021.)

ATZEI N., BATOLETTI M. i CIMOLI T., „A Survey of Attacks on Ethereum Smart Contracts (SoK)“, u: MAFFEI M. i RYAN M. (ur.), *Principles of Security and Trust* (Springer, 2017.)

BIRYUKOV A., KHOVRATOVICH D. i TIKHOMIROV S., „Privacy-preserving KYC on Ethereum“ (2018.) 2 (12) *Reports of the European Society for Socially Embedded Technologies* <https://dl.eusset.eu/handle/20.500.12015/3165> (pristupljeno 21. 6. 2021.)

BLOCHER W., „The next big thing: Blockchain – Bitcoin – Smart Contracts“ (2016.) 66 *Anwaltsblatt* 612

BUTERIN V., „Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform“ (*Ethereum White Paper*, 2014.) <https://ethereum.org/en/whitepaper/> (pristupljeno 21. 6. 2021.)

BUTERIN V., „On Public and Private Blockchains“ (*Ethereum Blog*, 7. 8. 2015.) <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> (pristupljeno 21. 6. 2021.)

CARDEIRA H., „Smart contracts and possible applications to the construction industry“ (2015.) 1 (1) *Romanian Construction Law Review* 35

CHEN T. i dr., „Under-Optimized Smart Contracts Devour Your Money“, u: PINZGER M., BAVOTA G. i MARCUS A. (ur.), *SANER 2017: 24th IEEE International Conference on Software Analysis, Evolution and Reengineering* (IEEE, 2017.)

CHOHAN U. W., „The Decentralized Autonomous Organization and Governance Issues“ (2017.) <https://ssrn.com/abstract=3082055> (pristupljeno 21. 6. 2021.)

COLBERT Y., „Privacy group wants better regulation for GPS starter interrupt devices“ (*CBC News*, 13. 8. 2018.) <www.cbc.ca/news/canada/nova-scotia/gps-starter-interrupters-privacy-technology-laws-1.4780860> (pristupljeno 21. 6. 2021.)

COLEMAN L., „Smart Contracts: 12 Use Cases For Business And Beyond“ (*CCN*, 10. 12. 2016.) <www.ccn.com/smart-contracts-12-use-cases-for-business-and-beyond/> (pristupljeno 21. 6. 2021.)

CORKERY M. i SILVER-GREENBERG J., „Miss a Payment? Good Luck Moving That Car“ (*The New York Times*, 24. 9. 2014.) <https://archive.nytimes.com/dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/> (pristupljeno 21. 6. 2021.)

COX L., „5 Applications of Smart Contracts“ (*Disruption Hub*, 4. 1. 2018.) <https://disruptionhub.com/smart-contract-uses/> (pristupljeno 21. 6. 2021.)

GATTESCHI V. i dr., „Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?“ (2018.) 10 (2) *Future Internet* 1

HYMAN G. M. i DIGESTI M. P., „New Nevada Legislation Recognizes Blockchain and Smart Contract Technologies“ (2017.) 25 (8) *Nevada Lawyer* 13

JOHNSON E. L. i KIRKENDALL C., „Starter Interrupt and GPS Devices: Best Practices“ (*PassTime Blog*, 14. 1. 2016.) <https://passtimegps.com/blog/starter-interrupt-and-gps-devices-best-practices/> (pristupljeno 21. 6. 2021.)

JUELS A., KOSBA A. i SHI E., „The Ring of Gyges: Investigating the Future of Criminal Smart Contracts“, u: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications* (Association for Computing Machinery, 2016.)

