Tehnološki i pravni izazovi pametnih ugovora

Balentović, Vladimir

SVEUČILIŠTE U ZAGREB

FAKULTET PROMETNIH ZNANOSTI

Vladimir Balentović

TEHNOLOŠKI I PRAVNI IZAZOVI PAMETNIH UGOVORA

DIPLOMSKI RAD

ZAGREB, 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 6. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Telekomunikacijska legislativa i standardizacija**

DIPLOMSKI ZADATAK br. 6927

Pristupnik: **Vladimir Balentović (0135232545)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Tehnološki i pravni izazovi pametnih ugovora**

Opis zadatka:

Pametni ugovori su jedna od nadogradnji na koncept blockchaina, u kojoj se kao vrsta podataka, u blockchain upisuje programski kod, a blockchain omogućuje da su podaci u njemu nepromjenjivi. Ako se dvije strane sporazume da će pametni ugovor, nije im potrebna treća strana koja će odobriti, zapisati, ili nadgledati taj ugovor. U radu treba navesti, objasniti i razraditi tehnološke i pravne aspekte pametne ugovore, posebno uključujući mogućnosti Ethereum platforme.

Mentor:

izv. prof. dr. sc. Goran Vojković

Predsjednik povjerenstva za diplomski ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

Tehnološki i pravni izazovi pametnih ugovora

Technological and legal challenges of smart contracts

Mentor: izv.prof. dr. sc. Goran Vojković

Student: Vladimir Balentović

JMBAG: 0135232545

Zagreb, mjesec 2022.

SAŽETAK

Svrha je istraživanja u ovom diplomskom radu utvrditi što je potrebno za pravno i tehnološko unapređenje i usklađivanje pametnih ugovora kako bi pametni ugovori imali širu primjenu i pravnu prihvaćenost te bili ravnopravni s tradicionalnim ugovorima u pisanom obliku. Cilj je istraživanja dokazati spremnost tehnologije koja omogućava pametne ugovore te objasniti zašto pametni ugovori nisu do sad pravno regulirani i prihvaćeni. Analizom i usporedbom definicija za blockchain tehnologiju i pametne ugovore ponuđena je vlastita definicija za blockchain tehnologiju i pametne ugovore. Usporedili su se tradicionalni i pametni ugovori kako bi se istaknule prednosti i nedostaci pametnih ugovora te su se ponudila rješenja za nedostatke pametnih ugovora. Prijedlozi za tehnološko unapređenje pametnih ugovora su ponuđeni za Ethereum blockchain jer je to prva platforma za pametne ugovore koja je najveća i najpopularnija. Ponuđena su rješenja za prepreke koje su detektirali regulatori pojedinih država i organizacije. Pravna unapređenja pametnih ugovora su predložena na temelju analizi stava sudionika u pravnom sustavu.

KLJUČNE RIJEČI: blockchain; pametni ugovori; Ethereum; analiza; tehnološki i pravni izazovi

SUMMARY

The purpose of the research in this thesis is to determine what is needed for the legal and technological improvement and harmonization of smart contracts so that smart contracts have wider application and legal acceptance and are equal to traditional contracts in written form. The aim of the research is to prove the readiness of the technology that enables smart contracts and to explain why smart contracts have not yet been legally regulated and accepted. By analyzing and comparing the definitions for blockchain technology and smart contracts, we offer our own definition for blockchain technology and smart contracts. Traditional and smart contracts were compared to highlight the advantages and disadvantages of smart contracts, and solutions were offered for the disadvantages of smart contracts. Proposals for the technological advancement of smart contracts are offered for the Ethereum blockchain because it is the first smart contract platform that is the largest and most popular. Solutions are offered for obstacles detected by the regulators of individual countries and organizations. Legal improvements of smart contracts are proposed based on the analysis of the attitude of the participants in the legal system.

KEY WORDS: blockchain; smart contracts; Ethereum; analysis; technological and legal challenges

SADRŽAJ

1. UVOD

S napretkom tehnologije dolaze nova rješenja, ali isto tako je i prilika da teorije postanu stvarnost. Ideju o pametnim ugovorima formirao je Nick Szabo s ciljem povećanja ispunjenja ugovornih obveza i smanjenja ekonomskih rizika. Pametni ugovori nisu bili aktualni sve do pojave blockchain tehnologije i Ethereuma. Bitcoin je prva kriptovaluta koja je koristila blockchain tehnologiju dok je Ethereum platforma koja omogućava korištenje pametnih ugovora na blockchainu. Pametni ugovori najviše su se počeli koristiti u decentraliziranim financijama. Zagovornici pametnih ugovora ističu da će se njihovom korištenjem smanjiti potreba za skupim odvjetnicima i da neće biti potrebe za posrednicima dok tradicionalni sudionici smatraju da nije moguće sklapati ugovore u sadašnjem obliku te da tehnologija treba savladati vlastite tehničke nedostatke prije nego se mogu primjenjivati.

Kako bi se ispitala korisnost novih tehnologija, nužna je analiza relevantnih sudionika koji su je doveli do sadašnjeg oblika. Također je bitno ispitati stav sudionika koji moraju dati odobrenje o prihvatljivosti nove tehnologije. Bez njihovog odobrenja i stavljanje unutar regulatornih okvira nova tehnologija ne može steći širu primjenu i ostat će se koristi u ograničenom obliku unutar zajednice entuzijasta. Ovim se diplomskim radom želi utvrditi s kojim se to izazovima suočava nova tehnologija na svom putu do šire primjene te se nude rješenja kako bi bila spremna za masovno korištenje. Naslov rada je „Tehnološki i pravni izazovi pametnih ugovora”. U izradi rada korištena je opsežna novija literatura i radovi. Rad je strukturiran u 9 cjelina:

1. Uvod
2. Blockchain tehnologija
3. Prednosti i nedostaci blockchain tehnologije
4. Kriptovalute - Bitcoin i Ethereum
5. Pametni ugovori na Ethereum platformi
6. Vrste pametnih ugovora
7. Prihvaćanje pametnih ugovora u praksi
8. Unapređenje pravnog i tehnološkog okvira pametnih ugovora
9. Zaključak

U drugom poglavlju je opisana koncept blockchain tehologije, njezini elementi, struktura, vrste, nužni algoritmi za rad i partneri bez kojih ne bi mogla funkcionirati.

U trećem poglavlju prikazat će se prednosti i nedostaci koje dolaze s blockchain tehnologija.

Četvrto poglavlje čine kriptovalute Bitcoin i Ethereum koje su zaslužne za predstavljanje mogućnosti blockchain tehnologije i za njezinu popularizaciju.

Peto poglavlje predstavlja nužne korake koji se moraju proći i naučiti kako bi se mogli koristi pametnim ugovorima.

U šestom poglavlju navedene su podjele pametnih ugovora.

U sedmom poglavlju istraženo je koje bi djelatnosti mogle koristiti pametne ugovore te koju bi korist imale od njihove primjene.

U osmom poglavlju predložena je nova definicija za pametne ugovore i blockchain tehnologiju. Usporedbom pametnih i tradicionalnih ugovora prikazala su se prednosti i nedostaci pametnih ugovora. Prikazane su tehnički i pravni izazovi pametnih ugovora te su ponuđena rješenja.

2.BLOCKCHAIN TEHNOLOGIJA

2.1. DEFINICIJA BLOCKCHAINA

Blockchain je distribuirani sustav ravnopravnih računala koji je kriptografski osiguran, samo dodajući, nepromjenjiv i jedino ažuriran putem konsenzusa ili dogovorom između računala [1].

Za lakše razumijevanje tehničkog aspekta blockchiana poslužit će se primjerima kako bi se objasnio ovaj koncept. Kada pojedinac stavi depozit u bankarsku instituciju, on vjeruje da će se ta suma tu zadržati dok god se ne odluči razmijeniti je za neko dobro ili uslugu. Pojedinac vjeruje banci da će imati točan zapis o transakciji kao što je iznos, klijent, datum i vrijeme depozita. Društvo se oslanja na središnje repozitorije kao što su banke ili javne institucije kako bi održavala, prikupljala i štitila upisane radnje od neželjenih akcija pojedinaca ili institucija [2].

Blockchain se razlikuje od centraliziranih repozitorija na način da decentralizira izvor povjerenja. Pojedinac deponira sredstva u digitalni novčanik i vrijednost se bilježi na blockchain. Ako pojedinac kupi pjesmu u digitalnom obliku, transakcija se bilježi na blockchainu zajedno s promjenom iznosa sredstava u digitalnom računu. Banka nije potrebna kao povjerljiv posrednik. Pouzdani zapis je zabilježen u blockchainu koji se dijeli između svih sudionika u mreži [2].

Distribuirana glavna knjiga poznata je kao transakcijska kopija i pohranjen podatak od svake stranke ili čvora na blockchain mreži. Konflikti ili pogreške unaprijed se automatski rješavaju unutar baze podataka pomoću pravila glavne knjige. Fundamentalne karakteristike distribuirane glavne knjige uključuje [2]:

- funkcioniranje s mrežom ravnopravnih računala
- decentralizirana pohrana izvršenih transakcija
- transakcije temeljene na povjerenju ili konsenzusu i
- otpornost na neovlašteno rukovanje.

Blockchain je sličan bazama podataka, ali se općenito ne koristi za pohranu podataka nego za pohranu informacija o transakcijama. Nekada će blockchain posjedovati same transakcije ili posjedovati dokaz o ispravnosti transakcije [2].

2.1. ELEMENTI BLOCKCHAINA

Blockchain se sastoji od tri osnovna dijela [2]:

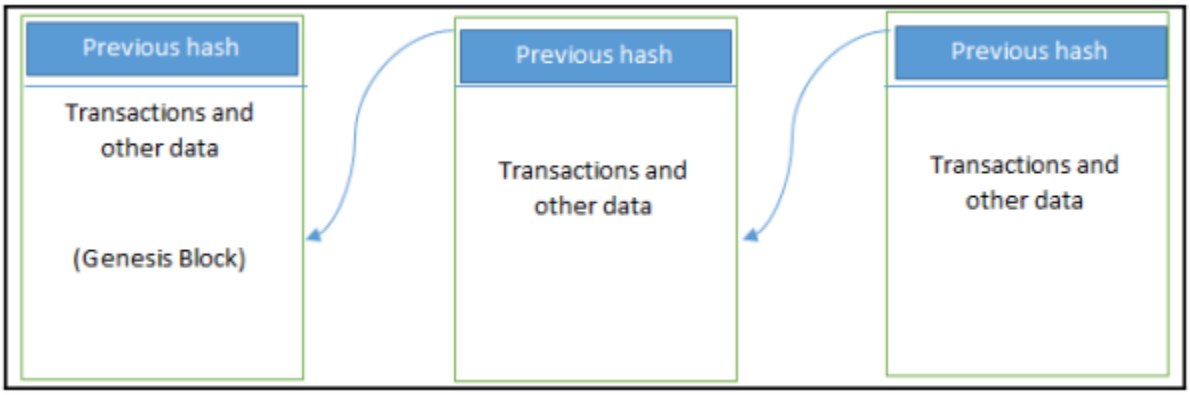
- Blok – popis zabilježenih transakcija tijekom razdoblja. Transakcije mogu predstavljati gotovo bilo koju aktivnost od upisa u zemljišne knjige do pojedinačne kupnje. Sva pravila vezana za sami blok temelje se kada se mreža kreira prvi put. Primjerice, maksimalni broj transakcija u blok ili veličina bloka može se ograničiti.
- Lanac – kada blok dosegne maksimalni broj transakcija, on se veže ili niže na prijašnji blok u *hash*. Hash vrijednost jednog bloka umeće se u sljedeći blok. To čini vezu između novog bloka i prethodnoga. Ponavljajući hash funkciju na isti blok podataka, uvijek će generirati istu vrijednost jednake dužine. Konačna hash vrijednost bit će drugačija ako je došlo do izmjene podataka u bloku. Korisnik može vidjeti da je hash promijenjen i zaključit će da je izvorni blok promijenjen i da nije pouzdan.
- Mreža – mreža se sastoji od čvorova koji sadrže cijeli zapis svih transakcija na blockchainu. Ne postoji „službena“ centralizirana kopija i nijedan čvor nije „pouzdan“. Integritet podatak na blockchainu održava se tako što se on kopira na sve ostale čvorove.

Čvor možemo predočiti kao grupu servera koja rade na blockchainu. Operateri čvorova potiču se da upravljaju čvorovima tako da ih se nagrađuje za njihov trud. Primjerice, kod kriptovaluta (engl. *cryptocurrency*) čvorovi se natječu da riješe kriptografske zagonetke. Ostali čvorovi moraju potvrditi rješenje čvora koji prvi riješi zagonetku. Kada je rješenje potvrđeno, čvor koji je riješio zagonetku dodaje blok na blockchain i nagrađen je kriptovalutama za svoj rad. Taj se proces naziva rudarenjem u koji su uključeni rudari s resursima. Čvorovi su raspoređeni diljem svijeta zbog čega je njihovo upravljanje zahtjevno. Približno je potrebno oko pet tisuća čvorova za infrastrukturu jedne kriptovalute. Rudari nisu nužni za ostale dijelove blockchaina, ali su zato potrebni za platformu kriptovaluta. Svaki blockchain ima svoja pravila ili algoritme preko kojih čvorovi

upravljaju s potvrđivanjem transakcija koje imaju za cilj unos na blockchain. Ta se pravila zovu mehanizmi konsenzusa i uspostavljaju se prilikom kreiranja blockchaina. Ugrađivanjem mehanizma konsenzusa blockchain stvara način za strane koje ne znaju mogu li jedna drugoj vjerovati oko unosa u blockchain. Time se obračunava s problemom bizantskih generala [2].

Problem bizantskih generala je problem gdje se mora postići jedinstveni plan akcije kako bi se osvojio neprijateljski grad. Generali komuniciraju samo putem glasonoša. No, neki od tih generala mogu biti izdajice kojima je cilj spriječiti lojalne generale od izvršenja plana i donošenja konsenzusa, odnosno slaganja oko plana napada [3].

Svaki blockchain ima svoj mehanizam konsenzusa ovisno o tipu transakcija koje zapisuje. Za sada su poznata tri mehanizma konsenzusa: *proof of work, proof of space* i *proof of stake*. Ti mehanizmi olakšavaju autentičnost ili nepromjenjivost transakcijskih zapisa. Svaka stranica u knjizi transakcija formira blok u blockchain tehnologiji. Taj će blok imati utjecaj na sljedeći blok ili stranicu u kriptografski *hashing*. Kada je blok dovršen, on stvara jedinstveni sigurnosni kod koji je vezan za sljedeći blok ili stranicu na taj način stvarajući lanac blokova ili blockchain (Slika 1.) [2].



SLIKA 1. OPĆA STRUKTURA BLOCKCHAINA [1]

2.2. KRIPTOGRASKA HASH FUNKCIJA

Kriptografska hash funkcija je posebna klasa hash funkcije koja ima određena svojstva koja je čine prikladnom za uporabu u kriptografiji. Općenito, hash funkcija je bilo funkcija koja za ulaz ima podatke proizvoljne veličine, a kao izlaz vraća podatke fiksne veličine. Vrijednost hash

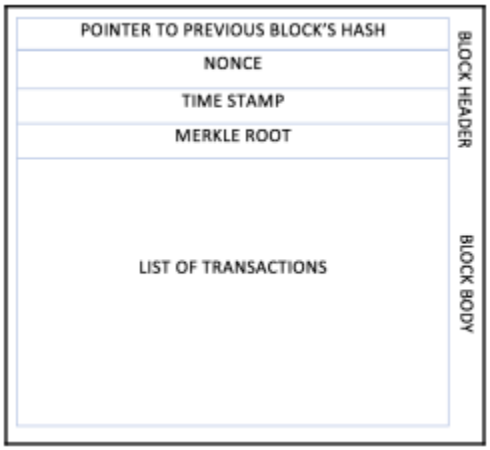
funkcije često naziva hash vrijednost ili kratko hash dok se ulazni podatak naziva poruka. Kriptografske hash funkcije su jednosmjerne, odnosno nemaju inverziju. Jedini način da se kreiraju ulazni podaci kriptografske hash funkcije iz izlaza je pokušati pretraživanje brute-force algoritmom, isprobavanjem svih mogućih vrijednosti ulaza kako bi se vidjelo koji od ulaza odgovara izlazu koji posjedujemo. Poželjno je da kriptografska hash funkcija zadovoljava sljedećih pet svojstava [4]:

- Deterministička je. Vrijedi ako su dva izlaza dobivena pomoću iste funkcije različiti, tada su i ulazi bili različiti.
- Lako i brzo se može izračunati vrijednost funkcije za bilo koji ulaz.
- Neisplativo je generirati ulaz za određeni izlaz isprobavanjem svih mogućih vrijednosti ulaza.
- Mala promjena na ulaznim podacima treba promijeniti vrijednost funkcije tako da se ne naslućuje nikakva sličnost između stare i nove vrijednosti funkcije.
- Postoji mogućnost kolizije, dobivanja istih vrijednosti za različite ulazne podatke, ali je neisplativo traženje dvaju takvih ulaznih podataka [4].

Kriptografske hash funkcije imaju mnogo primjena. Mogu se koristiti za implementaciju različitih struktura podataka poput tablica, lista ili stabala. Primjenjuju se za digitalno potpisivanje poruka između korisnika u nesigurnom sustavu. Također pri radu s datotekama hash funkcije omogućuju stvaranje digitalnog „otiska prsta“ (engl. *fingerprint*) na sadržaj datoteke. Pomoću „otiska prsta“ lako je identificirati je li sadržaj datoteke promijenjen. Mnogi operacijski sustavi koriste kriptografske hash funkcije za enkripciju zaporki te su one sastavni dio mnogih mehanizama za provjeru autentičnosti. Kriptovalute takve funkcije koriste kako bi bez središnjeg autoriteta postigle siguran prijenos novca [4].

2.3. STRUKTURA BLOKA

Blockchain se sastoji od niza blokova koji su lančano povezani. Blok (Slika 2.) sastoji se od zaglavlja bloka i tijela bloka. Zaglavlje bloka sadrži informacije o bloku dok tijelo bloka pohranjuje informacije o transakcijama [1].



SLIKA 2. GENERALNA STRUKTURA BLOKA [1]

TABLICA 1. STRUKTURA BLOKA

Veličina	Naziv	Opis
4 bajta	veličina bloka	veličina bloka u bajtovima
80 bajtova	zaglavlje bloka	metapodaci o bloku
1 – 9 bajtova	brojač zapisa	ukupan broj zapisa u bloku
varijabilno	zapisi	zapisi pohranjeni u bloku

Izvor: [1], [4]

Zaglavlje svakog bloka sastoji se od 80 bajtova podataka tablica 1. koji služe kao dodatne tehničke informacije o bloku i povezivanju blokova u lanac. Struktura zaglavlja bloka dana je u tablici 2. [4].

TABLICA 2. STRUKTURA ZAGLAVLJA POGLAVLJA

Veličina	Naziv	Opis
4 bajta	verzija	verzija protokola u vrijeme nastajanja bloka (samo za bitcoin)
32 bajta	Hash prethodnog bloka	Referenca na prethodni blok u lancu koji je još nazivamo roditelj bloka

32 bajta	korijen binarnog hash stabla	kriptografski hash koji sadrži informacije o svim zapisima u bloku
4 bajta	vremenska oznaka	vrijeme kada je blok kreiran i uključen u blockchain
4 bajta	težinska oznaka	težina algoritma čije je rješenje potrebno za uključivanje bloka u blokchain
4 bajta	*Nonce*	broj pomoću kojeg je riješen algoritam za uključivanje bloka u blokchain

Izvor: [1], [4]

Hash prethodnog bloka predstavlja rezultat dvostruke primjene SHA-256 (256-bitni algoritam za sigurno haširanje) hash funkcije nad zaglavljem prethodnog bloka u lancu. Hash bloka, koji je zapravo hash zaglavlja bloka, jedinstveni je identifikator svakog pojedinog bloka. Prema tablici 2. i 1. hash bloka zapravo nije dio strukture bloka. On se izračunava na strani svakog čvora kada čvor ima potrebe za tim, na primjer kada primi novi blok koji je uključen u lanac. Također, u svrhu vremenske uštede čvor može održavati zasebnu bazu podataka u kojoj su spremljeni hashevi blokova. Vremenska oznaka predstavlja vrijeme kada je blok dodan u lanac. Polja težinska oznaka i nonce su metapodaci koji se koriste prilikom dodavanja bloka u lanac. Korijen binarnog hash stabla predstavlja informaciju dobivenu od svih zapisa u bloku [4].

2.4. VRSTE BLOCKCHAINA

Postoje tri vrste blockchaina, a to su javni, privatni i hibridni. Javni blockchain nije ni u čijem vlasništvu. On je otvoren prema svima i bilo tko može sudjelovati kao čvor u procesu donošenja odluka. Korisnici mogu i ne moraju biti nagrađeni za svoj doprinos. Korisnici glavnih knjiga bez dozvole ili bez ovlaštenja održavaju kopiju glavne knjige na svom lokalnom čvoru i koriste distribuirani mehanizam konsenzusa kako bi odlučivali o konačnom stanju glavne knjige. Bitcoin i Ethereum smatraju se javnim blockchainom [1].

Privatni je blockchain jedino otvoren prema udruženim ustanovama, grupama pojedinaca ili organizacijama koje su odlučile dijeliti glavnu knjigu između sebe. Postoje različiti blockchaini koji su dostupni u toj kategoriji kao što su *HydraChain* i *Quorum*.

U hibridnim blockchainima dio blockchaina je javan, a dio je privatan. Treba napomenuti da je danas to još uvijek koncept i Proof of Concept još nije razvijen. U hibridnim blokchainima privatni dio kontroliraju grupe pojedinaca dok je javni dio otvoren prema svima koji žele sudjelovati. Hibridni se model može koristiti u slučajevima gdje privatni dio blockchaina ostaje interni i dijeljen između poznatih sudionika dok javni dio blockchaina može koristiti bilo tko uz mogućnost da rudarenjem osiguravaju blockchain. Na takav način čitav blockchain je osiguran koristeći Proof of Work čime se pruža valjanost i postojanost za javni i privatni dio blockchaina. Ovakva vrsta blockchainaa može se nazvati polucentralizirani model gdje je upravljan jednim entitetom, ali dopušta više korisnika da se pridrži mreži pritom da slijede odgovarajuće procedure [1].

2.5. ALGORITMI

Konsenzus je proces dogovora između distribuiranih čvorova oko konačnog stanja podataka. Koriste se različiti algoritmi kako bi se postigao konsenzus. Jednostavno je postići dogovor između dva čvora, ali kada više čvorova sudjeluje u distribuiranom sustavu i trebaju postići dogovor oko jedne vrijednosti, tada postaje izazov kako bi se postigao konsenzus. Distribuirani konsenzus je proces postizanja dogovora oko zajedničkog stanja ili vrijednosti između višestrukih čvorova s time da neki čvorovi mogu zakazati [1].

Konsenzus predstavlja okosnicu blockchaina kao rezultat toga osigurava decentraliziranu kontrolu u dodatnom procesu poznatom kao rudarenje. Izbor o tome koji će se algoritam konsenzusa koristiti ovisi o vrsti blockchaina, tj. nisu svi tipovi blockchaina pogodni za svaki algoritam konsenzusa. Tako je Proof of Work pogodniji za javni blockchain bez dozvole nego da se koristi jednostavni mehanizam za dogovor koji se bazira na Proof of Authority. Zbog toga je jako bitno odabrati odgovarajući konsenzusni algoritam za specifični blockchain projekt [1].

Mehanizam konsenzusa je niz koraka koji su poduzeti od većine ili svih čvorova u blockchainu kako bi se dogovorili oko predloženog stanja ili vrijednosti. Postoje razni uvjeti koji se moraju zadovoljiti kako bi se postigli traženi rezultati u mehanizmu konsenzusa [1]:

- Dogovor - svi pošteni čvorovi odlučuju o istoj vrijednosti

- Raskid - svi pošteni čvorovi izvršavaju raskid proces konsenzusa i u konačnici dođu do odluke
- Valjanost – vrijednost oko koje se dogovore svi pošteni čvorovi mora bit jednaka vrijednost početne vrijednosti koja je predložena od barem jednog poštenog čvora
- Otporan na kvarove – algoritam konsenzusa mora biti sposoban raditi u prisutnosti pogreške ili zlonamjernih čvorova
- Integritet – uvjet koji mora bit zadovoljen kako ne bi jedan čvor mogao donijeti više do jedne odluke u jednom konsenzusnom ciklusu.

Konsenzus je koncept distribuiranog računalstva koji se koristi u blockchainu kako bi se pružio način dogovora oko jedine verzije istine između kolega u blockchain mreži [1].

Za potrebe ovog rada opisat će se algoritmi konsenzusa koji se mogu najčešće sresti u praksi:

- Proof of Work (PoW) - ovaj tip mehanizama konsenzusa oslanja se na dokazu po kojem se mora prije potrošiti adekvatna računalna sredstava nego li se može predložiti vrijednost koju će mreža prihvatiti
- Proof of Stake (PoS) - ovaj algoritam radi na ideji da čvor ili korisnik ima adekvatan udio u mreži, tj. korisnik je uložio dovoljno u sustav da bi prevagnulo bilo kakav pokušaj zlonamjernog djelovanja korisnika i korist koju bi time dobio. Peercoin je prvi predstavio takvu ideju, a koristi se i u Ethereum blockchainu verziji *Serenity*. Još jedan važan koncept kod PoS je *coin age* koji predstavlja izvedeni kriteriji za vrijeme i količina kovanica koji nisu potrošeni. U ovakvom modelu što je veći *coin age* raste prilika za predlaganje i upisivanje sljedećeg bloka.
- Delegated Proof of Stake (DPoS) - predstavlja inovaciju naspram PoS gdje svaki čvor koji ima udio u mreži može glasovanjem odrediti valjanost transakcija drugim čvorovima [1]

2.6. BLOCKCHAIN PARTNER

Blockchain partner održava blockchain sa svim zapisima počevši od prvog bloka na koji se nadovezuju svi ostali blokovi sve do zadnjeg kreiranoga. Za razliku od novčanika blockchain

partner nema potrebe za oslanjanjem na ostale partnere u svrhu pretraživanja blockchaina ili provjere integriteta podataka. Ako je riječ o zapisu transakcija u blockchainu, blockchain partner u svrhu validacije nove transakcije ima mogućnost provjeriti pripadaju li sredstva koja korisnik želi potrošiti u novoj transakciji zaista tom korisniku. To će napraviti na način da poveže novu transakciju sa svim prijašnjim transakcijama tog korisnika sve do generičkog bloka. Takav partner oslanja se na ostatak mreže samo kako bi u realnom vremenu primio novokreirane blokove koje nakon toga verificira i nadovezuje na svoju lokalnu kopiju blockchaina [4].

2.6.1. NOVAČNIK ZA KRIPTOVALUTE

Glavna zadaća koju novčanik obavlja je kreiranje novih zapisa u skladu s protokolom koji propisuje sustav. Softverski se novčanik koristi za pohranu privatnog, javnog ključa i adresu kriptovaluta. U stanju je primati ili slati novčiće. Privatni se ključ generira slučajno tako da se nasumično izabere 256-bitni broj od softvera. Novčanik za kriptovalute koristi privatne ključeve za potpisivanje odlaznih transakcija dok se javni ključevi koriste za potpisivanje dolaznih transakcija. Novčanici ne pohranjuju novčiće i ne postoji koncept koje pohranjuje novčiće, oni ustvari i ne postoje nego se pohranjuju informacije o transakcijama na blockchain koje se koriste kako bi izračunao broj novčića [1].

2.6.1. RUDAR KRIPTOVALUTA

Partneri rudari preuzimaju nove zapise koje su kreirali novčanici, formiraju ih u blokove i dodaju u blockchain [4].

Rudar je mrežni čvor koji traži prihvatljiv PoW za nove blokove tako što ponavlja *hashing*. Rudar ustupa računalne resurse (procesorska moć središnje procesorske jedinice ili grafičke procesorske jedinice) za rješavanje PoW kako bi potvrdio i zabilježio transakciju u blok te dodao u blockchain. Rudar je nagrađen novčićima kada otkrije novi blok rješavanjem PoW. U slučaju bitocoina rudarima se plaća i naknada za transakciju za to što dodaju transakcije u odgovarajuće blokove [5].

3. PREDNOSTI I NEDOSTACI BLOCKCHAIN TEHNOLOGIJE

Svaka nova tehnologija dolazi sa svojim prednostima i nedostacima. U ovom će se poglavlju prikazati prednosti i nedostaci koje donosi sa sobom blockchain.

3.1. PREDNOSTI BLOCKCHAIN TEHNOLOGIJE

Blockchain tehnologija je decentralizirani sustav i to je glavna prednost korištenja ove tehnologije. To podrazumijeva da ne mora nužno surađivati s organizacijama trećih strana ili sa središnjim upravama. Sustava funkcionira bez posrednika i svi sudionici sudjeluju u donošenju odluka [6].

Izbjegavanjem posrednika i njihovih usluga postiže se ušteda novca koji bi inače bio namijenjen njima, a novac se može negdje drugdje preusmjeriti [7].

Svaki sustav ima bazu podataka i ona se mora zaštititi jer kada baza podatka radi s organizacijama trećih strana postoji rizik od hakerskog napada na bazu podatka što može rezultirati da podaci iz baze podatak završe u krivim rukama. Zaštita baze podatka zahtijeva puno vremena i ulaganja. Korištenjem blockchain tehnologije ti se rizici mogu izbjeći jer blockchain tehnologija ima vlastiti dokaz ispravnosti i autorizacije s ciljem provođenja ograničenja. Svaka je aktivnost zabilježena na blockchainu, zapisi podatka dostupni su svakom sudioniku u blockchainu i ne mogu se obrisati ni promijeniti. Ovakav način zapisa omogućava blockchain tehnologiji da bude transparentna, postojana i pouzdana. Pouzdanost se blockchain tehnologije zasniva na dva ili više sudionika koji se ne znaju međusobno. Transakcije koje su stvarne i imaju svrhu odvijat će se između nepoznatih osoba. Pouzdanost se može povećati dodavanje još zajedničkih procesa i zapisa. Potvrđene transakcije su nepromjenjive i raspoređene se preko cijelog blockchaina. Nije moguće promijeniti ni obrisati transakciju koja je pridodana blockchainu. Također, ovisi o kakvom se sustavu radi jer ako je sustav centraliziran tada jedna osoba može u njemu mijenjati brisati, tj. donositi odluke. U sustavu koji je decentraliziran i oslanja se na blockchain svaka će se transakcija pridodati i kopija te transakcije i bit će zapisana na svakom računalu koji se nalazi u blockchain mreži. Takve odlike čine blockchain tehnologiju nepromjenjivom i neuništivom te takav način rada omogućava

korisnicima blockchaina da kontroliraju sve informacije i transakcije. Izmjena ili brisanje informacija, uključujući i zapise prije nego budu dodani u blockchainu, moguće je jedino ako uljez ima veliku procesorsku moć. Blockchain koji ima umreženo mali broj računala ranjiviji je nego onaj koji ima veliku količinu računalo te ujedno čini blockchain sigurnijim i transparentnijim. Transparentnost blockchaina postiže se procesom kopiranja transakcija jer se kopija transakcije pohranjuje na svakom računalu u blockchain mreži. Transparentnost i otvorenost je postignuta jer svaki sudionik može vidjeti sve transakcije što ujedno znači da je svaka aktivnost prikazana sudionicima u blockchanu. Nitko ne može ništa napraviti, a da se ne primijeti. Blockchain je dizajniran tako da može prikazati problem ako dođe do njega i ispraviti ga ako je to potrebno. Prednost blockchain tehnologije je da se sve može pratiti. Visoka razina sigurnosti blockchain tehnologije postiže se pri individualnom ulazu u mreži zato što je svaka osoba koja pristupa blockchainu osigurana s jedinstvenim identitetom koji je povezan s njihovim računom [6].

Korištenje javnih i privatnih ključeva osigurava visoku razinu sigurnost. Javni ključ predstavlja korisnikovu adresu unutar blockchaina gdje privatni ključ predstavlja lozinku koja omogućava korisniku pristup njegovoj/njezinoj digitalnoj imovini i omogućava interakciju s raznim mogućnostima koje pruža blokckhain [7].

Blockchain je siguran zato što koristi pouzdani lanac koji čini kriptografski hash. Svaki put kada je blok kreiran, potrebno je izračunati hash vrijednost za novi blok. Ujedno novi hash uključuje i prethodnu hash vrijednost. Hash se sastoji od identifikacijskog broja bloka, prethodne hash vrijednosti, vremena kada je blok kreiran, identifikacijskog broja korisnika, rudareve komponente i Merkleov korijen gdje su informacije pohranjene o prijašnjim transakcijama i hashevima. Samim time nemoguće je izmijeniti informacije u hash vrijednosti [6].

Podaci ne mogu završiti u blockchainu ako nisu potvrđeni, što uklanja mogućnost unosa krivih podataka i ostale pogreške koje bi mogle nastati ljudskim djelovanjem [7].

Postojanje više glavnih knjiga može za sudionike sustava uzrokovati nered i komplikacije. Blockchain tehnologija je pojednostavljena jer se sve transakcije dodaju u javnu glavnu knjigu. Još jedna prednost blockchain tehnologije je brže vrijeme obrade. Tradicionalno, bankarske su transakcije sporije i mogu potrajati do tri dana od njihovog pokretanja do njihovog potvrđivanja. U blockchain tehnologiji to može trajati u minutama ili sekundama [6].

Zbog svojih odlika i karakteristika blockchain tehnologija odličan je izbor za one grane industrije kojima je brzina, točnost, sigurnost i pouzdanost bitna za svakodnevno funkcioniranje. Ne moraju se koristiti samo za kriptovalute nego se mogu primijeniti i u financijskom sektoru, osiguravajućim kućama, državnim službama, administrativnim poslovima, kampanjama za prikupljanje novčanih sredstava, izvršavanju ugovora, izvršavanju transakcija za nekretnine, maloprodaji i proizvodnji, zdravstvenoj skrbi, prodaji glazbe i organiziranju demokratskih izbora [7].

3.2. NEDOSTACI BLOCKCHAIN TEHNOLOGIJE

Svaka tehnologija koja ima prednosti mora imati i nedostatke. Blockchain tehnologija ne može pohraniti veliku količinu podataka i to se ne može mijenjati [7].

Iako postoji blockchina koji se temelji na protokolu, dokaz o prostoru (engl. *Proof of Space*), gdje rudari umjesto da ustupaju procesorsku moć ustupaju slobodan prostor na čvrstom disku, nije povezano s problemom pohrane podataka [8].

Glavni je nedostatak blockchain tehnologije velika potrošnja električne energije. Stalna potrošnja električne energije potrebna je kako bi se glavna knjiga održavala u realnom vremenu [6].

Problem s velikom potrošnjom električne energije je danas posebno osjetljiva tema budući uslijed dugih sušnih perioda došlo je opadanja vodostaja rijeka što ugrožava proizvodnju električne energije putem hidroelektrana. Za vrijeme pisanja ovog rada Europa se našla u energentskoj krizi zbog sankcija koja je nametnula Ruskoj Federaciji zbog agresije na Ukrajinu. Kako bi namirila dio potreba za električnom energijom Europska unija ju je uvozila iz Ruske Federacije [54].

Prilikom kreiranja čvora uspostavlja se komunikacija sa svim ostalim čvorovima čime se postiže transparentnost. Za potvrđivanje transakcije na mreži rudari koriste veliku količinu električne energije. Zbog toga čvorovi imaju veliku toleranciju na pogreške i neprekidan rad čini podatke pohranjene na blockchainu nepromjenjivim i otpornima na cenzuru. Ovakvim načinom rada dolazi do rasipanja električne energije i vremena jer svaki čvor ponavlja postignuće do kojeg se prethodno došlo konsenzusom. Potvrda potpisa predstavlja izazov za blockchain jer svaka transakcija mora

biti potpisana pomoću kriptografske sheme za koju je potrebna velika procesorska moći kako bi ona bila potpisana. Također, predstavlja jedan od razlog za veliku potrošnju električne energije. Sljedeći problem do kojeg može doći je podjela lanca. Čvorovi neće prihvatiti transakciju na novom lancu ako funkcioniraju na starom softveru. Povijest starog lanca koji se temelji na starom softveru koristit će se za kreiranje novog lanca. Taj se proces naziva račvanje i postoje dvije vrste račvanja, meko i tvrdo. Meko račvanje uspostavlja nova pravila za blokove u protokolu. Čvorovi se moraju ažurirati kao bi provodili novo uspostavljena pravila. Blokovi koji su prije bili ispravni, a nisu u skladu s novim pravilima koju su nastali mekim račvanjem, neće se uzeti u obzir. Naprimjer, ako je veličina bloka prije bila 1MB, a novo pravilo propisuje veličinu od 500kB, to znači da svi blokovi koji dođu veći od 500kB neće biti potvrđeni u novom lancu. Meko račvanje koristi se kada se želi postrožiti pravila u novom lancu. Tvrdo račvanje koristit će se kada želimo popustiti pravila za blokove u protokolu. U mekom račvanju veličina bloka smanjivala se s 1MB na 500kB dok se kod tvrdog račvanja povećava na 2MB. Ako blok zadovolji sva pravila tvrdog račvanja bit će dodan u lanac čak da prethodno nije bio u lancu. Uspostavljanje ravnoteže između količine čvorova i povoljnih troškova za korisnike je izazov s kojim se blockchain mora boriti. Ako nema dovoljno čvorova za ispravan rad s potrebnom moći, troškovi za korisnike bit će veći jer čvorovi dobivaju veće naknade. Čvorovi stavljaju prioritet na transakcije koje nose sa sobom veće naknade, a one koje nose manje naknade bit će sporije završene i čvorovi neće aktivno raditi. Blockchain raste kako se dodaju novi blokovi i dolazi do potrebe za većom procesnom moći. Svi čvorovi ne mogu osigurati potreban kapacitet kada dođe do povećanja. Zbog toga dolazi do dva problema. Prvi problem je da je glavna knjiga manja zato što čvorovi ne mogu imati cijelu kopiju blockchaina čime se krši postojanost i transparentnost blockchaina. Drugi je problem da blockchain postaje centraliziraniji što je u suprotnosti s korištenje blockchaina. Zbog velike potrošnje električne energije cijene naknada za obavljanu transakciju postaju visoke. Prosječna naknada po transakciji je od 75 do 160 dolara. Veliki inicijalni kapitalni troškovi isto pridonose visokoj cijeni naknade za obavljanu transakciju [6].

Blockchain u usporedbi s centraliziranim sustavom nije skalabilan. Primjer je Bitcoin mreža gdje brzina obavljanih transakcija ovisi o zagušenosti mreže. Povećanjem broja čvorova i korisnika povećava se vjerojatnost za usporavanjem mreže. Rješenje koje se nameće za problem usporavanja mreže je da se transakcije obavljaju izvan blockchain mreže, a blockchain se koristi za pohranu i pristup informacijama. Dodatna dva rješenja koja se mogu uzeti u obzir su postavljanje mreže s

pristupom ili korištenje blockchaina s drugačijom arhitekturom. Može se reći da je blockchain tehnologija sigurna tehnologija zbog svoga načina rada, ali nije bez ranjivosti. Blockchain tehnologija ima pet sigurnosnih propusta [9]:

- Napad s 51 % - napad je na blockchain od pojedinca ili grupe koja kontrolira više od 50 % hash snage za rudarenje na mreži. Napadači koji kontroliraju većinu mreže mogu spriječiti druge rudare da dovrše blok tako što prekinu zapisivanje u novi blok. Ovakav će napad omogućiti napadačima da kreiraju nedosljedan blok koji će sadržavati transakcije koje se nikada nisu dogodile. S ovakvim napadom na određenom blockchainu mogu se kreirati novi novčići koji se mogu pohraniti u napadačev novčanik [10]
- Dvostruko trošenje - napad je u kojem dolazi do trošenja više od jednom po transakciji određenog skupa novčića. Postoji rizik da digitalne kriptovalute mogu biti potrošene dvaputa, što je nemoguće s fizičkim novcem jer ne možete istu novčanicu dati dvjema fizičkim osobama. Dvostruko trošenje dolazi kao posljedica napada od 51 % [11]
- Distribuirani napad uskraćivanja usluga – pojavljuje se kada više (prethodno) kompromitiranih sustava preplavljuje resurse ciljanih sustava, jednog ili više poslužitelja [12].

  Blockchain serveri, kriptomjenjačnice, kriptonovčanici na mreži i ostale usluge povezane s blockchain tehnologijom mogu biti žrtve distribuiranog napada uskraćivanje usluge (engl. DDoS - *Distributed Denial-of-Service*). DDoS napad se izvršava putem uređaja koji ima pristup internetu, a on je povezan na centralnu točkom koju predstavlja server. DDoS napad mora imati pristup više različitih čvorova u isto vrijeme kako bi napravio značajnu štetu mreži zato što je blockchain decentralizirani sustav koji je povezan s višestrukim čvorovima. DDoS napadi mogu se spriječiti daljnjom decentralizacijom mreže. Decentralizacijom mreže smanjio bi se opseg DDoS napada i omogućila bi se propusnost servera koji su pod napadom bez da se ugrožava lanac. Čak da i neki serveri budu narušeni tako da nisu funkcionalni ili je poremećen njihov rad, blockchain može i dalje biti operativan i potvrđivati transakcije. Čvorovi koji su doživjeli poremećaj u radu mogu se oporaviti i ponovno sinkronizirati s onima koji nisu bili pod utjecajem DDoS napada [13].
- Sybil napad – vrsta je napada gdje napadač kreira pseudoračune kako bi se predstavljao kao više osoba. To predstavlja veliki problem pri povezivanju na mrežu ravnopravnih računala. Napadač kontrolira i manipulira s cijelom mrežom koju je zadobio kreiranjem lažnih

identiteta. U Sybil napadu napadač ima za cilj napasti cijelu mrežu. Jedini način kako spriječiti Sybil napad je da se poveća trošak kreiranja novog identiteta. Trošak kreiranja novog računa mora biti uravnotežen kako ne bi bio skup za one korisnike koji žele napraviti legitimne račune. Također cijena kreiranja novog računa mora biti dovoljno visoka kako bi kreiranje velikog broja računa u malom vremenskom razdoblju bilo skupo [14].