LAWSON B., „What is Gas: An overview of Gas and how it is used on the blockchain" (*MyEtherWallet*) <https://help.myetherwallet.com/en/articles/5878945-what-is-gas> (pristupljeno 21. 6. 2021.)
LEONARD A., „Can Aragon Build an Unstoppable Robotic Government?" (*BreakerMag*, 20. 2. 2019.) <http://18.207.229.55/can-aragon-make-decentralized-autonomous-governance-work/> (pristupljeno 21. 6. 2021.)
MAMUT J., „Mogućnosti i opasnosti korištenja pametnih ugovora" (diplomski rad, Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti, 2019.)
MASON J. i ESCOTT H., „Smart contracts in construction: Views and perceptions of stakeholders" (FIG Congress 2018, Istanbul, 6. – 11. 5. 2018.) <http://eprints.uwe.ac.uk/35123/> (pristupljeno 21. 6. 2021.)
MOSTARAC M., „Primjena 'blockchain' tehnologije u međunarodnim plaćanjima – poslovanje rambursnih banaka" (diplomski rad, Ekonomski fakultet Sveučilišta u Splitu, 2019.)
MÖHLENKAMP M. i WESSEL T., „Smart Contracts in der Versicherung – Chancen und rechtliche Herausforderungen" (*Wilhelm Rechtsanwälte*, 7. 5. 2018.) <www.wilhelm-rae.de/de/aktuelles/smart-contracts-in-der-versicherung-chancen-und-rechtliche-herausforderungen> (pristupljeno 21. 6. 2021.)
MUNSTER B., „Inside Moloch: A new DAO aims to fix Ethereum" (*Decrypt*, 15. 2. 2019.) <https://decrypt.co/5206/fixing-ethereum> (pristupljeno 21. 6. 2021.)
NAKAMOTO S., „Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin Project: White Paper*, 31. 10. 2008.) <https://bitcoin.org/bitcoin.pdf> (pristupljeno 21. 6. 2021.)
NORTA A., „Designing a Smart-Contract Application Layer for Transacting Decentralized Autonomous Organizations", u: SINGH M. i dr. (ur.), *Advances in Computing and Data Sciences* (Springer, 2017.)
ORIWOH E. i CONRAD M., „'Things' in the Internet of Things: Towards a Definition" (2015.) 4 (1) *International Journal of Internet of Things* 1
PERKUŠIĆ M., „Pravna pitanja elektroničkog plaćanja" (doktorska disertacija, Pravni fakultet Sveučilišta u Rijeci, 2019.)
RASKIN M., „The Law and Legality of Smart Contracts" (2017.) 1 *Georgetown Law Technology Review* 305
WERBACH K. i CORNELL N., „Contracts *ex machina*" (2017.) 67 *Duke Law Journal* 313
WRIGHT A. i DE FILIPPI P., „Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (2015.) <https://ssrn.com/abstract=2580664> (pristupljeno 21. 6. 2021.)
YERMACK D., „Is Bitcoin a Real Currency? An economic appraisal" (2013.) *NBER Working Paper* 19747 <www.nber.org/papers/w19747> (pristupljeno 21. 6. 2021.)

POSSIBILITIES OF USE AND REGULATION OF THE SO-CALLED SMART CONTRACTS IN THE REPUBLIC OF CROATIA

SUMMARY

This chapter defines the term and structure of 'smart contract'. In this context, blockchain technology is explained, as it is essential for a future expansion of smart contract solutions, especially in sectors like insurance, construction, and lending, to name a few. Key characteristics and the legal categorisation of smart contracts are especially meticulously elaborated due to their relevance for future regulation. Furthermore, this chapter

investigates the dangers concerning smart contracts, like cyber-crime or programming flaws and critically analyses the existing legal framework in Croatia in order to give concrete suggestions regarding the implementation of effective regulatory mechanisms. Here the authors conclude that smart contracts must be regulated in a manner that takes into account their purpose and form. It is essential to consider whether a smart contract is based on an entirely public system or whether it is based on a private or hybrid system. Furthermore, a key factor is the categorisation of a smart contract from the legal standpoint, as smart contracts in most cases will be means of execution of a contract, but in some cases, they will represent the content of the contract itself and thus must be regulated accordingly.

KEYWORDS: smart contract, blockchain, Ethereum, contract in electronic form, oracle, contractware.