- Dekriptiranje - obrnuti postupak kojim se može doći do kriptiranih podataka koristeći kvantnim algoritmima kao što je Shora algoritam koji može dekriptirati RSA enkripciju. Ali se radi na istraživanjima s kriptografskim algoritmima koji se temelje na hash funkciji [6].

4. KRIPTOVALUTE – BITCOIN I ETHEREUM

U ovom će se poglavlju upoznati s bitcoinom i ethereum kriptovalutom. Bitcoin predstavlja mrežu s konsenzusom koja omogućava slanje i primanje digitalnih valuta. Bitcoin je uspješno premostio izazove s kojima su se suočavale digitalne valute opisano u Poglavlju 3.2 te je nastao kao odgovor na inflaciju koja predstavlja pad vrijednosti tiskanog novca i financijske krize koje su se događale neodgovornim ponašanjem financijskoga i bankarskog sustava. Bitcoin ujedno predstavlja standard koje ostale kriptovalute ugrađuju u svoj rad. Ethereum je alternativa Bitcoinu s time da se na njemu može i programirati uz funkciju prijenosa sredstava s računa na račun uz naknadu.

4.1. BITCOIN

Bitcoin je predstavljen 2008. godine pod člankom *Bitcoin: A Peer-to-Peer Electronic Cash System*. Autor članka je Satoshi Nakamoto za koje se pretpostavlja da je pseudonim ili pravo ime osobe ili grupe ljudi. Glavna ideja koja se prezentirala u članku je elektronički novac u mreži ravnopravnih poslužitelja gdje ne postoji potreba za posrednikom kao što je banka za prijenos novčanih sredstava između sudionika. Bitcoin je izgrađen na temelju desetljeća istraživanja koja se bave kriptografijom kao što je Merkle stablo, hash funkciji, kriptografiji javnih ključeva i digitalnog potpisa. BitGold, B-money, hashcash i vremenske su oznake koje su uz pomoć kriptografije postavili temelje za nastanak bitcoina. Pametnim kombiniranjem tih tehnologija kreiran je bitcoin koji predstavlja prvu decentraliziranu valutu. Problem bizantskih generala (opisano u Poglavlju 2.2) glavni je problem na koji je bitcoin dao rješenje zajedno s problemom dvostrukog trošenja (opisano u Poglavlju 3.2). Originalna ideja iza kreiranje bitcoina je razvoj sustava e-novac kojem nije potreban pouzdani posrednik, a korisnici bi bili anonimni. Bitcoin može biti definiran na više načina od toga da je protokol, digitalna valuta i platforma. Bitcoin predstavlja kombinaciju mreže ravnopravnih poslužitelja, protokola, softvera koji olakšava stvaranje i korištenje digitalne valute bitcoin. Bitcoin s velikom početnim slovom "B" koristi se kako bi se odnosilo na Bitcoin protokol gdje bitcoin s malim početnim slovom "b" se odnosi na valutu. Čvorovi u mreži ravnopravnih sudionika komuniciraju međusobno koristeći Bitcoin protokol [1].

4.1.1. TRANSAKCIJE

Bitcoin se ne pohranjuje na korisnikovo lokalno računalo. On je ulazi u blockchain. Dok centralizirane digitalne valute pohranjuju račune i iznose, Bitcoin na blokchain pohranjuje transakcije. Transakcije čini lista ulaznih transakcija i lista izlaznih transakcija. Svaka izlazna transakcija sadrži dva podatka: količinu novca i adresu primatelja. Adresa je izvedena iz javnog ključa te jedino vlasnik tajnog ključa može otključati sredstva pohranjena u izlaznu transakciju. Kako bi pristupio sredstvima, vlasnik tajnog ključa mora potpisati transakciju kojom šalje sredstva na novu Bitcoin adresu. Ulazna transakcija sadrži izvješće o prethodnoj ulaznoj transakciji i potpis koji dokazuje da se mogu trošiti primljena sredstva iz prethodne izlazne transakcije. Potpis se mora napraviti pomoću tajnog ključa povezanog s javnim ključem u Bitcoin adresi. Ako se potpis ne poklapa, transakcija se smatra nevažećom i mreža je odbacuje. Transakcije se sastoje od nekoliko ulaznih i izlaznih transakcija, s tim da svaka mora sadržavati barem jedna ulaznu i jedna izlaznu transakcija. Njihova je svrha rasporediti sredstva među korisnicima. Ulazi transakcija odgovaraju izlazima prethodnih transakcija. Ti izlazi ne smiju biti potrošeni, inače se transakcija smatra nevažećom. Da bi transakcija bila valjana, zbroj iznosa ulaza mora biti veći ili jednak zbroju iznosa izlaza. Razlika između ulaza i izlaza (ukoliko postoji) je naknada za transakcije. Transakcijsku naknadu skupljaju rudari koji uključuju transakcije u blockchain. Izlazi u blockchainu mogu biti potrošeni samo jednom te moraju biti potrošeni u potpunosti. Ako je iznos izlaza veći od potrošenog iznosa, transakcija stvara ostatak. Pošiljatelj transakcije može prikupiti ovaj ostatak uključujući adresu ostatka kao dodatnu izlaznu transakciju. Činjenica da ostatak na adresi obično kontrolira pošiljatelj transakcije može se aktivno koristiti u algoritmima za rudarenje podataka primijenjenim na blockchain. Adresa s koje potječu sredstva može se koristiti kao adresa na koju će stići ostatak nakon obavljene transakcije, no ipak se preporuča generirati potpuno novu adresu za ostatak pri svakoj transakciji s ciljem povećanja privatnosti [15].

4.1.2. DIGITALNI KLJUČEVI

Na Bitcoin mreži adrese, javni ključevi i privatni ključevi predstavljaju oslonac za posjedovanje bitcoina i prijenos vrijednosti putem transakcija. U Bitcoin mreži kriptografija eliptičnih krivulja se koristi kako bi se generirali parovi javnih i privatnih ključeva. Privatni se ključevi moraju čuvati na siguran način i ne bi se smjeli dijeliti ni s kim. Privatni se ključevi koriste kako bi se digitalno potpisala transakcija i dokazalo vlasništvo na bitcoinima. Privatne ključeve predstavlja 256-bitni brojevi koji su nasumično odabrani u rasponu koji je definiran na preporuku secp256k1 ECDSA (engl. *Elliptic Curve Digital Signature Algorithm*) krivulje. Kako bi se lakše koristili i kopirali privatni ključevi, kodiraju se koristeći WIF (engl. *Wallet Import Format*). WIF omogućuje prikaz privatnog ključa u punoj dužini na drugačiji način. Privatni se ključ može konvertirati u WIF i obrnuto [1].

Javni ključevi postoje na blockchainu i mogu ih vidjeti svi sudionici u mreži. Zbog svoje specijalne matematičke veze s privatnim ključevima javni su ključevi izvedeni iz privatnih ključeva. Kada transakcija potpisana privatnim ključem bude emitirana Bitcoin mrežom, javni se ključevi koriste od čvorova kako bi potvrdili kako je transakcija doista potpisana s odgovarajućim privatnim ključem. Takvim procesom verifikacije dokazuje se posjedovanje bitcoina. Bitcoin koristi kriptografiju eliptičnih krivulja koje se temelje na standardu secp256k1. Točnije koristi ECDSA kako bi osiguralo da su novčana sredstva sigurna i da mogu bi potrošena od zakonitih vlasnika. Javni su ključevi jednake dužine kao i privatni ključevi [1].

4.1.3. DIGITALNI POTPIS

Svaka transakcija u blockchainu i svaki blok sadrži jedinstveni digitalni potpis. Digitalni potpis, pojednostavljeno je jedinstvena lozinka koja otključava Bitcoin novčanik i omogućava izvršenje transakcija. Svaka transakcija ima potpuno drugačiji digitalni potpis. Digitalni potpis je dokaz da je poruka autentična. S obzirom da svaka transakcija ima drugačiji digitalni potpis koji je jedinstven isključivo za tu transakciju, otklanja se mogućnost kopiranja lozinke koja je potrebna za otključavanje bitcoin novčanika. Digitalni je potpis jedna od zaštitnih mjera Bitcoin mreže koja sprečava pristup tuđim novčanim sredstvima. Digitalni potpis koristi dva ključa, privatni i javni.

Privatni se koristi za kreiranje potpisa, a javni kako bi ostali sudionici u mreži mogli provjeriti legitimnost transakcije. Može se reći da je privatni ključ prava lozinka korisnika, a da je potpis posrednik koji sprečava otkrivanje korisnikove lozinke. Za javni ključ može se reći da je dolazna adresa neke transakcije [16].

Da bi korisnik mogao trošiti novac, prvo mora dokazati da je pravi vlasnik adrese, tj. javnog ključa na kojeg je novac poslan. To se ostvaruje tako što se generira digitalni potpis iz transakcije poruke i svog privatnog ključa. Time se dolazi do zaključka da je digitalni potpis funkcija poruke i privatnog ključa. Zato što je digitalni potpis funkcija privatnog ključa i poruke, svaki je potpis drugačiji i ne može se ponovno koristiti za drugu transakciju. Time se također sprečava modificiranje poruke dok se prosljeđuje u mreži. Svaka promjena poruke učinit će je nelegitimnom. Prilikom obavljanja nove transakcije, kako bi transakcija bila autentična, sudionici u transakciji generiraju novi privatni i javni ključ te se poruka kodira hash funkcijom. Hash funkcija kreira 32-bitnu riječ bilo koje proizvoljne dužine poruke koristeći SHA-256 hash funkciju. Privatni i javni ključ u kombinaciji s porukom kodiranom SHA-256 hash funkcijom čine nemogućim predviđanje kriptiranog izlaza. Jedini način da se poruka dekodira je *pogađanjem* kako je ranije spomenuto. Moguće je da se traženi ključ pogodi iz prvog pokušaja, ali prosječno *pogađanje* traje oko 10 minuta. Ključna stvar prilikom *pogađanja* ključa je iznos hash brzine [16].

4.1.4. RUDARENJE BITCOINA

U Poglavlju 2.7.1. objašnjeni su općeniti zadaci rudara kriptovaluta, a u ovom pod poglavlju fokus je isključivo na rudarenje Bitcoina. U procesu rudarenja bitcoini se dodaju u opticaj. Također rudarenje osigurava sustav Bitcoina od lažnih transakcija ili od dvostrukog trošenja. Rudar osigurava računalnu snagu za Bitcoin mrežu u zamjenu za priliku da bude nagrađen s bitcoinom. Rudari potvrđuju nove transakcije i upisuju ih u glavnu knjigu. Svaki novi blok koji sadrži transakcije prethodnog bloka je *pronađen* svakih 10 minuta čime su transakcije dodane u blockchain. Transakcije koje čine blok i dodane su u blockchain smatraju se potvrđene što novom vlasniku bitcoina omogućava da ih troši. Rudari primaju dvije vrste nagrada za rudarenje, a to su novi novčići koji su kreiranu s novim blokom i transakcijske naknade za sve transakcije koje su uključene u blok. Rudari se natječu za nagrade rješavanjem složenih matematičkih problema koji

se temelje na kriptografskom hash algoritmu. PoW je uključen u novi blok i predstavlja dokaz da je rudar potrošio računalnu snagu. Sigurnost Bitcona leži u nadmetanju tko će prvi riješiti PoW algoritam kako bi zaradilo nagrade i dobilo pravo na zapisivanja transakcija u blockchain. Generiranje novih novčića naziva se rudarenje zbog nagrada koje su kreirane tako da simuliraju silazne prinose koje je karakteristično za rudarenje plemenitih metala. Rudarenjem je kreirana ukupna ponudu bitcoina što je jednako tiskanju novih novčanica središnje banke. Svake četiri godine smanjuje se količina novih bitcoina koje rudar može dodati u blok ili otprilike nakon svakih 210.000 blokova. U 2009. godine nagrada za blok je iznosilo 50 bitcoina dok u 2020. godine ona iznosi 6,25 bitcoina. Zbog formule prema kojoj se bitcoin nagrade eksponencijalno smanjuju, do 2140. godini svi će bitcoini biti *pronađeni*. Rudari bitcoina zarađuju i na naknadama za transakcije. Neće uvijek svaka transakcija uključivati naknadu koja predstavlja razliku bitcoina koji je poslan i koji je primljen. Rudar Bitcoina koji osvoji bitcoin zadržava razliku transakcije koja je uključena u dobitni blok. Naknade predstavljaju mali iznos koji rudari dobiju za rudarenje bitcoina, one se kreću od 0.5% ili manje ukupne zarade rudara. S vremenom će se nagrade za rudarenje bitcoina smanjivati jer će se smanjivati i broj bitcoina koji se može rudariti, stoga će se zarada od naknada povećati jer će biti i više transakcija. Poslije 2140. godine sva zarada rudara bit će u obliku naknada. Generiranje novih novčića ili nagrade nisu svrha rudarenja iako se na prvu tako čini jer nagrade potiču rudarenje i ulaganje u opremu za rudarenje. Rudarenje je ujedno i decentralizirani klirinški sustav po kojem se sve transakcije potvrđuju i poravnavaju. Bitcoin sustav je zaštićen rudarenjem koje omogućava rad mreže na temelju konsenzusa bez središnjeg autoriteta. Rudarenje ima ulogu decentraliziranog sigurnosnog mehanizma koji je temelj ravnopravnog digitalnog novca zbog čega je Bitcoin poseban [5].

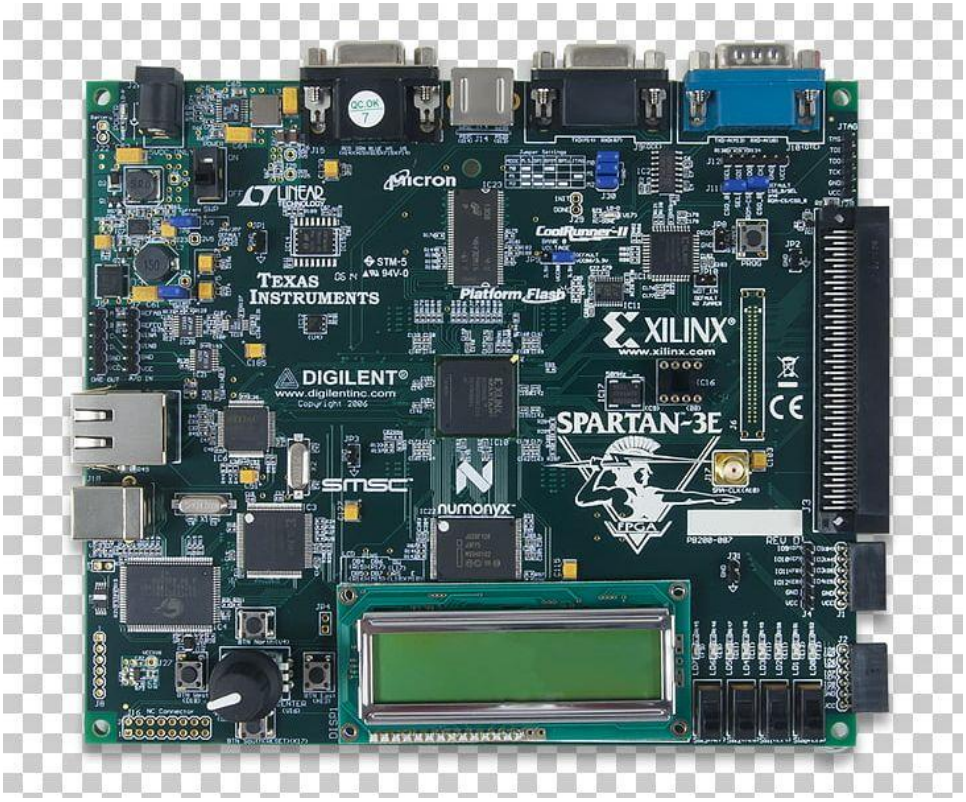
Za rudarenje prvog bitcoina korištene su središnje procesorske jedinice (Slika 3) koje se mogu naći u stolnim računalima i prijenosnim računalima. Rudarenje pomoću procesora bilo je profitabilno godinu dana od uvođenja Bitcoina i zamijenjeno je profitabilnijom hardverom.

SLIKA 3. SREDIŠNJA PROCESORSKA JEDINICA [17]

Sljedeći hardver koji su rudari koristili za rudarenje su grafičke kartice (Slika 4) koje su u sebi imale grafičke procesorske jedinice. Izračuni koji su programirani programskim jezikom OpenCL brže se izvode na grafičkim procesorskim jedinicama što je predstavljalo brže računanje nego korištenje procesora. Rudari kako bi maksimalizirali iskoristivost grafičkih kartica podizali su radni takt grafičkih procesora. Kako je moguće koristiti više grafičkih kartica po računalu, potražnja za njima je naglo porasla. Međutim, rudarenje grafičkim karticama ima ograničenja u obliku generirane topline, potrebe za specijaliziranim matičnim pločama i dodatnim hardverom koji omogućava montiranje više grafičkih kartica. Povećana potražnja za grafičkim karticama je negativno utjecala na sve one koji je žele kupiti i koristiti u druge svrhe [1].

SLIKA 4. GRAFIČKE KARTICE [18]

Poslije rudarenja pomoću grafičkih kartica došlo je do rudarenja pomoću programibilnih polja logičkih blokova (engl. FPGA - *Field Programmable Gate Array*), tj. integriranih krugova (Slika 5) koji se mogu programirati za određene operacije. FPGA se programira pomoću jezika za opisivanje sklopovlja kao što je Verilog i VHDL. Izvedba FPGA je bolja od grafičkih kartica, no problemi s pristupačnošću, težinom programiranja i zahtjevi za posebni vještinama iz programiranja te konfiguriranja FPGA nije omogućilo da se dugo zadrži [1].



SLIKA 5. FPGA [19]

Dolazak integriranih krugova za specifičnu primjenu (engl. ASIC - *Application Specific Integrated Circuit*) (Slika 6) ubrzao je nestanak rudarenja sustava koji su se oslanjali na FPGA. ASIC-i su dizajnirani da izvode SHA-256. Zbog brzog porasta težine za rudarenje profitabilnost jednog ASIC nije isplativa [1].

SLIKA 6. INTEGRIRANI KRUGOVI ZA SPECIFIČNU PRIMJENU [20]

4.2. ETHEREUM

Ethereum je globalna decentralizirana računalna infrastruktura otvorenog računalnog koda koja izvršava pametne ugovore. Koristi blockchain za sinkronizaciju i pohranu promjena stanja sustava, a kriptovalutu zvanu *ether* koristi za mjerenje i ograničavanje troškova izvršenja. Ether se označava s *ETH*, simbolom Ξ (dolazi od grčkog slova Xi) i ne tako često s ♦ . Ethereum omogućava programerima da konstruiraju moćne decentralizirane aplikacije s ekonomskim funkcijama. Smanjuje ili uklanja cenzuru i smanjuje određene rizike drugih strana pritom omogućavajući visoku razinu dostupnosti, transparentnosti i neutralnosti s mogućnošću revizije. Vitalik Buterin rusko-kanadski programer zajedno je s Gavinom Woodom 2013. godine osnovao Ethereum. Kao optimist za Bitcoinom Buterin je razmišljao kako proširiti mogućnosti Bitcona i Mastercoina (prekriveni protokol koji proširuje Bitcoin koji bi ponudio pametne ugovore). U listopadu iste godine predložio je timu Mastercoina ugovore s programskom podrškom i fleksibilnošću. Timu Mastercoina prijedlog se svidio, no bio je previše radikalan kako bi ga implementirali su svoj plan razvoja. Dva mjeseca kasnije u prosincu 2013. godine Vitalik je počeo dijeliti pregledani rad koji je opisivao Ethereum koji bi predstavljao blockchain za opću namjenu i *Turing-complete.* Cilj je bio postići blockchain koji bi omogućio programerima da razvijaju svoje aplikacije bez implementiranja mehanizma mreže ravnopravnih sudionika, blockchain, algoritam

konsenzusa itd. Iako Ethereum ima sličnosti s drugim javim blockchainima, u samoj je svrsi i konstrukciji drugačiji od ostalih uključujući i Bitcoin. Svrha Ethereuma nije da bude mreža za plaćanje digitalnom valutom, iako koristi ether valutu koja je sastavni dio Ethereum mreže i koja je potrebna za njezino djelovanje. Valuta ether zamišljena je da bude praktična valuta kojom se plaća korištenje Ethereum platforme kao svjetskog računala. Ethereum je dizajniran da bude automatiziran blockchain s općom svrhom koji se izvršava na virtualnom stroju koje je sposobno izvršavati složene računalne kodove dok Bitcoin ima ograničen programski jezik. Bitcoinov programski jezik namjerno je ograničen na ispitivanje istine/neistine prilikom trošenja gdje je Ethereumov jezik *Turing complete* što znači da može funkcionirati kao računalo [21].

4.2.1. ETHEREUM KORISNIČKI RAČUNI

Korisnički računi predstavljaju jednu od glavnih stavki Ethereum blockchaina. Na Ethereum se može gledati kao računalo koje je inicirano promjenama stanja zato što su stanja kreirana i ažurirana zbog interakcije korisničkih računa i izvršavanja transakcija. Prijelazna stanja su operacije koje se izvršavaju na korisničkim računima i između njih. Funkcija promjene stanja Ethereuma omogućava prijelazna stanja i radi na način da [1]:

- Potvrđuje ispravnost transakcija tako što provjerava sintaksu, ispravnost potpisa i *nonce* (broj pomoću kojeg je riješen algoritam)
- Adresa primatelja je zaključena pomoću potpisa, a naknada za transakciju je obračunata. Saldo se pošiljatelja provjerava i umanjuje za odgovarajući iznos dok se *nonce* povećava. Ako je iznos na računu nedovoljan, javit će se greška.
- Pomoću ethera se pokrivaju troškovi transakcije. Iznos troška transakcije je proporcionalno veličini transakcije koja se mjeri u bajtovima. Za vrijeme transakcije dolazi do prijenosa vrijednosti dok je smjer prijenosa od računa pošiljatelja do računa primatelja. Ako odredišna adresa koja je navedena u transakciji ne postoji, ona će se automatski kreirati. Kôd zapisan u ugovoru izvršit će se kada je odredišni korisnički račun naznačen u ugovoru. No, neće se svaki računalni kod izvršiti do kraja jer to ovisi koliko ima ethera na raspolaganju.

- Za situacije kada dođe do greške u transakciji zbog manjka iznosa ili nedovoljno ethera, sva promijenjena stanja vraćaju se u početno stanje osim naknade koja ide rudarima.
- Naknade se plaćaju rudarima u odgovarajućem iznosu, a ako postoji ostatak, on se šalje pošiljatelju, a u istom trenutku funkcija vraća konačno stanje koje se pohranjuje na blockchain.

Na Ethereum mreži postoje *Externally Owned Accounts* (EOA) i *Contract Accounts* (CA). EOA su povezani s korisnicima i njihova svojstva su da na sebi posjeduju ether saldo, mogu slati transakcije, nemaju na sebi pridružen računalni kod, kontrolirani su privatnim ključevima i sadrže ključeve za pristup bazama podataka. CA također sadrže u sebi ether saldo, imaju uz sebe pridružen računalni kod koji je čuva pohranjen ili u blockchainu memoriji. Mogu pokrenuti i izvršiti računalni kod na zahtjev transakcije ili poruke od drugih ugovora, održati svoje trajno stanje i pozivati druge ugovore, nisu povezani s korisnicima ni s bilo kojim akterima na blockchainu te isto posjeduju ključeve za pristup bazama podataka.

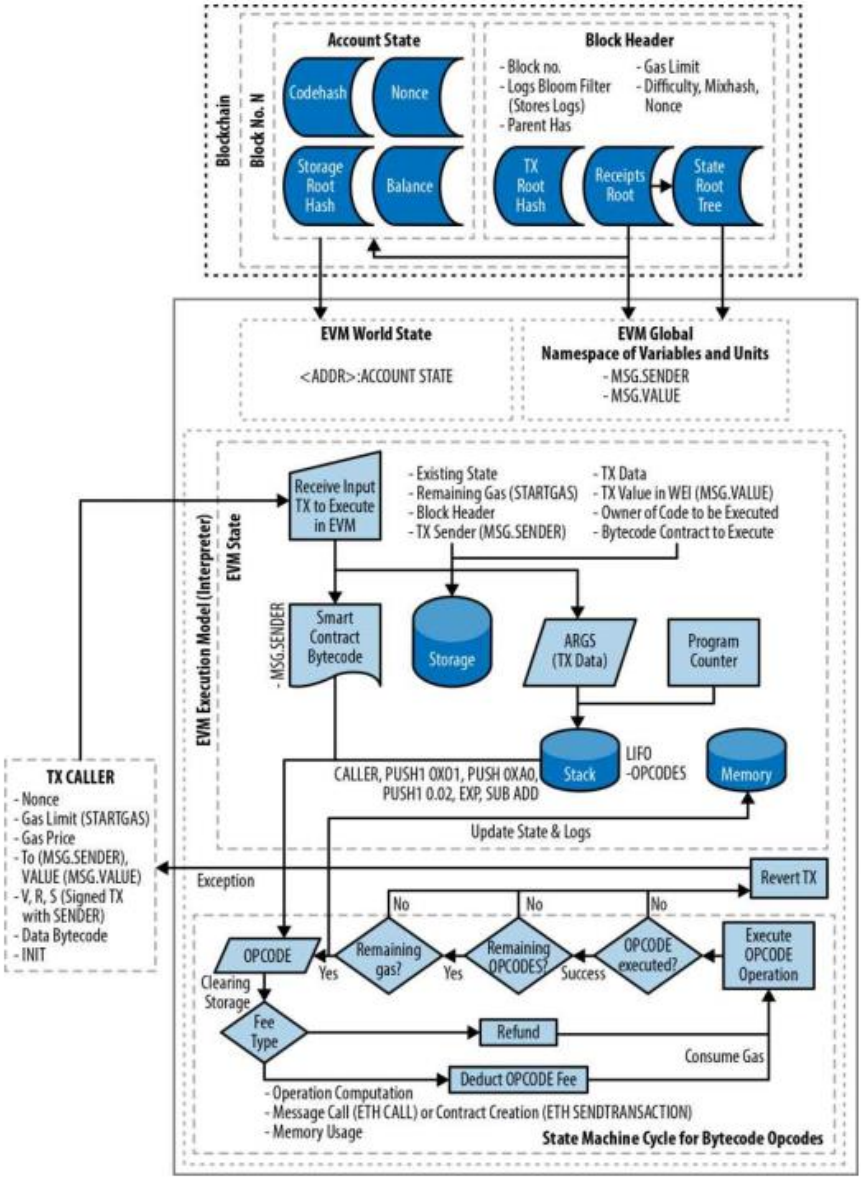
4.2.2. GAS

Gas nije ether nego je zasebna valuta koja ima vlastiti tečaj prema etheru. Ethereum koristi gas kao kontrolni mehanizam za iznos resursa koliko transakcija može koristiti. Otvoreni računalni model zahtijeva mjerenje kako bi se izbjegli napadi s uskraćivanjem resursa ili transakcije koje nenamjerno troše resurse. Gas je izdvojen od ethera kako bi se zaštitio sustav od nestabilnosti koje mogu nastati zbog nagle promjene vrijednosti ethera. Njegova je svrha također da se kontroliraju troškovi resursa (računalna snaga, memorija i pohrana podataka) koje se plaćaju gasom. Kod transakcija postoji polje pa nazivnom *gasPrice* i u njemu inicijator transakcije postavlja cijenu koju je on spreman platiti za gas. Cijena se transakcije mjeri u wei po jedinici gasa. Ether je podijeljen na manje jedinice, a najmanja jedinica je wei. Jedan ether je jednako 1 trilijun (10^{18}) wei. Novčanici mogu prilagoditi cijenu gasa kako bi ostvarili bržu potvrdu transakcija dok će transakcije koje nose nižu cijenu gasa rezultirati njihovim sporijim potvrđivanjem. Transakcije i koje su besplatne, tj. cijena gasa je postavlja na nula, bit će potvrđene jer ih ništa ne sprečava, no to je više izuzetak nego pravilo. Sljedeće polje po važnosti je *gasLimit* i ono ima funkciju da začetnik

transakcije postavi gornju granicu gasa koju je spreman kupiti kako bi mogao završiti transakciju [21].

4.2.3. ETHEREUM VIRTUALNI STROJ

Ethereum virtualni stroj (engl. EVM - *Ethereum virtual machina*) (Slika 7) računski je stroj koji je dio Ethereuma i zadužen je za dodjeljivanje i izvršavanje pametnih ugovora. EVM se ne koristi u slučaju kada je potreban prijenos vrijednosti od jednog EOA do drugoga. Rad EVM-a u sklopu Ethereum blockchaina na višoj razini može se zamisliti kao globalno decentralizirano računalo koje sadrži milijune objekata za izvršavanje gdje svaki objekt posjeduje vlastito mjesto pohrane. EVM se može smatrati kao zamjena za *Turing complete* stroj stanja zato što je izvršavanje procesa ograničeno na neki konačan broj koji temelji na dostupnom gasu koji se isporučuje za izvršavanje pametnog ugovora. Ovakav rad sprečava zastoja Ethereum platforme koja radi neprestano [21].



SLIKA 7. ARHITEKTURA I IZVRŠNI SLIJED EVM-A [21]

Arhitektura EVM je slojevita zbog čega se memorijske vrijednosti pohranjuju u slojevima. Podržava dužinu riječi do 256 bita i ima nekoliko adresabilnih komponenti kao što je nepromjenjiva ispisna memorija (engl. ROM – *Read Only Memory*) s bajt kodom za izvršavanje pametnih ugovora, promjenjiva memorija u kojoj je svaka lokacija inicijalizirana s nulom i trajnu pohranu koja je dio Ethereum stanja koja je inicijalizirana s nulom [21].

4.2.4. PAMETNI UGOVORI

O pametni ugovorima prvi je počeo raspravljati Nick Szabo 1997. godine u članku *Formalizing and Securing Relationships on Public Networks*. Prošlo je 20 godina prije nego li se otkrio njihov potencijal i prednosti koje bi došle s njihovim korištenjem. Prvu je primjenu imalo izumom Bitcoina i razvojem blockchain tehnologije. Szabo je u članku definirao pametan ugovor kao: „*...elektronički transakcijski protokol koji izvršava uvjete ugovora. Opći cilj je zadovoljenje uvjete ugovora, otkloniti odstupanja nastala slučajnim ili malicioznim događajem i smanjiti potrebu za pouzdanim posrednicima. Ekonomski ciljevi su smanjenje gubitaka koji nastaju zbog prevara, smanjenje troškova koji nastaju provođenjem i posredovanjem i ostali transakcijski troškovi* ". Pametan ugovor je računali program koji je napisan pomoću jezika koji može razumjeti računalo ili predviđeni stroj. S poslovne strane obuhvaća dogovor između dvije stranke. Jedna od glavnih ideja pametnih ugovora je da se automatski izvršavaju kada su zadovoljeni određeni uvjeti. Svi ugovoreni uvjeti izvršavaju se kako je definirano i očekivano čak u prisustvo protivljenja što znači da su pametni ugovori provedivi. Pametni ugovori ne oslanjaju se na tradicionalne metode provedbe nego rade na principu da je računalni kod zakon što podrazumijeva da nema potrebe za arbitrom ili trećom stranom koja bi kontrolirala ili utjecala na provedbu pametnog ugovora. Zato su pametni ugovori samonametnuti za razliku od legalno nametnutih. Moraju biti programirani tako da su otporni na greške, a izvršavanje mora biti u razumnu vremenu. U izvođenju na kraju uvijek daju isti izlaz i zbog takvog ponašanja poželjni su na blockchain platformama koje koriste mehanizme konsenzusa. Kako bi se ugovor smatrao pametnim, mora imati sljedeće četiri karakteristike: automatski izvršiv, provediv, semantički razumljiv (razumljiv čovjeku i računalu), siguran i nezaustavljiv. S time da su automatsko izvršenje i provedivost minimumi zahtjevi koji moraju biti zadovoljeni [1].

5. PAMETNI UGOVORI NA ETHEREUM PLATFORMI

U ovo poglavlju prikazat će se nužni alati za kreiranje, postavljanje i puštanje u rada pametnih ugovora.

5.1. PROGRAMSKI JEZICI ZA PISANJE PAMETNIH UGOVORA

EVM izvršava specijalni računalni kod pod nazivom *EVM bytecode* što je analogno x86_64 koje izvršava središnja procesorska jedinica. EVM bytecode je nezgrapan i jako težak za razumijevanje onima koji žele pomoću njega programirati, ali oni koji se smatraju dovoljno vještim mogu pomoću njega programirati pametne ugovore. Većina se Ethereum programera koristi višim programskim jezikom za pisanje programa dok ih kompajler prevodi u *bytecode*. Bilo koji viši programski jezik može se prilagoditi za pisanje pametnih ugovora, ali prilagođavanje programskog jezika da bude sukladan s EVM bytecode zahtijevan je posao te može doći do nedoumica. Zbog toga je došlo do pojave specijaliziranih programskih jezika za pisanje pametnih ugovora. Ethereum podržava nekoliko takvih jezika koji također podržavaju EVM bytecode. Općenito programski se jezici dijele na dvije paradigm, tj. na deklarativnu i imperativnu, a još poznata kao funkcionalna i proceduralna. U deklarativnom programiranju programi se pišu na način da se izražava logika programa, ali ne i njezina kontrola tijeka. Deklarativno se programiranje koristi za kreiranje programa gdje nema neželjenih pojava što podrazumijeva da nema promjene stanja izvan funkcije. Primjeri deklarativnog programskog jezika su SQL i Haskell. S imperativnim programiranjem programer piše skup procedura koje sadrže logiku i kontrolu tijeka za program. Primjeri imperativnog programskog jezika su Java i C++. Postoje i hibridni programski jezici što podrazumijeva da oni potiču deklarativno programiranje, ali se mogu koristiti za izražavanje imperativne programske paradigme. Predstavnici hibridnih programskih jezika su Python, JavaScript i Lisp. Imperativni programski jezik može se koristiti za pisanje programa prema deklarativnoj paradigmi, ali to može rezultirati neelegantnim kodom. Nasuprot tome, koristeći se izričito deklarativnim programskim jezikom, ne može se pisati program prema imperativnoj paradigmi. Programeri češće koriste imperativno programiranje, ali zna biti teže za pisanje programa koji će se izvršiti kako se očekuje od njih. Programi napisani imperativnim jezikom mogu

promijeniti stanja drugim programima što ostavlja puno prostora za pogreške. Za razliku od njega deklarativno programiranje omogućava lakše shvaćanje kako će se program ponašati s obzirom na to da nema neželjene događaje i svaki se izolirani dio programa može razumjeti. Pametni su ugovori osjetljivi na greške jer greške koštaju novac. Zato je bitno napisati pametne ugovore bez greške. Deklarativni programski jezik ima veću ulogu kod pametnih ugovora nego što ima kod programa opće namjene. No, najpopularniji programski jezik za pisanje pametnih ugovora je imperativni. Popis viših programskih jezika koji su podržani za pametne ugovore:

- *LLL* – prvi viši programski jezik za Ethereum pametne ugovore, funkcionalni programski jezik sa sintaksom sličnom kakvu ima Lisp
- *Serpent* – proceduralni programski jezik sa sličnom sintaksom koju koristi Python, može se koristiti za pisanje funkcionalnog koda, no mogući su neželjeni događaji
- *Solidity* – proceduralni programski jezik sa sličnom sintaksom koji imaju JavaScript, C++ i Java. Najpopularniji i najčešće korišten programski jezik za Ethereum pametne ugovore.
- *Vyper* – novo razvijen programski jezik koji je sličan Serpentu sa sintaksom koji ima Python. Razvijen je da funkcionalno bude što sličniji Pythonu nego Serpentu bez namjere da zamijeni Serpent.
- *Bamboo* – novo razvijen programski jezik pod utjecajem Erlanga s izričitim prijelazima stanja i bez petlji. Razvijen je s ciljem smanjenja nepoželjnih događaja i povećanja kontrole. Nov je programski jezik koji će tek postati široko prihvaćen.

Budući da je Solidity najpopularniji programski jezik, o njemu će se i najviše pisati, ali će se koristiti i istražiti ostale više programske jezike kako bi stegli razumijevanje različitih filozofija [21].

5.2. KREIRANJE PAMETNIH UGOVORA POMOĆU SOLIDITY

Solidity je kreirao dr. Gavin Wood isključivo za pisanje pametnih ugovora sa značajkom da izravno podržava izvršavanje u decentraliziranom okruženju koje predstavlja Ethereum kao svjetsko računalo. Na razvoju Solidity radili su Christian Reitiwessner, Alex Beregszaszi, Liana

Husikyan, i Yoichi Hirai te još nekoliko bivših glavnih Ethereum suradnika. GitHub je trenutačno je zadužen za razvoj i održavanje Solidityja [21].

GitHub je internetska platforma za razvoj softvera koji se koristi za praćenje, pohranu i suradnju na softver projektima. Omogućava programerima da učitaju vlastite datoteke s kodovima i kako bi surađivali s kolegama programerima na projektima otvorenog računalnog koda. Također, ima ulogu društvene mreže putem koje programeri mogu povezati, surađivati i predstavljati svoj rad [22].

Najveća vrijednost koju pruža Solidity je kompajler *solc* koji prevodi programe koji su napisani pomoću Solidity programskog jezika u EVM bytecode. Također, upravlja sa standardom za aplikacije s binarnim sučeljem za Ethereum pametne ugovore. Važno je istaknuti da svaka verzija Soliditya ima svoju specifičnu verziju kompajlera. Solidity se može preuzeti za Microsoft Windovs, Apple macOS i Linux operativne sustave. Za detaljnije upute kako preuzeti i instalirati Solidity za željeni operativni sustav posjetiti idući poveznicu. Za programiranje unutar Solidity može se koristiti bilo koji uređivač teksta i *solc* na naredbenoj liniji. Programi koji su napisani u Solidityju sačinjeni su od tekstualnih datoteka. Prilikom spremanje izvornog koda programa mora se spremiti pod ekstenzijom *.sol* kako bi Solidityjev kompajler mogao prepoznati datoteku kao Solidity program [21].

Prije nego li se pametan ugovor može učitati na Ethereum blockchain, on se mora prevesti u binarni heksadecimalni niz. Aplikacijsko binarno sučelje (engl. ABI - *application binary interface*) je sučelje između dva programska modula i to najčešće između operativnog sustava i korisničkih programa. Uloga ABI-a je da definira kako su funkcije i strukture podataka pridružene unutar strojnoga koda, pri tome ne treba ga zamijeniti s aplikacijskim programskim sučeljem. Primarna uloga ABI-a je da kodira i dekodira podatke unutar i izvan strojnoga koda. U Ethereum blockchainu ABI se koristi za kodiranje poziva na ugovore za EVM i kako bi iščitavao podatke iz transakcija. Svrha ABI-a je da definira koje se funkcije mogu pozvati u ugovoru, opiše kako će svaka funkcija prihvatiti argumente i vraćati rezultate na prihvaćane argumente [21].

5.3 VIŠI PROGRAMSKI JEZIK VYPER

Vyper je eksperimentalno ugovorno orijentiran programski jezik za EVM koji ima za cilj pružiti poboljšanu kontrolu kako bi omogućio programerima da kreiraju pametniji kôd. Jedan od principa Vypera je da onemogući programerima kako napisati kôd koji bi bio zavaravajući. Razlog pojave Vyper programskog jezika je pojava velikog broja Ethereum pametnih ugovora koji u sebi sadrže ranjivosti. Tri kategorije najčešće detektiranih ranjivosti su:

- Suicidalni ugovori – pametni ugovori koji su uništeni od strane proizvoljne adrese
- Pohlepni ugovori – pametni ugovori koji mogu postići stanje u kojem ne mogu osloboditi ether
- Rastrošni ugovori – pametni ugovori koji su kreirani kako bi oslobodili ether proizvoljnim adresama.

Ranjivosti koje sadrže pametni ugovori su sastavljene u računalnom kodu. Teško je utvrditi jesu li ranjivosti u računalnom kodu nastale namjerno ili nenamjerno. Zbog takvih ranjivosti dolazi do gubitaka sredstava kod Ethereum korisnika što nije prihvatljivo. Zato je Vyper dizajniran kako bi olakšao pisanje sigurnog računalnog koda ili jednako tako otežao njegovo pisanje da ispadne ranjiv ili zavaravajući. Ako će se uspoređivati sa Solidityjem, Vyper pokušava otežati pisanje nepouzdanog računalnog koda tako što izostavlja neke značajke Solidityja. Oni koji se žele služiti s programskim jezikom Vyper moraju biti upoznati sa značajke koje nema i zašto [21].

U Solidityju se može napisati funkcija koristeći modifikator, modifikatori se inače koriste kako bi se kreirali uvjeti za mnoge funkcije unutar ugovora. Modifikatora u Vyperu nema zato što njihovim korištenjem može doći do poziva funkcije koja može dovesti do promjene stanja ugovora. Vyper preporuča ako se primjenjuje tvrdnja pomoću modifikatora, onda treba koristiti provjere unutar reda i tvrdnje kao dio funkcije. Ako se prepravlja stanje pametnog ugovora, opet treba napraviti te promjene kao dio funkcije. Time se poboljšava kontrola i čitljivost za osobu koja bude htjela vidjeti što se postiže funkcijom. Klasa za nasljeđivanje dopušta programerima da koriste računalni kod koji je već prethodno napisan što znači da mogu dohvatiti postojeće funkcije, svojstva i ponašanja iz baze softvera. Iako Solidity podržava višestruko nasljeđivanje te poliformizam koji se smatraju ključnim značajkama objektno-orijentiranog programiranja dok ih Vyper ne podržava. Vyper također ne podržava sastavljanje u redu zato što smatra da gubitak

čitljivosti veliki u odnosu na koristi od dobitka veće računalne snage. Sastavljanje u redu inače omogućava programerima niski pristup EVM-u što omogućava programima napisanim pomoću Solidity da izvršavaju operacije izravno s EVM-im instrukcijama. Sljedeću funkciju koju Vyper ne podržava je preopterećenje funkcije. Preopterećenje funkcije inače služi programerima da pišu višestruke funkcije pod istim imenom, upotreba određene funkcije za danu situaciju ovisi o vrsti unesenih argumenata. Pisanje višestrukih funkcija je razlog zašto ih Vyper ne podržava jer može doći do zabune. Određivanje tipa varijable nije podržano od Vypera. Određivanje tipa varijable može biti implicitno i eksplicitno, implicitno nije podržano zbog toga što može doći do gubitka informacija dok eksplicitno može izazvati nepredviđeno ponašanje. Preduvjete, postuvjete i promjene stanja Vyper rješava eksplicitno. Omogućava maksimalnu čitkost i sigurnost pritom stvarajući redundantan računalni kod. Prilikom pisanja pametnog ugovora s Vyperom, programer mora obratiti pažnju na stanja u kojem se nalaze varijable stanja Ethereuma, što će biti pod utjecajem, a što neće, podudaraju li se ishodi za namjerama ugovora i razmotriti sve trajne ishode, posljedice i scenarije te interakcije s ostalim ugovorima [21].

Vyper podržava logiku dekoratera. Dekorateri se koriste za kako početak pisanja funkcije i postoje četiri vrste:

- *@private* - čini funkciju nedostupnom izvan ugovora
- *@public* - omogućava da funkcija bude vidljiva i javno izvršiva
- *@constant* – zabranjuje funkciji da mijenja varijable stanja
- *@payble* – dopušta prijenos vrijednosti

Svaki ugovor koji je napisan Vyperom sastoji se od jedne Vyper datoteke. Vyper zahtijeva da su sve ugovorne funkcije i deklaracije varijabli napisane u određenom nizu dok takvog uvjeta nema u Solidityju. Postoje uređivači računalnog koda i kompajleri samo za Vyper koji omogućavaju pisanje i kompiliranje pametnih ugovora u bytecode, ABI i LLL u internetskom pregledniku. internetskom kompajler ima više primjera napisanih ugovora. Pametni ugovori u Vyperu mogu se kompajlati pomoću komandne linije. Pogreške nastale preplavljivanjem nepoželjne su kada radi s pravim vrijednostima. Solidity programeri imaju pristup bibliotekama kao što je *SafeMath OSS*. Kada sigurnosne značajke nisu forsirane od programskog jezika, programeri mogu pisati nesigurne računalne kodove koji će se uspješno kompilirati zajedno sa svojim vrlinama i manama. Vyper ima ugrađenu zaštitu od preplavljivanja u dva pristupa. Prvi je osiguravanje istovjetne baze kao što je

SafeMath koja uključuje nužne izuzetke za slučaj aritmetičkog cijelog broja. Druga je upotreba spojnica kada se literalna konstanta učitava, vrijednost je proslijeđena funkciji ili se dodjeljuje varijabla. Spojnice su integrirane putem prilagođene funkcije u jeziku koji je slična LLL kompajleru i ne može se ukinuti. Operacije skladištenja su nužne komponente za većinu pametnih ugovora, a uključuje pohranu, čitanje i izmjena podataka. Pametni ugovori mogu zapisati podatke na dva mjesta:

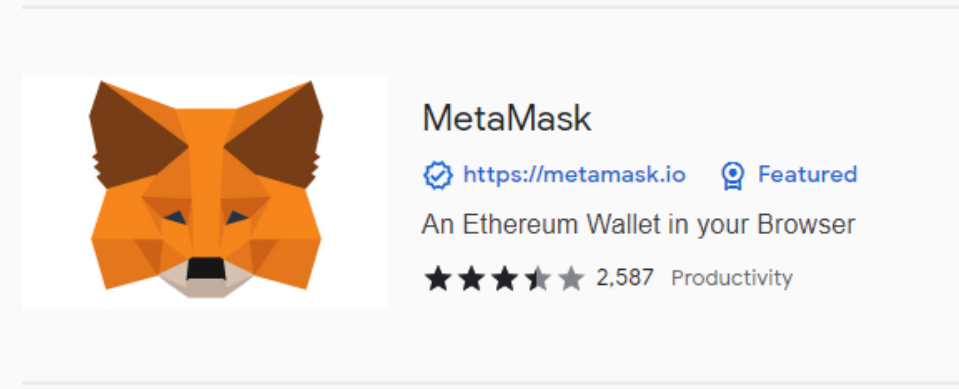
- Globalno stanje – varijabla stanja pametnog ugovora pohranjuje se u digitalno stablo koje je dio Ethereum globalnog stanja, pametni ugovori mogu se jedino pohraniti, čitati i mijenjati podatke samo za određenu adresu ugovora
- Zapisi – pametan ugovor može zapisivati na Ethereum podatkovni lanac putem zapisnika događaja. Na početku Vyper je imao svoju sintaksu zapisa _log_, ali je naknadno ažurirana kako bi bila u skladu s originalnom sintaksom koju koristi Solidity.

Iako pametni ugovori mogu zapisivati na Ethereum podatkovni lanac, oni nisu u mogućnosti čitati zapise na lancu o događajima koje su kreirali. Prednost takvog zapisivanja podataka je da zapisi mogu biti otkriveni i pročitani na javnom lancu od klijenata koji imaju ograničen pristup [21].

5.4 POSTAVLJANJE NOVČANIKA

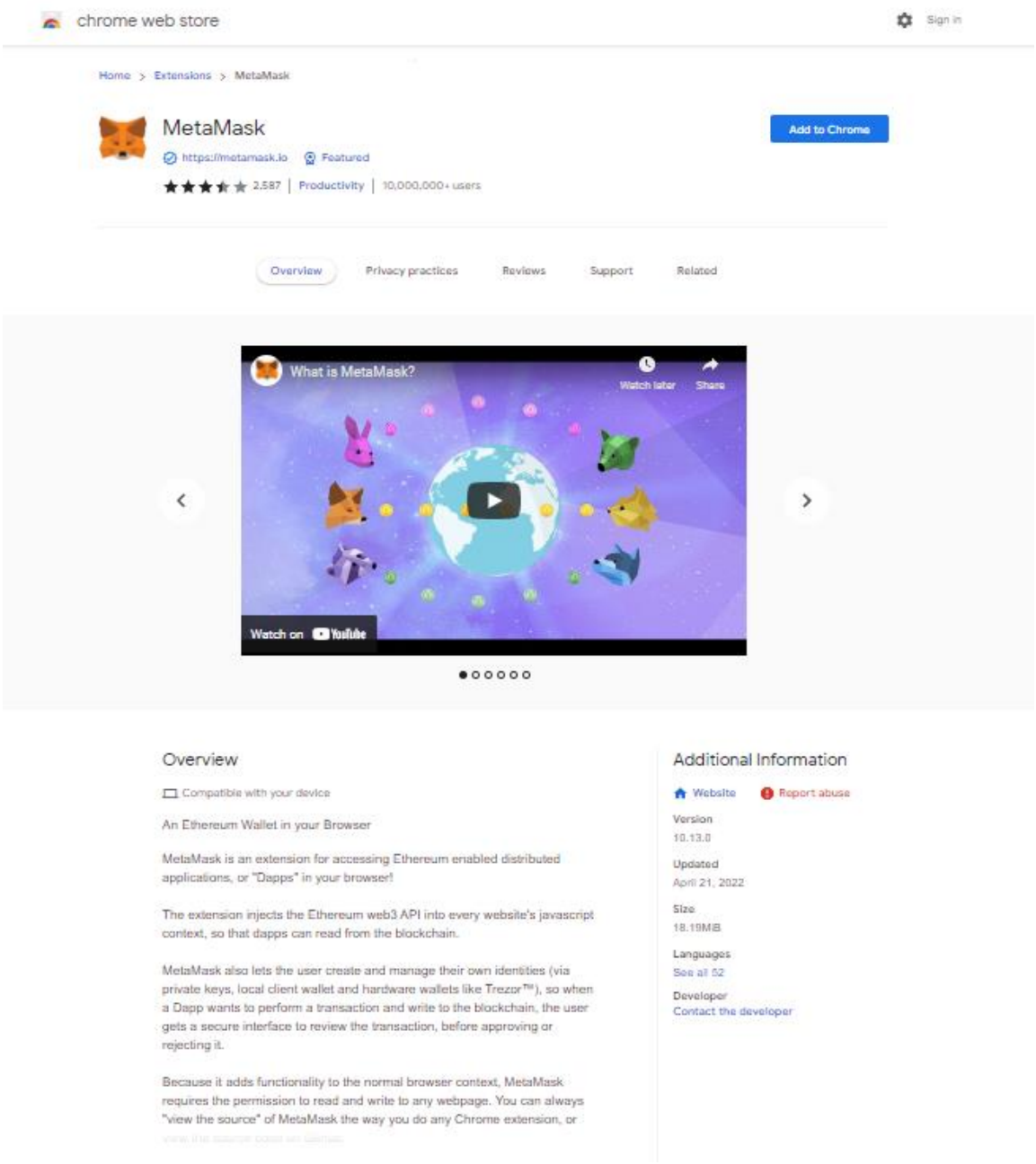
Prije nego li se može pametni ugovora pustiti u rad, potrebno je odabirati novčanik. Pojam novčanika je objašnjeno u Poglavlju 2.7.1, a na primjeru novčanika *MetaMask* objasnit će se postavljanje i puštanje u rad pametnog ugovora.

MetaMask je novčanik koji predstavlja proširenja preglednika koji radi unutar preglednika (Chrome, Firefox, Opera, Brave Browser) i pripada u kategoriju internetskih preglednika. Druge dvije verzije novčanika su mobilni i računalni program. Njegovo korištenje je jednostavno i praktično za izvođenje testiranja, može se priključiti na razne Ethereum čvorove i testirati razne blockchainove. Putem *chrome web store* ili hrvatske verzije *Chrome web trgovina* pod poveznicom "*Extensions - Chrome Web Store*" u tražilica će se upisati *MetaMask*. Orginalna poveznica MetaMask je prikazana na slici 8.



SLIKA 8. POVEZNICA ZA PROŠIRENJE INTERNET NOVČANIKA METAMASK U CHROME WEB STORE [23]

Odabirom te poveznice odvest će na početnu stranicu za MetaMask unutar Chrome web trgovine koja je na slici 9. Nakon preuzimanja novčanika trebaju se proći koraci za kreiranje novčanika i kreirati snažnu zaporku koja mora sadržavati minimalno osam znakova. Nakon što se postavi zaporka MetaMask će generirati *mnemonic backup* koji čini dvanaest slučajnih riječi na engleskom jeziku [21].



SLIKA 9. POČETNA STRANICA ZA METAMASK UNUTAR CHROME WEB STORE [24]

Tih dvanaest riječi mogu se koristi s bilo kojim odgovarajućim novčanikom kako bi povratili sredstva u slučaju da se nešto dogodi s MetaMask ili s računalom. Tih bi dvanaest riječi treba spremiti na dva papira koji će biti na različitim mjestima. Njihova je vrijednost jednaka novcu te ih treba tako tretirati i držati ih na sigurnim mjestima kojima nitko drugi nema pristup. Svatko tko bi došao do tih riječi imao bi pristup sredstvima koja su pohranjena na novčaniku. Svaki novi

kreiran novčanik bit će spojen na glavnu Ethereum mrežu, ali se može pridružiti i drugim javnim testnim ili privatnim mrežama. Najpopularnije testne, privatne mreža i njihova uloga:

- Testna mreža *Ropsten* – javna testna Ethereum mreža i blockchain, ETH na ovoj mreži nema vrijednost
- Testna mreža *Kovan* – javna testna Ethereum mreža i blockchain koja koristi konsenzusni protokol Aura s dokazom o ovlaštenju. ETH na ovoj mreži nema vrijednost i mreža je jedino podržana od strane *Parity*
- Testna mreža *Rinkeby* – javna testna Ethereum mreža i blockchain koja koristi konsenzusni protokol *Clique* s dokazom o ovlaštenju, ETH na ovoj mreži nema vrijednost
- *Localhost* 8545 - novčanik se povezuje na čvor koji radi na istom računalu kao i preglednik. Čvor može biti dio bilo kojeg javnog blockchaina (glavni ili testni) ili privatna testna mreža
- Prilagođeni *RPC* - omogućava MetaMasku da se poveže na bilo koji čvor koji je kompatibilan s *Geth Remote Procedure Call* (RPC) sučeljem. Čvor može biti dio bilo kojeg javnog ili privatnog blockchaina [21]
- Testna mreža *Morden* – javna testna Ethereum mreža i blockchain koji koristi konsenzusni mehanizam dokaz o radu za Ethereum Classic, a kasnije je zamijenjena s *Mordor* [25].

5.5. KOMPILIRANJE PAMETNOG UGOVORA

Napisani pametni ugovor obrađuje se Solidity kompajlerom kako bi se računalni kod koji je napisan pomoću Solidity prebacio u EVM bytecode za EVM koji će ga izvršiti na blockchanu. Solidity kompajler nalazi se unutar integriranog razvojnog okruženja (engl. IDE - *Integrated Development Environments*) [21].

Integrirano razvojno okruženje je softver za izradu aplikacija koje kombinira uobičajene alate za razvojne programere u jedno grafičko korisničko sučelje. IDE se sastoji od:

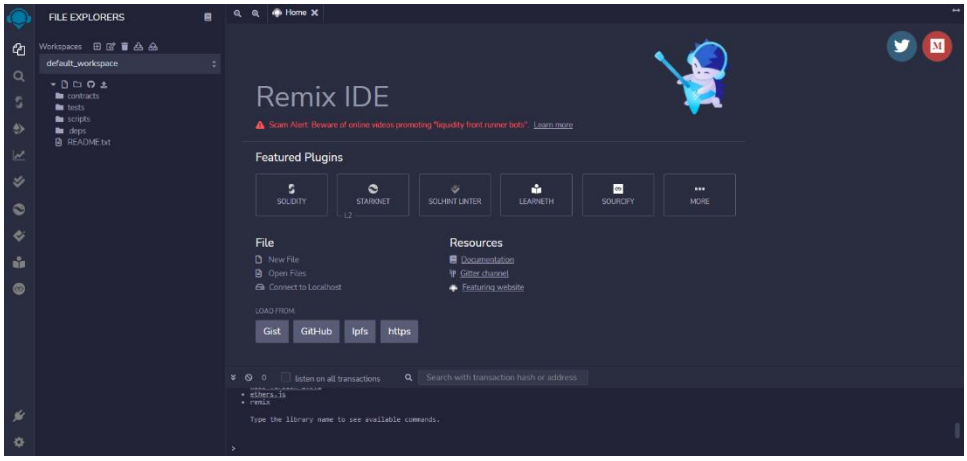
- Uređivač izvornog koda – tekstualni urednik koji pomaže kod pisanja softverskog koda uz pomoću značajki naglašavanja sintaksi s vizualnim znakovima, automatsko dovršavanje za specifične jezike i provjeravanje grešaka u kodu za vrijeme pisanja

- Automatizacija izgradnje – usluge automatiziranja repetitivnih zadataka u sklopu kreiranja lokalne izrade softvera koji će koristiti razvojni programeri za kompiliranje izvornog koda u binarni kod, pakiranje binarnog koda i izvođenje automatskih testova
- Ispravljanje pogrešaka - program za testiranje drugih programa koji grafički prikazuje mjesto greške u izvornom kodu.

IDE omogućava programerima da brzo programiraju nove aplikacije jer ne moraju ručno podešavati razne usluge. Većina značajki IDE-a ima za cilj uštedjeti vrijeme u inteligentnom dovršavanju koda i automatskom generiranju koda čime se izbacuje potreba za pisanjem cijelih nizova znakova. Ostale uobičaje IDE komponente imaju za cilj pomoći programerima da organiziraju tijek rada i rješavanje problema [26].

Remix je aplikacija otvorenog koda koja može funkcionirati kao Internet i *desktop* aplikacija. On se koristi u cijelom procesu kreiranja ugovora, a služi za učenje i predavanje o Ethereumu. Remix IDE je dio Remix Projekta koja je platforma za razvoj alata koja koristi arhitekturu s dodatkom. Obuhvaća pod projekte koji uključuju *Remix Plugin Engine, Remix Libs* i Remix-IDE. Remix IDE je snažan alat otvorenog koda koji pomaže pri pisanju ugovora pomoću Solidity izravno iz preglednika. Remix je napisan s JavaScriptom i može se koristiti putem preglednika, ali se može izvoditi i lokalno u *desktop* verziji [27].

Putem preglednika Google Chrome ili nekog drugog preglednika za instaliranje novčanika otvora se Remix IDE koji se nalazi na stranici https://remix.ethereum.org/ . Početna stranica Remix IDE je prikazana na slici 10 [21].



SLIKA 10. POČETNA STRANICA REMIX IDE UNUTAR PREGLEDNIKA [28]

Klikom na ikonu Create New File koja je označena na slici 11. kreirat će se novi ugovor kojem se mora dati novo ime s nastavkom *.sol*, npr. *SakupljacNaknada.sol*.

SLIKA 11. IKONA (OZNAČENA CRVENIM KVADRATOM) ZA KREIRANJE NOVE DATOTEKE [28]

Zatim će se otvoriti nova kartica s poljem u kojem možemo pisati ili kopirati gotov pametan ugovor koji je prethodno napisan. Ako je ugovor uspješno ili neuspješno kompiliran, Remix IDE će o tome dati povratnu informaciju [21].

5.6. POSTAVLJANJE PAMETNOG UGOVORA NA BLOCKCHAIN

Napisan ugovor koji je pretvoren u bytecode mora se postaviti na Ethereum blockchain kako bi izvršavao funkciju koja mu je zadana. Prvo se mora odabrati mreža na koju će ga se postaviti kako bi se registrirao ugovor na blockchain, mora se prvo kreirati posebna transakcija čija će adresa biti 0x0000000000000000000000000000000000000000 koja je poznata kao nulta adresa. Nulta adresa je posebna adresa koja javlja Ethereum blockchainu da se želi registrirati ugovor. Ako se koristi Remix IDE, on će to odraditi taj dio za korisnika i poslat će transakciju prema novčaniku, tj. MetaMask. Pod ikonom *Deploy & run transactions* koja se nalazi na alatnoj traci na lijevoj strani te pod izbornikom *ENVIRONMENT* odabrati opciju *Injected Web3*. Ovom se radnjom povezuje Remix IDE s MetaMask novčanikom. Potvrdom na ikonu *Deploy* Remix će kreirati transakciju i MetaMask će tražiti njezino odobrenje. U MetaMasku će se otvoriti potvrda transakcije koja će prikazati trošak postavljanja ugovora na blockchain, potvrdom transakcije završava postupak postavljanja ugovora na Ethereum blockchain. Svaki će novi ugovor koji se kreira imati vlastitu adresu [21].

6. VRSTE PAMETNIH UGOVORA

6.1. FORME PAMETNIH UGOVORA

Pametni ugovori mogu poprimiti tri forme s obzirom na razinu automatizacije. Iako se sve tri forme ugovora mogu definirati kao pametni ugovori, oni će se razlikovati u obvezama koje nose sa sobom. Prva forma ugovora je ugovor napisan ljudskim jezikom s automatskom izvedbom pomoću računalnog koda. U ugovoru koji je napisan ljudskim jezikom neke ili sve ugovorne obveze se automatski izvršavaju pomoću računalnog koda. Sam računalni kod ne definira nikakve ugovorne obveze, ali je alat koji je zadužen od jedne ili obje strane za izvršavanje ugovornih obveza. Ovakav tip pametnog ugovora može se prozvati kao *vanjski* ugovor zbog toga što računalni kod izlazi izvan okvira djelokruga stranaka koje su vezane dogovorom. Ovakvi su ugovori najčešća forma pametnih ugovora u sadašnjem vremenu. Ugovori s ovakvom formom ne otvaraju nova pravna pitanja u smislu interpretacije i formiranje ugovora [29].

Druga forma pametnih ugovora su hibridni ugovori. Hibridni legalni pametni ugovori je ugovor u kojem su neke ugovorne obveze definirane u ljudskom jeziku, a druge su definirane računalnim kodom. Sve ili neke se ugovorne obveze automatski izvršavaju putem koda. Gledano s jedne strane uvjeti hibridnih ugovora mogu se primarno pisati pomoću računalnog koda i s nekoliko izraza na ljudskom jezikom za definiranje mjerodavnog prava i nadležnosti. S druge strane, uvjeti hibridnog ugovora mogu biti primarno napisani ljudskim jezikom s nekoliko uvjeta napisanih pomoću računalnog koda. Također je moguće napisati uvjete ugovora s oba jezika. Uvjeti napisani ljudskim jezikom mogu se uključiti u dogovor napisan s ljudskim jezikom ili u tekst s ljudskim jezikom koji je uključen u računalni kod [29].

Treća forma ugovora su ugovori koji su isključivo zapisani u računalnom kodu. U ovakvoj formi ugovora svi su ugovorni uvjeti definirani i automatsko izvođeni računalnim kodom. Verzija ugovora koja se dogovora s ljudskim jezikom ne postoji. U ovoj formi pametnog legalnog ugovora predstavlja najviše izazova iz perspektive ugovornog prava. Problem nastaje kod utvrđivanja je li

sklopljen legalan ugovor i kada je sklopljen te kako se može takav ugovor tumačiti. Pametni legalni ugovori napisani pomoću računalnog koda vjerojatno će biti rijetki u praksi. Budući da su tradicionalni ugovori suviše ekspresivni, teško ih je svesti isključivo na računalni kod. Uvođenje ovakvih ugovora otvara nova pravna pitanja koja se moraju definirati prilikom sklapanja ugovora i pravnih lijekova. Njihova bi se proširenost ubuduće mogla povećati jer temeljne tehnologije postaju sve naprednije [29].

6.2. TIPOVI PAMETNIH UGOVORA

Prva primarna kategorija su legalni pametni ugovori. Legalne pametne ugovore definiramo kao legalno obvezujuće ugovore u kojem su neke ili sve ugovorne obveze definirane i automatske, izvedene pomoću računalnog programa. Legalni pametni ugovori prate uvjetovanu logiku s preciznim i objektivnim ulazom gdje ako dođe do događaja *A*, izvrši se radni *B*. Njihovim se korištenjem očekuje povećanje efikasnosti u određenim poslovanjima i smanjuje se povjerenje između ugovornih strana koje je prebačeno u računalni kod. Može se reći da su dvije glavne odlike legalnih pametnih ugovora: računalni program izvršava neke ili sve ugovorne obveze i ugovori su legalno provedivi [29].

Druga primarna kategorija su decentralizirane autonomne organizacije (engl. DAO - Decentralized autonomous organizations) kojima je okosnica pametan ugovor. Ugovor definira pravila organizacije i čuva riznicu grupe. Nitko ne može mijenjati pravila, mijenjati se mogu jedino putem glasovanja kada ugovor postane aktivan na Ethereum blockchainu. Svatko će biti bezuspješan tko pokuša nešto napraviti što nije pokriveno pravilima i logikom koda. Zbog toga što je i riznica definirana pametnim ugovorom nitko ne može trošiti sredstva bez odobrenja grupe. DAO-om upravlja grupa, a ne središnja vlast. Sredstva se troše jedino ako se odobri sustavom glasovanja. Unutar DAO-a postoji tri vrste članstava kojim se odlučuje funkcioniranje glasovanja i ključni dijelovi DAO-a:

- Članstvo temeljeno na žetonima - ovisi o tome koji se žetoni koriste, trgovati se njima može u potpunosti bez odobrenja. Žetonima za upravljanje može se trgovati bez odobrenja na

decentraliziranoj mjenjačnici. Ostali se žetoni moraju zaraditi pružanjem likvidnosti i nekim oblikom dokazom o radu. Posjedovanjem žetona ostvaruje se pravo na glasanje.

- Članstvo temeljeno na udjelu – ovakvo članstvo je s dopuštenjem, ali i dalje prilično otvoreno. Svaki potencijalni član može podnijeti zahtjev za priključenjem DAO-u, obično nudeći nekakav oblik vrijednosti koja može biti u formi žetona ili rada. Udjel predstavlja izravno pravo na glasovanje i vlasništvo. Članovi mogu izaći u bilo kojem trenutku sa svojim proporcionalnim udjelom u riznici.
- Članstvo temeljeno na reputaciji – reputacija predstavlja dokaz o učešću i dodjeljuje pravo na glasovanje u DAO-u. U odnosu na prethodna dva članstva, u DAO-u temeljenom na reputaciji nema prijenosa vlasništva na suradnike. Reputacija se ne može kupiti, prenijeti ili izabrati. DAO članovi moraju steći reputaciju sudjelovanjem. Bez odobrenja se može glasovati putem glavnog lanca i potencijalni članovi mogu slobodno priložiti zahtjev za priključenjem DAO-u te zahtijevati dobivanje reputacije i žetone kao nagradu u zamjenu za njihov doprinos [30].

I zadnja treća primarna kategorija pametnih ugovora su ugovori s logikom aplikacije. Ugovori s logikom aplikacije sadrže računalni kod za aplikacije koji je usklađen s ostalim blockchain ugovorima. Oni mogu omogućiti komunikaciju između različitih uređaja primjerice integriranjem Internet stvari s blockchain tehnologijom. Ovakvi su ugovori ključni dio multifunkcionalnih pametnih ugovora i većinom rade pod programom za upravljanje [31].

7. PRIHVAĆANJE PAMETNIH UGOVORA U PRAKSI

U ovom će se poglavlju analizirati slučajevi upotrebe i primjena pametnih ugovora u svakodnevici. Budući da su pametni ugovori računalni program, oni se mogu programirati prema željama programera. Pametni se ugovori programiraju na način da se postave uvjeti koje je potrebno ispuniti kako bi se izvršili pametni ugovori koji su pogodni za primjenu u operacijama koje se mogu izvršiti logikom uvjetovanja.

7.1. PAMETNI UGOVORI KOD INTERNET STVARI

Internet stvari (engl. IoT – *Internet of Things*) vrlo je obećavajuća tehnologija koja može podržati razne primjene kao što je upravljanje opskrbnim lancima, sustavima kontrole inventara, maloprodaju, kontrolom pristupa, knjižnicama i e-zadravstvo. Glavna ideja IoT-a je integriranje *pametnih* objekata s Internetom i pružiti razne usluge. Pomoću IoT-a implicitno se predlagalo da se automatiziraju poslovne transakcije. S integracijom pametnih ugovora Internet bi stvari dobile novi zamah i ostvarile bi neostvarene potencijale. Primjerice u industrijskoj proizvodnji većina proizvođača održava svoj ekosistem IoT-a na centralizirani način. Ugrađeni softver za razne IoT uređaje može se zadobiti ručno kod središnjeg servera tako da ne čekaju u redu [32].

Problemi koji mogu nastati u ovakvom načinu rada odnose se na mogućnosti neispravnosti središnjeg servera da ne može obavljati svoju funkciju ispravno što bi izravno utjecalo na uređaje da dobiju nužni ugrađeni softver kako bi ispravno funkcionirali. Isto tako prilikom hakerskog napada, kada bi napadač zadobio kontrolu nad središnjim serverom, mogao bi ga koristiti za širenje zlonamjernog koda na IoT uređaje.

Kako bi poboljšali proces održavanja, proizvođači mogu pohraniti ažuriranja za ugrađeni softver na pametne ugovore koji bi se distribuirali blockchain mrežom čime bi se uštedilo na resursu i vremenu. E-poslovanje IoT-a može se unaprijediti koristeći pametne ugovore. Mogu se primijeniti kod plaćanja koja su inače riješena preko trećih strana koje izvršavaju naplatu. Takav centralizirani način naplate je skup i ne može u potpunosti iskoristiti prednost IoT-a. Postoji prijedlog da se u DAO-u automatiziraju transakcije kod kojih nema tradicionalnih uloga kao što

su državne vlasti ili tvrtke koja se bave naplatom. Kad bi se primijenili pametni ugovori, DAO bi bio u stanju raditi automatski bez uplitanja ljudske strane. Pametni bi ugovori također ubrzali standardne opskrbne lance. Integracija pametnih ugovora s lancima opskrbe može automatizirati ugovorna prava i obveze za vrijeme naplate i isporuke dobara dok sve stranke imaju u proces to povjerenje [32].

Energetski bi sektor imao korist od integracije pametnih ugovora i IoT-a. Putem njih bi se osiguralo da energija koja se generirana i distribuirana bude u skladu s dogovorenim uvjetima. Sektor automobilizma i transporta, točnije punjenje električnih automobila imalo bi korist od pametnih ugovora. Budući da su vozila većinom opremljena s IoT senzorima, pametni ugovori bili bi učinkovit način za izvršavanje poslovnih procesa za punjenje vozila čime bi korisnici na raspolaganju imali opciju sigurnog plaćanja. Putem pametnih ugovora korisnici bi se pretplatili distributeru energije nakon što bi prihvatili njihove odredbe i uvjete [33].

7.2. PAMETNI UGOVORI U DISTRIBUIRANIM SIGURNOSNIM SUSTAVIMA

Korištenje pametnih ugovora može poboljšati sigurnost distribuiranih sustava. Napadi uskraćivanjem usluga glavne su prijetnje sigurnosti u računalnim mrežama. Napad je zamišljen tako da napadač/i generiraju velike količine mrežnog prometa čime se preopterećuje sustav zbog čega dolazi do postupnih prekida ili isključenja internetskih usluga. Pojavio se prijedlog mehanizma koji bi ublažilo takve napade. Shema je rješenja zamišljena da se obračuna s takvim napadom na decentralizirani način. Jednom kada bi server bio po napadom, Internet protokol adresa napadača bi bila pohranjena na pametan ugovor. Ostali bi čvorovi putem pametnog ugovora bili obaviješteni o adresama s kojih dolaze napadi nakon čega bi se odmah primijenile dodatne zaštitne mjere [32].

Računalstvo u oblaku je tehnologija koja pruža pristup zajedničkom skupu resursa računalne snage i pohrane. Korisnici mogu kupiti usluge od pružatelja usluga u oblaku. Utvrđivanje povjerljivosti pružatelja je izazov zato što se oni znaju međusobno dogovarati kako bi ostvarili veći profit. Jedan prijedlog koji je nastao za taj problem temelji se na teoriji igara i pametnih ugovora. Ideja je zamišljena tako da klijent zatraži od dva pružatelja usluga u oblaku da izvrše isti zadatak.

U međuvremenu se pametni ugovori koriste kako bi se stimulirala napetost, prevara i nepovjerenje između pružatelja. Iz toga zadatka korisnik može zaključiti koji se pružatelji ne dogovaraju i ne varaju. Brokeri se inače koriste u računalstvu u oblaku. Brokeri provjeravaju korisnikove zahtjeve kako bi bili u skladu s uslugama pružatelja. Korisnici i pružatelji moraju imati povjerenje u brokera. Ako bi broker bio kompromitiran ili uhićen, onda obje strane ne bi imale povjerenje jedna u drugu. Prijedlog rješenja koje se nudi za ovaj problem je korištenje pametnih ugovora kako bi se zaobišla upotreba brokera. Ideja je da se koriste distribuirani ugovori o razini usluge za pružatelja usluga u oblaku. Također je predložena djelotvorna funkcija koja procjenjuje dogovore prema željama stranaka kako bi se riješio problem razilaženja [32].

7.3. PAMETNI UGOVORI U FINANCIJSKOM SEKTORU

Korištenje pametnih ugovora u financijskom sektoru može potencijalno smanjiti financijske rizike, smanjiti administraciju i cijene usluga te poboljšati efikasnost financijskih usluga. Ovo su primjeri u kojima bi korištenje pametnih ugovora poboljšalo tradicionalne financijske usluge [32]:

- Investicijske banke i tržište kapitala - tradicionalno tržište kapitala pati od sporih ciklusa zaključenja. Pametni ugovori mogu značajno smanjiti razdoblje zaključenja na 20 dana pa sve do 6 dana što bi povećalo atraktivnost kod kupaca. Rezultat toga bio bi povećanje potražnje pa shodno time i povećanje prihoda
- Maloprodajno i komercijalno bankarstvo - industrija hipotekarnih kredita imala bi korist kada bi usvojila pametne ugovore. Tradicionalne su hipoteke inače komplicirane u stvaranju, procesu financiranja i održavanju što posljedično stvara dodatne troškove i zastoje. Pametni bi ugovori smanjili dodatne troškove i zastoje automatizacijom procesa za hipoteke s digitalizacijom pravnih dokumenata na blockchain.
- Osiguranja - primjena pametnih ugovora u industriji osiguranja smanjila bi troškove obrade i troškove podnošenja zahtjeva. Pametni bi ugovori automatizirali potraživanja za podmirenje obveza dijeleći pravne dokumente putem distribuirane glavne knjige čime bi se povećala efikasnost, smanjilo vrijeme obrade zahtjeva i smanjili troškovi usluga [32].

7.4. PAMETNI UGOVORI KOD PODRIJETLA PODATKA

Pametni ugovori mogu se koristiti kako bi se osigurala kvaliteta informacija u znanstvenim istraživanjima i u javnom zdravstvu. S obzirom na to da se u današnjem vremenu stvara velika količina netočnih informacija, a lažiranje postaje sve češći problem, nepostojećim se podacima može u krivi smjer navesti aktivno istraživanje ili ugroziti oporavak pacijenta. Posljedica toga je narušavanje povjerenja u znanost i smanjiti povjerenje javnosti u institucije. Kako bi se ublažili takvi problem, predložilo se istraživanje o podrijetla podataka. Ideja o podrijetlu podatka sastoji se od pohrane informacija o metapodacima koje predstavljaju izvornost podataka, izvršavanja i transformacije. Većina alata za evidentiranje prijave kao što su Progger i modul o vjerodostojnosti platforme, pohranjuju podatke o aktivnostima skupa s osjetljivim privatnim informacijama. Pojavio se prijedlog sustava o podrijetlu podatka koji koristi pametne ugovore i blockchain. U tom bi sustavu istraživači mogli dostaviti kriptirane podatke u sustav. Kada bi došlo do promjene podataka, pametni ugovori bi bili pozvani da nađu gdje je došlo do transformacije podataka čime bi se zlonamjerne zabilježile. Zaštita intelektualnog vlasništva digitalnog medija imali bi koristi od primjene pametnih ugovora. Primjerice svaki digitalni proizvod štitio bi se putem ugrađenog jedinstvenog digitalnog vodenog žiga (adresa novčanika kupca i identifikacijski broj proizvoda). Kada bi došlo do kršenja prava, službenik za provedbu zakona može ući u trag ilegalnom dokumentu pomoću originalnog te pomoću metode ekstrakcije digitalnog vodenog žiga usporediti digitalnu adresu novčanika i novčanika kupca. Rezultat toga bi bilo lako prepoznavanje povredu prava vlasništva, a cijeli proces može proći preko pametnih ugovora i blockchaina [32].

7.5. PAMETNI UGOVORI U EKONOMIJI DIJELJENJA

Ekonomija dijeljenja donosi mnoge povlastice kao što je smanjenje troškova za kupce posuđivanjem i recikliranjem artikala, poboljšanjem iskorištenja resursa, unapređenjem kvalitete usluge i smanjenjem negativnih utjecaja na okoliš. Međutim, većina platformi s ekonomijom dijeljenja pate od visokih troškova transakcija za kupca, izlaganje privatnosti i nepouzdanosti trećih strana u koje bi trebali imati povjerenje zbog centraliziranog načina rada. Pametnim bi se ugovorima decentralizirala centralizirana priroda platformi s ekonomijom dijeljenja. Postoji

prijedlog za platforme s ekonomijom dijeljenja koja se temelji na Ethereum pametnim ugovorima. Sustav bi omogućavao korisnicima da registriraju i dijele svoje artikle bez pouzdane treće strane, a privatne bi informacije bile zaštićene. Suradnjom IoT-a i pametnih ugovora korištenje bi ekonomije dijeljenja napredovalo [32].

7.6. PAMETNI UGOVORI U JAVNOM SEKTORU

Pametni ugovori zajedno s blockchain tehnologijom mogu uvesti pozitivne promjene u sektor javnog upravljanja. Korištenjem blockchaina može spriječiti lažiranje podataka i omogućiti bolju transparentnost javnih informacija. Tako primjerice kod javnih natječaja, kada bi se koristila blockchain tehnologija i pametni ugovori, moglo bi se utvrditi identitet ponuditelja i naručitelja, proces javnog natječaja bio bi automatiziran s podrškom i pomoći s revizijom [32].

Prilikom razmjene podataka između sustava uredskog poslovanja blockchain tehnologija i pametni ugovori bi se koristiti za utvrđivanje izvornosti, cjelovitost i sljedivosti podataka [55].

U današnjem se vremenu ne mora biti na mjestu prebivališta tijekom glasovanja i umjesto toga može se glasati putem e-glasovanje. E-glasovanje se suočava s nekoliko izazova kao što je utvrđivanje identiteta korisnika i očuvanje privatnosti korisnika. Postoji prijedlog da se potvrdi identitet korisnika bez otkrivanja privatnosti korisnika, ali bi se i dalje oslanjalo na treći povjerljivi autoritet da miješa glasače kako bi došlo do otkrivanja privatnosti korisnika. Idući prijedlog zauzima se za korištenje protokola za glasovanje koji koristi znanje samo prebrojavanja kako bi se izgradio pošteni sustav glasovanja koji se temelji na pametnim ugovorima. Na taj se način čuva tajnost glasova uz to što je moguća potvrda identiteta korisnika [32].

Pametni ugovori mogu se upotrijebiti za uspostavljanje osobnog digitalnog identiteta i ugleda. Postoji prijedlog u kojem bi se kreirao profil osobe koji bi se temeljio na osobnom, internetskom, i poslovnom ugledu. Korisnici mogu štititi svoje privatne informacije pametnim ugovorima koji bi omogućili pristup za druge korisnike preko funkcionalnih klauzula. Sve se transakcije zapisuju na blockchain i ne mogu se neovlašteno mijenjati ili brisati [32].

7.7. PAMETNI UGOVORI U ZDRAVSTVENOM SUSTAVU

S napredovanjem tehnologije raste i standard življenja. Novo razvijeni uređaji u zdravstvu omogućuju praćenje zdravstvenog stanja pacijenata iz udobnosti njihovog doma. Već postoji niz uređaja koji prate razne atribute u ljudskom tijelu. Podaci o zdravstvenom stanju mogu se pratiti pomoću jeftinih uređaja i procesuirati brzo kako bi se dobile informacije. Integriranjem blockchain tehnologije u zdravstveni sustav osigurala bi se privatnost pacijenta, a podaci bi se čuvali i ažurirali u formatu digitalne glavne knjige. Uloga pametnih ugovora bila bi činiti sustav pouzdanijim i automatiziran. Pametni bi se ugovori mogli koristiti za pisanje odredbi i uvjeta, a kada bi se prikupili potrebni podaci, aktivirali bi se uvjeti ugovora za izvršenje ugovora [34].

8. UNAPREĐENJE PRAVNOG I TEHNOLOŠKOG OKVIRA PAMETNIH UGOVORA

U sljedećem poglavlju analiziraju se i definiraju pametni ugovori i tehnologija koja ih omogućava, trenutna upotreba pametnih ugovora te njihova buduća upotreba. Usporedbom klasičnih i pametnih ugovora prikazat će se prednosti i nedostaci pametnih ugovora. Proučit će se mogu li pametni ugovori funkcionirati služeći se sadašnjim načinom rada kako bi podržali veliki broj korisnika. Prezentirat će se stajalište pravne struke i regulatornih tijela na upotrebu pametnih ugovora te njihove želje za nužnim promjenama pametnih ugovora. Predložit će se poboljšanja koja bi imala cilj olakšanje pravne regulacije pametnih ugovora kako bi se osiguralo njihovo šire prihvaćanje.

8.1. ANALIZA DEFINICIJA BLOCKCHAIN TEHNOLOGIJE

U trećem se poglavlju definiralo što je blockchain tehnologija, njezini elementi i uloga. Elemente ne treba posebno objašnjavati zbog toga što se radi tehničkim elementima koji su davno definirani. S obzirom da je blockchain nova tehnologija koja se pojavila, njezina definicija nije jedinstveno usuglašena zbog različitih tumačenja te će se analizom sljedećih primjera predložiti definicija za blockchain tehnologiju.

IBM kaže: *Blockchain je zajednička glavna knjiga koja olakšava proces evidentiranja transakcija i praćenja imovine u poslovnoj mreži. Imovina može biti opipljiva (kuća, automobil, novac, zemljište) ili neopipljivo (intelektualno vlasništvo, patent, autorska prava, brend). Praktički bilo što posjeduje vrijednost može se razmijeniti i pratiti na blockchain mreži pritom smanjujući troškove i rizik za sve koji su uključeni.* [35]. Definiciju koju je ponudio IBM je jednostavna za razumijevanje i ne zahtijeva nikakvo prethodno znanje o blockchainu kako bi se razumjela. Definicija je primjerena početnicima i svima onima koji tek počinju učiti o blockchain tehnologiji. Definiciji nedostaje objašnjenje strukture blockchain tehnologije i tehničke pojedinosti.

Ethereum zajednica kaže: *Blockchain je javna baza podataka koja se ažurira i dijeli na mreži između sudionika. Block označava podatke i stanja koja su pohranjena u grupama pod imenom*

blocks. Ako se želi nekome poslati ethereum, podaci o transakciji se moraju dodati u blok kako bi ona bila uspješna. Chain označava da svaki novi blok ima kriptografsku poveznicu sa svojim prethodnikom. Drugim riječima, blokovi se povezuju u lanac. Podaci u bloku ne mogu se mijenjati bez da se ne mijenjaju svi naredni blokovi za što bi bila potrebna suglasnost cijele mreže. Svako računalo u mreži mora usuglasiti svaki novi blok i lanac u cjelini. Računala koja sudjeluju u mreži se nazivaju ″čvorovi″. Čvorovi osiguravaju da svi koji komuniciraju s blockchainom imaju iste podatke. Blockchain treba mehanizam sa suglasnošću kako bi postigao distribuiran dogovor oko podataka. [36]. Definicija koju je ponudila Ethereum zajednica sastoji se od više tehničkih informacija o tome što je blockchain. U fokusu definicije je pojašnjenje dviju riječi iz kojih je nastalo izraz blockchain te koja je njihova uloga. U definiciji tehnički opisi su točni osim prve rečenice gdje stoji da se radi o bazi podatka što je nije točno. Kvalitetno napisana definicija, lako razumljiva, preporučljiva za sve one koji žele znati više o blockchain tehnologiji u sklopu Ethereum blockchain.

OCED kaže: *Blockchain je zajednička glavna knjiga transakcija između stranki u mreži koja nije kontrolirana od strane ni jedne središnje vlasti. Glavna knjiga se može zamisliti kao knjiga zapisa koja zapisuje i pohranjuje sve transakcije kronološkim putem između korisnika. Umjesto da jedna vlast kontrolira glavnu knjigu (kao što je banka), ista kopija glavne knjige je održana od strane svih korisnika u mreži koji se nazivaju čvorovi.* [37]. Definiciju koju je sastavila OECD više se fokusira na upravljanje blockchaina. Definicija je tehnički ispravna s dobrim primjerima usporedbu za bolje razumijevanje kako funkcioniraju glavne sastavnice.

Karim Sultan, Umar Ruhi i Rubina Lakhani (2018) u radu *Conceptualizing Blockchains: Characteristics & Applications* nude svoju definiciju blockchain tehnologije zato što postoji velika razlika u interesu za tim područjem i znanstvene literature. Definicija oko koje su se usuglasili i složili glasi: *decentralizirana baza podataka koja sadrži slijedno povezane kriptografske blokove s transakcijskom imovinom koja je digitalno potpisana i upravljana modelom konsenzusa.* [38]. U definiciji su naglasili glavne sastavnice koje čine blockchain tehnologiju i kako su one povezane te kako se upravlja njima. Odlučeno je da se umjesto pojma *glavne knjige* koristi izraz *decentralizirana baza podataka.* Iako je to dobar primjer kako bi se lakše razumjelo, nije tehnički ispravno zato što baze podataka imaju svoje specifične karakteristike. Baze podataka su centralizirani računalni sustavi koji pohranjuju više tipova zapisa, podržavaju izmjenu podataka od

administratora i imaju dobru proširivost s brzim načinom rada. To su karakteristike koje blockchain tehnologija ne posjeduje. Ovaj primjer i kao prethodni predstavljaju razlog zašto postoji ovaj rad jer korištenje krivih izraza može dovesti do krivog objašnjenja tehnologije.

Gavin Wood i Andreas M. Antonopoulos kažu: *U Ethereumu, blockchain je niz blokova koju su potvrđeni od sustava koji radi na principu dokaza o radu, svaki je blok povezan sa svojim prethodnikom sve do početnog bloka. Razlikuje se od Bitcoin protokola u tome što on nema ograničenje veličine bloka umjesto toga Ethereum koristi promjenjivo ograničenje gasa.* [21]. U knjizi *Mastering Ethereum Building Smart Contracts and Dapps* Gavin Wood i Andreas M. Antonopoulos (2019) u svojoj definiciji stavljaju naglasak na međusobnu povezanost blokova te koja je razlika u odnosu na blokove koje koristi Bitcoin protokol. Ova je definicija specifična za jedna protokol, ali nije dobra za opću definiciju.

Iz izabranih primjera može se uočiti da imaju sličnosti i da se podudaraju u nekim riječima, ali su definicije prilagođene vrsti blockchaina i što se njime želi postići. Ovih je pet primjera dovoljno kako bi se dokazala pretpostavka. Cilj je predložiti definiciju koja je lako razumljiva, precizna i sažeta tako da sadrži sve osnovne elemente. Predloženom se definicijom cilja na skupinu ljudi koji traže objektivnu definiciju na akademskoj razini i žele znati više o blockchain tehnologiji. Prijedlog blockchain definicije glasi: *Blockchain je distribuirana glavna knjiga transakcija u kojoj su blokovi kriptografski povezani lančano i ažurirana je jedino konsenzusnim mehanizmom od strane čvorova koju čine mreža ravnopravnih računala.*

8.2. ANALIZA DEFINICIJA PAMETNIH UGOVORA

U Poglavlju 4.2.4. izložena je definicija pametnih ugovora koju je predložio Nick Szabo. Ostale su definicije proizašle iz vlastitog truda. Analizom definicija pametnih ugovora cilj je pronaći onu koja je najbolje tehnički opisana. Ako ni jedna nije zadovoljavajuća, ponuditi će se prijedlog definicije. Prilikom izbora definicija gledat će se da se izaberu definicije koje su iz stručnih izvora. Također, izabrat će se primjeri koji su kreirale vladine institucije kako bi se razumjelo njihovo poimanje nove tehnologije.

Pametan ugovor je nezaustavljiv i siguran računalni program koji predstavlja dogovor koji je automatski provediv i izvršiv. [1]. Definicija koju je predstavio Bashir I. nastoji pružiti generaliziranu definiciju pametnog ugovora. Definicija je pametno konstruirana zbog toga što je u jednoj rečenici sažeta osnova što je pametan ugovor. Fokus definicije je da kratko i jasno objasni što oni predstavljaju i kakvu funkciju izvršavaju. Nedostatak ove definicije je da izostanak spomena blockchain tehnologije koja ih omogućava da funkcioniraju.

Ethereum organizacija kaže: *Jednostavno ″pametan ugovor″ je program koji se izvodi na Ethereum blockchanu. To je zbirka kodova (i funkcija) i podataka (i stanja) koji se nalaze na jedinstvenoj Ethereum blockchaina adresi.* [39].

Pametni ugovori su vrsta Ethereum računa. To podrazumijeva da imaju saldo i mogu slati transakcije preko mreže. Međutim oni nisu kontrolirani od strane korisnika umjesto toga su raspoređeni na mreži i izvršavaju se onako kako su programirani. Korisnički računi mogu s njima komunicirati slanjem transakcija koje izvršavaju funkciju koja je definirana u pametnom ugovoru. Pametni ugovori mogu definirati pravila kao redovni ugovor i putem koda ih može automatski primjenjivati. Prema zadanim postavkama pametni ugovori se ne mogu obrisati, a interakcija s njima je neponištiva [39]. Ethereum organizacija definira pametne ugovore u skladu s njihovim funkcioniranjem na Ethereum blockchain mreži. Iz definicija se može vidjeti odnos korisnika i pametnog ugovora. Osoba mora imati korisnički račun i saldo kako bi mogla slati transakcije putem mreže. Jednom kada je pametan ugovor pušten u rad korisnik nema kontrolu nad njime, a jedini način da ima interakciju s njime je transakcijom. Definicija je specifična za Ethereum mrežu i nije pogodna za opću definiciju.

Pravna komisija Ujedinjenog Kraljevstva kaže: *Pametni ugovori su računalni programi koji se izvršavaju automatski ili poluautomatski bez potrebe za ljudskom interakcijom. Pametni ugovori mogu izvršavati transakcije na decentraliziranim mjenjačnicama kriptovaluta, distribuirana glavna knjiga može pomoći igrama kroz razmjenu kolekcionarskih predmeta između sudionika i pokretati programe za kockanje putem interneta. Pametni ugovori se mogu koristiti za definiranje i izvođenje obveza za pravno obvezujuće ugovore.* [40]. Pravna komisija Ujedinjenog Kraljevstva definira pametne ugovore kao računalne programe koji se izvršavaju bez ljudske intervencije. Definicija nedostaje spomen tehnologije koja omogućava pametne ugovore. Navode primjere u kojim se slučajevima pametni ugovori mogu primijeniti i koristiti.

Wood G. i Antonopoulos A.M. (2019) kažu: *Pametni ugovori su nepromjenjivi računalni programi koji rade deterministički u kontekstu EVM kao dio Ethereum mrežnog protokola na decentraliziranom "svjetskom" Ethereum računalu. Pametni ugovori su jednostavno računalni programi. Riječ ugovor u ovom kontekstu nema nikakvo legalno značajne. Računalni kôd pametnog ugovora se ne može mijenjati jednom kada je pametan ugovor pušten u rad. Jedini način da se pametan ugovor promijeni je da se novi pusti u rad. Pametni ugovori su deterministički jer svatko tko ga pokrene dobit će jednak ishod i to u kontekstu izvršavanja na Ethereum blockchainu. Djelovanje pametnih ugovora u kontekstu izvršenja je ograničeno. Oni su u stanju pristupit stanju u kojem se nalaze, transakciji koja ih je pozvala i informacijama o prijašnjim blokovima. Cijeli sustav funkcionira kao jedno "svjetsko računalo" zato što svi primjeri EVM djeluju na istom inicijalnom stanju te isporučuju isto konačno stanje, iako EVM radi lokalno na svakom Ethereum čvoru* [21]. Wood G. i Antonopoulos A.M. (2019) definiraju pametne ugovore u sklopu rada Ethereum blockchain mreže. Oni pak navode da riječ *ugovor* nema legalno značenje čime odbacuju ideju da su ovakvi ugovori dopušteni zakonom. Opisuju detaljnije kako sustav funkcionira koji omogućuje rad pametnih ugovora od prijašnjih definicija. Ova je definicija specifična jer daje informacije o njihovom funkcioniranju na Ethereum blockchainu. Ova će definicija odgovarati onima koji je traže za Ethereum blockchain, no može poslužiti za one koji traže generalnu definiciju jer se podudaraju u nekim svojstvima iz kojih se može zaključiti što predstavljaju pametni ugovori.

NARA kaže: *Pametan ugovor je ugovor koji je preveden u softverski jezik za blockchain na kojem je pohranjen i događaj može pokrenuti njegovo automatsko izvršenje. Drugačije rečeno, pametan ugovor je niz if/then programiranih tvrdnji spremljeno na blockchanu. Ugovor će se automatski izvršiti i jednom kada su svi zahtjevi ispunjeni, rezultati nastali tom akcijom će se pohraniti i dijeliti na blockchainu.* [41]. Državni arhiv i uprava za evidenciju (engl. NARA - *National Archives and Records Administration*) savezne vlade SAD-a je ponudila dvije definicije pametnih ugovora. U prvoj su definiciji riječ *program* zamijenili *ugovorom koji je preveden u softverski jezik,* no to ne mijenja smisao. U drugoj su izraz *program* dodatno pojednostavili s *niz if/then programiranih tvrdnji*. Prednost ove definicije što je daje dva objašnjenja i sve aspekte pokriva. Njezin nedostatak je što se ne zna je li program promijeniv ili ne.

U ovih pet primjera cilj je pokazati kako se definicije pametnih ugovora razlikuju. Sve definicije imaju zajedničko da definiraju pametne ugovore kao računalne programe. Problem je u

daljnjem opisu definicije gdje dolazi do neusklađenosti. Predlaže se opća stručna definicija koja ima za cilj u sebi sadržavati samo osnovna obilježja pametnih ugovora kako bi razlikovala generalna definicija i specifična. Definicija će biti točna, sažeta i jednostavna za razumijevanje. Predlaže se sljedeća definicija: *Pametan ugovor je nezaustavljiv i nepromjenjiv računalni program koji se automatski izvršava i pohranjuje na blockchain mrežu onda kada su ugovoreni uvjeti zadovoljeni.*

8.3. ANALOGIJA TRADICIONALNIH I PAMETNIH UGOVORA

Pametni ugovori kao i tradicionalni ugovori dolaze sa svojim prednostima i nedostacima. Usporedbom pametnih i tradicionalnih ugovora prikazat će se prednosti koje donose pametni ugovori sa sobom, ali i rješenja koja su nužna kako bi se smanjili nedostaci pametnih ugovora na najmanju moguću mjeru.

Predložak koji inače čini standardni dio ugovora nalazi se na kraju ugovora i mnogi ga ne pročitaju jer ga smatraju formalnošću. Tu je problem u sadržaju koji je izostavljen iz predloška, a ne što je u njemu sadržano što može dovesti osobu koja na slijepo potpisuje ugovor u pravnu opasnost. Stoga je nužno detaljno čitati predložak kako bi se izrazilo slaganje ili protivljenje što je sadržano u predlošku. Ovaj problem pametni ugovori rješavaju jasnim objašnjenjem obveza za uključene strane putem koda ili platforme s korisničkim sučeljem [42].

Tradicionalni ugovori mogu se koristit kako bi se pogodovalo jednoj strani zato što strana koja nudi *standardni ugovor* ne mora nužno značiti da je u skladu s potrošačkim ugovornim pravom Europske unije. Pametni ugovori ovaj problem rješavaju ponudom više vrsta pametnih ugovora tako da stranke mogu izabrati ugovor koji zadovoljava njihove potrebe i prilagoditi ovisno u slučaju upotrebe [42].

Budući da se nisu svi ugovori standardizirani, nužno je angažirati posrednike koji bi sastavili ugovor i stranu koji bi osigurala provedbu odredaba ugovora. To povećava troškove sklapanja i čekanja za ispunjenje ugovora.

S pametnim je ugovorima sve napravljeno unaprijed programiranim ugovorima čime su eliminirani posrednici, a i ubrzala se cijena sklapanja ugovora i njegova provedba [42].

Tradicionalni ugovori napisani su na računalu i stavljani na papir zbog čega su izloženi riziku od neovlaštenog rukovanja pa tako mogu biti obrisani ili izmijenjeni, a papir na kojem je ugovor napisan i potpisan može biti uništen, a potpis može biti krivotvoren.

Pametni ugovori nemaju problema s time zato što su kriptirani i distribuirani između čvorova u decentraliziranom registru čime su zaštićeni od gubitka, uplitanja neovlaštenih osoba i računalnih napada. Budući da ne postoji mogućnost ručnog ispunjavanja obrazaca, čovjek ne može napraviti grešku prilikom shvaćanja ili nemogućnosti čitanja rukopisa. Tradicionalni ugovori nisu sami po sebi problematični, oni također posjeduju prednosti koje dolaze s njima. Tradicionalni ugovori predstavljaju dokaz sklapanja dogovora između stranaka koje su uključene. Sprečavaju nerazumijevanja i sporove u budućnosti jer omogućava informiranost prije sklapanja ugovora Uvjeti dogovora koji su napisani na papir pružaju sigurnost i jamče da oni neće biti promijenjeni. Daju jasne upute kako da se sporovi odlučuju. Pojašnjavaju koji uvjeti moraju biti zadovoljeni kako bi se ugovor mogao raskinuti prije nego li je posao obavljen [42].

Prednosti koje sa sobom nose tradicionalni ugovori mogu se umetnuti u pametne ugovore, ali stavljanje pametnog ugovora na papir za one koji ga žele u papirnatom obliku predstavlja izazov. Za to bi bio potreban prevoditeljski program koji bi preveo pametni ugovor u format i jezik koji je razumljiv čovjeku. Time se otvara poslovna prilika za sve tvrtke koje se bave razvojem softvera, a ujedno i izazov za pravnu struku da ih odobri.

Pametni ugovori imaju jasne prednosti u odnosu na tradicionalne ugovore, ali i oni imaju svoje nedostatke.

S obzirom da je čovjek pisao pametne ugovore, uvijek postoji mogućnost da nastane pogreška i zamjene. Pametan ugovor je siguran i učinkovit ako je računalni kod napisan precizno i ispravno. Greške koje nastaju prilikom programiranja zbog ljudskog faktora mogu ugroziti sustav. Trenutačno neke države tek rade na prijedlozima koji bi regulirali pametne ugovore i blockchain tehnologiju. Problem koje može nastati u procesu predlaganja pravnog okvira za pametne ugovore je da ne budu usklađeni s postojećim pravnim okvirima. Za programiranje pametnih ugovora potreban je iskusan programer koji bi napisao nepogrešive pametne ugovore koji bi se prihvatili u unutarnjim strukturama kompanije. Potrošači nisu svjesni novih tehnologija i jako su sumnjičavi prema njima zato što ih ne razumiju. Budući da se podaci zapisuju na blockchain, nemoguće je napraviti izmjene što bi zahtijevalo kreiranje novog pametnog ugovora. To bi moglo dovesti do

grešaka u sustavu čime bi postalo manje siguran. Treće strane iz svijeta tradicionalnih ugovora ne bi nestali nego bi dobili nove uloge kao što su odvjetnici koji su iskusni u informatičkim tehnologijama, a bili bi nužni programerima pametnih ugovora za konzultiranje oko kreiranja novih vrsta ugovora [42].

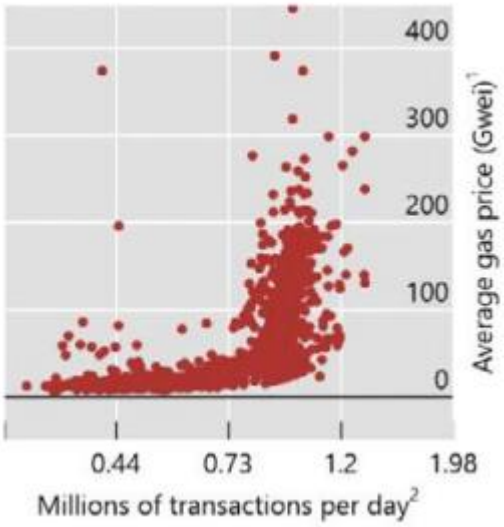
8.4. PROŠIRIVOST ETHEREUM BLOCKCHAIN

Izvedba pametnih ugovora je povezana s korištenim blockchainom. Kako bi blochchain bio siguran, on se mora raditi unutar strogih pravila koja se ne mogu mijenjati bez konsenzusa mreže. Zbog tih pravila koja čine blockchain sigurnim, ujedno ga i ograničava koliko može maksimalno i efikasno raditi. U ovom radu ograničit će se samo na Ethereum mrežu kako bi vidjeli s kojima ograničenjima radi trenutačna mreža te što je čeka u budućnosti.

Sloj 1 je osnovni blockchain. Ethereum je sloj 1 blockchain zbog toga što predstavlja temelj na kojem će se graditi različite mreže sloja 2. Ethereum također funkcionira kao sloj s dostupnim podacima za sloj 2. Projekti koji će koristiti sloj 2 postavljat će svoje transakcijske podatke na Ethereum na koji će se oslanjati za dostupnost podataka. Ti će se podaci koristiti kao bi dohvatili stanje sloja 2 ili za osporavanje na sloj 2. Ethereum kao sloj 1 u sebi ima ugrađenu[43]:

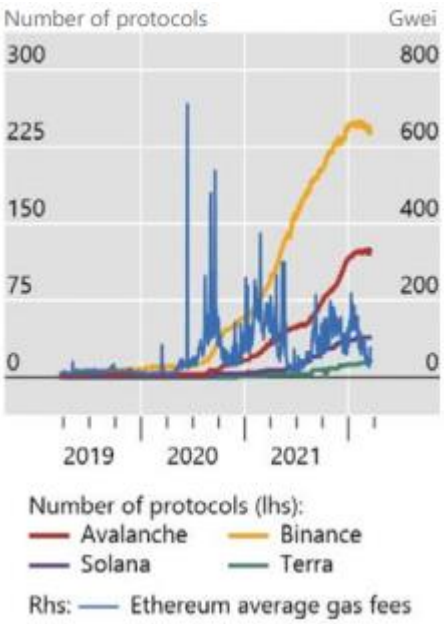
- Mrežu operativnih čvorova koji osiguravaju i evidentiraju mrežu
- Mrežu kreatora blokova
- Blockchain i povijest transakcija
- Mehanizam za konsenzus mreže [43].

Boissay et al. (2022) u svome radu dobro opisuju i prikazuju grafovima ograničenja s kojima je suočen sloj 1. Na Ethereum blockchainu maksimalan broj transakcija po bloku je 15 u sekundi. Jednom kada broj transakcija dođe do toga ograničenja, dolazi do zagušenja i cijena transakcije raste eksponencijalno prikazano na slici 12 [44].



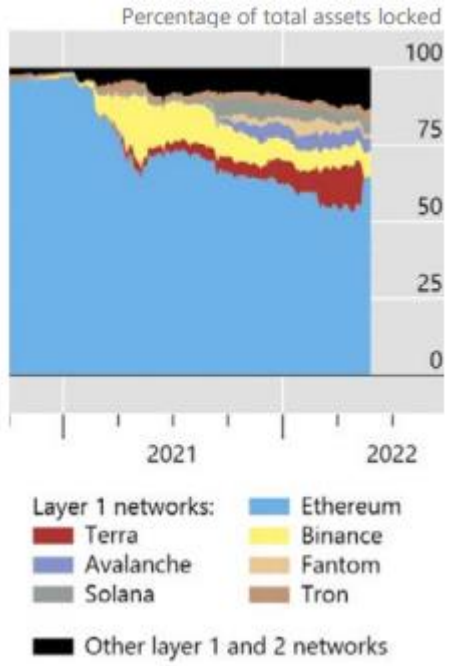
SLIKA 12. RAST CIJENE TRANSAKCIJE KAD DOĐE DO ZAGUŠENJA [44]

Za vrijeme zagušenja one transakcije koje nose sa sobom veće naknada prije će biti obrađene kako bi izbjegle duža čekanja. Tako primjerice za vrijeme slabog prometa prosječna cijena transakcije iznosi 1 dolar dok za vrijeme zagušenja taj se iznos može biti 75 puta veći. Povećanjem broja rudara neće se riješiti problem zagušenja zbog nužnog ograničenja broja transakcija kako bi se održao konsenzus. Ugrađena ograničenja i visoke cijene transakcija dovode do fragmentacije korisnika koji odlaze od visokih cijena gasa na alternativne blockchainove koji imaju niže naknade po transakciji. Nagli rast gasa kod Ethereum protokola ima za posljedicu povećanja broja protokola kod drugih blockchainova kao što su Avalanche, Binance ili Solana prikazano na slici 13 [44].



SLIKA 13. RAST PROTOKOLA DRUGIH BLOCKCHAINOVA ZA VRIJEME ZAGUŠENJA U ETHEREUM PROTOKOLU [44]

Novi blockchainovi u početku dijele protokole sa starijim, ali se razlikuju u posebno dizajniranim značajkama. Prvi protokoli koji su radili na novim blockchainovima već su bili dostupni na Ethereum blockchain (Slika 14) [44].



SLIKA 14. FRAGMENTACIJA DECENTRALIZIRANIH FINANCIJA NA MREŽAMA SLOJA 1 [44]

Na slici 14. može se uočiti uzorak koji sugerira da se korisnici prebacuju na druge blockchainove kako bi obavili svoje transakcije koje su s vremenom postale skuplje na Ethereum blockchainu. Novi blockchainovi često ciljaju na veći broj transakcija što rezultira većom centralizacijom i slabijom sigurnošću [44].

Zbog toga je došla potreba za slojem 2 koji će omogućiti nadogradnju Ethereum blockchaina. Sloj 2 je kolektivan izraz koji opisuje skup rješenja za nadogradnju Ethereuma, predstavlja odvojen blockchain koji proširuje Ethereum i nasljeđuje njegove sigurnosna jamstva. Inače, tri su poželjne karakteristike blockchaina nadogradivost, decentraliziranost i sigurnost. Problem s jednostavnim blockchainom je da može postići samo dvije poželjne karakteristike od poželjnih tri. Glavni cilj nadogradnje je povećanje brzine zaključenja transakcija i maksimalan broj transakcija u sekundi bez žrtvovanja decentraliziranosti i sigurnosti. Sloj 2 blockchain radi na način da komunicira s Ethereum (prilaganjem skupova transakcija) kako bi osiguralo jamstava za sigurnost i decentraliziranost. Sve to bez potrebe za mijenjanjem sloja 1 koji će upravljati sa sigurnošću, dostupnost podataka i decentralizacijom dok će sloj 2 uspravljati s nadogradnjom. Sloj 2 preuzet će zadatak upravljanja transakcijama od sloja 1 i njemu će samo slati konačne dokaze o transakcijama. Rolanje je trenutačno preferirano rješenje sloja 2 za nadogradnju Ethereuma. Rolanje je postupak okrupnjivanja više transakcija u jednu transakciju koja se šalje na sloj 1 jednom kada je postignut konsenzus. Korist od rolanja je značajno smanjenje cijene naknade u odnosu na sloj 1 koje može iznositi i do 100 puta manja nego na sloju 1 [43].

Postoji dva tipa rolanja s različitim sigurnosnim modelima:

- Optimistično rolanje - pretpostavlja da su transakcije u skladu sa zadanim postavkama važeće i vrši obrađivanje putem dokaza o prijevari ako dođe do izazova. Dokaz o prijevari je sigurnosni model koji se pokreće ako se sumnja da je došlo do prevare.
- Rolanje s nultim znanjem - vrši obradu izvan lanca i prilaže lancu dokaz o valjanosti. Dokaz o valjanosti je sigurnosni model koji vrši transakcijske obrade izvan lanca te ih prilaže glavnom lancu s dokazom o valjanosti [45].

Rolanje je samo jedno od rješenja koje se koristi Ethereum na sloju 2, Ethereum također koristi kanale stanja, sporedne lance, plazmu i Validium. Kanali stanja koriste ugovore s višestrukim potpisima kako bi omogućili sudionicima da brzo izvršavaju transakcije izvan glavnog lanca te kasnije šalju konačnu verziju glavnoj mreži. Korištenjem kanala stanja značajno se smanjuje

zagušenje mreže, iznosi naknada i zastoji. Dva tipa kanala koja se koriste su kanali stanja i platni kanali. Sporedni su lanci nezavisni blockchainovi koji su usklađeni s EVM-ima koji rade paralelno s glavnom mrežom. Oni su usklađeni s Ethereum preko dvostrukih mostova i rade pod vlastitim pravilima za konsenzus i parametrima za blok. Mostovi se koriste za povezivanje dva blockchaina. Plazma lanac je izdvojeni blockchain koji je usko vezan za Ethereum lanac i koristi dokaz o prijevari kako bi razriješio sporove. Validium je lanac koji koristi dokaz o valjanosti isto kao i rolanje s nultim znanjem s time što ne pohranjuje podatke na sloj 1. To omogućava da svaki Validium lanac može obraditi do 10 tisuća transakcija u sekundi i višestruki lanci mogu se izvoditi paralelno [45].

Da se zaključiti da je glavni Ethereum blockchain ograničen koliko može obraditi transakcija. Stoga ako bi ostao u takvom obliku ne bi bio primjeren za široku upotrebu jer ne bi mogao obraditi veliki broj zahtjeva bez kašnjenja i skupih naknada. Iako je primjereno da su cijene veće kada je zagušenje veće, ono nije pravedno jer pogađa one koji ne mogu platit veću cijenu naknade. Stoga su ove nužne promjene kako bi blockchain mogao zadovoljavati potrebe koje se nalaze pred njime. Ujedno je put da pametni ugovori dobiju priliku biti dostupni široj masi.

8.5. SADAŠNJE I BUDUĆE REGULATORNO STAJALIŠTE PAMETNIH UGOVORA

Da bi pametni ugovori imali široku primjenu, oni moraju biti u skladu s zakonima države, kontrolirani od državnog tijela te imati suglasnost pravne struke. Prvo će se prikazati stajalište Blockchain foruma i knjižnica Europske unije (u nastavku EU Blockchian) koji predstavlja pilot projekt Europskog parlamenta, radi pod okriljem glavne uprave za komunikacijske mreže, sadržaji i tehnologije Europske komisije.

EU Blockchain ideju o legalnim pametnim ugovorima smatraju neodoljivom s obzirom na koristi koje donosi sa sobom. Isto smatraju da ako nešto radi pomoću koda, ne znači da može dobiti pravi status. Prezentirali su pet problema koja se pojavljuju upotrebom pametnih ugovora u praksi [46]:

1. Prva prepreka koja se pojavljuje su pravne prepreke. Smatraju ga važnim problemom koji se često precijenjuje i uključuje pitanje mogli li ili ne pametni ugovori zadovoljiti pravne zahtjeve koji su zakonom propisani kako bi bili pravno obvezujući sporazumi [46].

2. Druga je prepreka stavljanje potpisa na pametan ugovor. Pametni ugovori moraju biti potpisani u digitalnom obliku. Digitalni potpisi na blockchainu moraju biti potvrđeni od pružatelja usluga povjerenja (engl. TSP – *Trust Service Providers*) kako bi bili pravno valjani u Europi pod uredbom o elektroničkoj identifikaciji i uslugama povjerenja (engl. eIDAS - *electronic Identification Authentication and Signature*). Automatski legalni pameti ugovori koji zahtijevaju digitalni potpis moraju također biti sposobni utvrditi je li potpis važeći, je li povezan s pripadajućom osobom i imali li ta osoba punomoć da potpiše ugovor [46].

3. Treća prepreka je nepromjenjivost pametnih ugovora jer, jednom kada su programirani i postavljeni na blockchain, oni ostaju u tom obliku. Iako je to jedna od njihovih prednosti da će se izvršiti kako su programirani, što u slučaju da dođe do promjene uvjeta koji se moraju poštovati kako bi bili ponovno legalni. Poslovni subjekti koji predstavljaju stranke u ugovorima imaju šire ovlasti kad je u pitanju odustajanje od obveza takvih nagodbi zbog čega profesionalni subjekti općenito mogu podnijeti rizik korištenja pametnih ugovora dok je ograničene obveze i odgovornost teže nadomjestiti u odnosima poslovnih subjekta i korisnika. Zbog toga može doći do nagodbi koje se moraju rješavati izvan blockchain sustava i, ako se ne uspostavi zalog za neispunjavanja obveza, onda će provedba ugovora jedino biti moguća sudskim putem. Pametni ugovori ne rješavaju ni eliminiraju problem kršenja ugovora, ugovornih obveza i njihovu provedbu. Problem je i nedostatak alata za identificiranje sudionika na blockchainu. Zato je potrebno rješenje između blockchain predstavnika i državnih vlasti te između samih sudionika u blockchainu [46].

4. Četvrta prepreka je osiguranje kvalitete i provjera ispravnosti pametnih ugovora. Ako pametan ugovor ima greške unutar sebe, može naštetiti uključenim stranama. Greška ne mora biti nužno povezana sa softverom nego može doći do greške zbog složenosti pravilnog programiranja ugovornih obveza. Zbog toga se postavlja pitanje moraju li povjere ispravnosti postati obvezne ili moraju biti pravno priznate kako bi pametni ugovori postali ispravni [46].

5. Peta prepreka je legalan status, provedba i posljedice općenito pametnih ugovora. Ako se transakcije zabilježene na blockchainu, ne mogu prikazati i biti štićene u stvarnom svijetu tada je njihov potencijal puno manji. Da bi imovine koja se prijenosi preko blockchaina imala vrijednost

u stvarnom svijetu, ona mora imati jednaka prava. Problem je i primjena tradicionalnih pravila na kriptoimovinu. Različita vrsta kriptoimovine imat će različita rješenja i različitu razinu decentralizacije. Rješenje koje se nameće je da sudionici na blockchainu izaberu mjerodavno pravo za blockchain [46].

Kako bi se prevladala prva prepreka, država mora klasificirati pametne ugovore kao pravno obvezujući sporazum i mora definirati u kojim se situacijama oni mogu koristiti. Budući da su pametni ugovori programirani pomoću više programskog jezika, nužno ih je staviti u okvir koji svatko može pročitati i razumjeti. Rješenja za prijevod moraju ponuditi poslovni subjekti koji imaju znanje iz područja blockchain tehnologije, a na državi je javnim natječajima potaknuti nova rješenja. Za savladavanje druge prepreke digitalni potpisi moraju biti usklađeni s eIDAS te ih mora potvrditi TSP. Da bi se odredilo tko smije ili ne smije potpisati pametan ugovor, nužna su rješenja koja će povezivati blockchain s vanjskim bazama podataka korisnika. Treća prepreka i problem nepromjenjivosti pametnih ugovora može se riješiti tako da se postavi nova ažurirana verzija ugovora koji će u sebi sadržavati zadovoljene postojeće obveze koje ne zahtijevaju izmjene. Drugo rješenje za ovaj problem je postavljanje uvjeta koji će obustaviti izvršenje ugovora te će stranka vratiti njihova sredstva. Kršenje odredaba pametnih ugovora ne nastane ljudskom intervencijom, nego greškom koda. Rješenje za to bi bilo postojanje ugovora u rezervi koji bi vratio stvari na početno stanje. Za entitete koji žele koristi pametne ugovore nužna će biti identifikacija jer ako ne bi postojala, onda se otvara prostor zlouporabu. Četvrta se prepreka može riješiti na dva načina. Prvi je način da se koristi programski jezici koji rade na sličnom ili istom principu kao što radi programski jezik Vyper. Drugi je način da se prvo testiraju pametni ugovori na testnom blockchainu prije nego li se postavi na stvarnom. Problem pete prepreke, prikaz i primanja informacija iz vanjskog svijeta, može se riješiti korištenjem blockchain proročanstva (engl. *Oracle*). Blockchain Oracle služi kao most između stvarnog svijeta i blockchaina te je sposoban primiti i proslijediti podatke iz stvarnog svijeta za blockchain i obrnuto. Chainlink je ponudio rješenja za taj izazov. Vrijednost kriptoimovine morat će definirati i regulirati državnim regulatornim agencijama. Tako primjerice za vrijeme pisanja diplomskog rada došlo je do velikog rasta nezamjenjivih tokena (engl. NFT – *non-funguble token*). NFT-ovi su digitalna imovina ili token koji predstavlja vlasništvo nad digitalnim ili fizičkim imovinom. Oni su se pojavili kao odgovor na problem autorskih prava u digitalnom svijetu te pokazuju potencijal u drugim područjima. Iako su kreirani s dobrom namjerom, također dolaze s lošim praksama kao što je

korištenje za pranje novca. Trenutačna tri najveća problema s kojim se susreću NFT-ovi su neovlaštena prodaja kopija drugih NFT-ova, kreiranja NFT-ova s sadržajem koji se ne posjeduje i prodaja setova NFT-ova koju sliče vrijednosnom papiru.

Sljedeće regulatorno stajalište prikazat će Ujedinjeno Kraljevstvo kojim upravlja Zakonska Komisija Engleske i Velsa. Zakonska komisija Engleske i Velsa je zakonsko nezavisno tijelo koje ima za cilj osigurati da je zakon pravedan, jednostavan i isplativ. Provode istraživanja i rasprave kako bi napravili sistematske preporuke koje se upućuju u Parlament, standardiziraju zakone, eliminiraju anomalije, ukidaju zastarjele i nepotrebne akte i smanjuju broj zasebnih statuta [47].

Zakonska komisija je 25.11.2021. objavila savjet Vladi Ujedinjenog Kraljevstva u kojem zaključuju da trenutačni legalni radni okvir Engleske i Velsa može podržati i omogućiti korištenje legalnih pametnih ugovora bez potrebe za zakonodavnom reformom. Fleksibilnost njihovog općeg prava osigurava da nadležnost Engleske i Velsa predstavljaju idealnu platformu za inovaciju i poslovanje. Uz postupni i karakterni razvoj općeg prava u specifičnom kontekstu mogu se trenutačni legalni principi primijeniti na legalne pametne ugovore kao što se mogu na tradicionalne. Postojeći legalni principi mogu se prilagoditi za neke vrste legalnih pametnih ugovora koji bi mogli postaviti nova pravna pitanja i činjenične događaje. Također su odvojeno razmotrena dva povezana područja zakona kao što su zakon o djelima i pravila o nadležnosti. Zakon o međunarodnom privatnom pravu i djelima dva su područja koja zahtijevaju poboljšanja kako bi se podržala upotreba tehnologije pametnih ugovora u odgovarajućim okolnostima [40].

Zakonska komisija Engleske i Velsa ima pozitivan stav zato što su utvrdili da sadašnji pravni okviri mogu podržati korištenje pametnih ugovora. Iako su svjesni da bi neki tipovi pametnih ugovora mogli imati poteškoće oko njihove legalnosti, smatraju da su njihovi pravni principi dovoljno dobro definirani da se mogu primijeniti na nove tehnologije.

Zadnje regulatorno stajalište koje će se prikazati je ono Sjedinjenih Američkih Država. Povjerenica Američke komisije za reguliranje i trgovinu vrijednosnim papirima (engl. SEC - *U.S. Securities and Exchange Commission*) Caroline A. Crenshaw iznijela je stajalište SEC-a za pametne ugovore i koje prepreke vide njihovim korištenjem.

U Sjedinjenim Američkim Državama višestruke federativne vlasti imat će ovlasti nad decentraliziranim financijama, a uključuje Ministarstvo pravosuđa (engl. *Deparment of Justice*),

Ured za suzbijanje pranja novca (engl. *Financial Crininal Enforcement Network*), Služba unutarnjih prihoda (engl. *Internal Revenue*), Državna komisija za terminsku trgovinu (engl. *Commodity Futures Trading Commission*), Američka komisija za reguliranje trgovinu vrijednosnima papirima i Sjevernoamerička udruga upravitelja vrijednosnih papira (engl. NASAA - *North American Securities Administrators Association*). Svi potencijalni investitori moraju znati da je investiranje u projekte koji nisu registrirani u SEC-u riskantnije nego na tradicionalnim tržištu. Iako su transakcije zabilježene na javnom blockchainu, to ne čini decentralizirane financije transparentnim. Nedostatak transparentnosti potiče dvije vrste tržišta jedno je tržište profesionalnih investitora i insajdera koji ubiru zaradu na povratima dok je tržište malih investitora izloženo većem riziku, lošijim ponudama i imaju male šanse da budu uspješni. Većina decentraliziranih financija financira se rizičnim kapitalom koji predstavljaju financijske institucije ili imućni pojedinci i ostalih profesionalnih investitora. Nije jasno koliko su mali investitori upoznati s time, ali temeljni ugovori o financiranju često profesionalnim ulagačima nude kapital, opcije biranja, savjetodavne uloge, pristup upravljanju projektima, iznošenje formalnog i neformalnog mišljenja o upravljanju i operacijama, zadržavanje istog iznos vlasničkog udjela u slučaju izdavanja novih dionica i mogućnost raspodjele interesa za kontrolom između saveznika i ostale prednosti. O ovakvim se dogovorima rijetko raspravlja, ali imaju značajan utjecaj na vrijednost investicija i njihov ishod. Zbog toga su mali investitori u nepovoljno položaju u odnosu na profesionalne investitore. Ako decentralizirane financije imaju za cilj privući veći broj investicija, one moraju shvatiti da velika većina populacije neće biti upoznata s rizicima koji su povezani s kodom. Decentralizirane financije funkcioniraju bez posrednika i djeluju izvan postojećeg zaštitnih mehanizma za postojeće investitore i tržište. Zbog toga su mali investitori zakinuti na pristup profesionalnim financijskom savjetnicima i ostalim posrednicima koji provjeravaju da potencijalne investicije budu kvalitetne i zakonite čime se smanjuju prevare i daju savjeti oko potencijalnih rizika u tradicionalnim financijama [48].

Drugi izazov s kojim se susreće tržište decentralizirane financije skrivena su imena zbog čega je teško detektirati manipuliranje tržištem. Iako su transakcije zabilježene na blockchainu tako da ih mogu svi vidjeti, ta vidljivost je djelomična zbog toga što se adrese pošiljatelja i primatelja ne mogu povezati s identitetom osobe koja ih kontrolira. Bez efikasne metode utvrđivanja identiteta mešetara ili vlasnika pametnog ugovora teško je utvrditi jesu li cijene imovine i volumeni trgovanja prirodni ili su rezultat manipulativnog trgovanja. Iako je anonimnost jedna od zagovaranih

prednosti decentraliziranih financija, pokazalo se da investitori u SAD-u prihvaćaju kompromise u kojim su spremni žrtvovati jednu razinu privatnosti u entitetima putem kojih trguju s vrijednosnim papirima. Projekti koji nađu rješenje za pseudoanonimnost imaju veće šanse uspjeti jer će investitori biti sigurni da vrijednost imovine reflektira interesom pravih investitora [48].

Oba problema koja je predstavio SEC ozbiljno dovode u pitanje legitimnost pametnih ugovora i decentraliziranih financija u sadašnjem obliku. Nedostatak transparentnosti kod projekta može izazvati sumnju da se radi Ponzijevoj shemi.

Ponzijeva shema je vrsta prevare koja obećava velike prinose na investiciju s malim rizikom. Radi na principu tako da isplati postojeće investitore sa sredstvima prikupljenih od novih investitora. Druga karakteristika Ponzijeve sheme su investicije koje nisu registrirane u državnim regulatorima [49].

Problem transparentnosti projekata moglo bi se riješiti registracijom i odobrenjem od državnog regulatora i njihovom objavom na internetskim stranicama državnog regulatora. Ovim bi se načinom promovirali legitimni projekti za investiranje čime bi se olakšalo proces donošenja odluka potencijalnim investitorima. Na temelju tih informacija korisnici mogu sami odlučiti kome će ukazati povjerenje i s kime će u budućnosti surađivati. Problemi s anonimnošću može se riješiti uvođenjem strožih uvjeta registracije i potvrde korisnika. Registracija korisnika mora djelovati na dva načina, jedan je način da se onemogući kreiranje više računa od jednog korisnika i drugi način je potvrda korisničkim računom putem mobilnog broja.

8.6. STAJALIŠTE PRAVNE STRUKE NA PAMETNE UGOVORE

Budući da će pametni ugovori sigurno donijeti promjene u pravnu struku, nužno je razumjeti njihovo stajalište prema novoj tehnologiji s kojom će morati u budućnosti rukovati. Bitno je uvažavati njihove sugestije jer oni najbolje mogu predvidjeti potencijalne probleme te analizirati njihova pozitivna stajališta i dobiti koju bi imali od korištenja nove tehnologije. Prikazat će se tri stajališta s tri razine, prva razina će biti međunarodna, druga će biti državna i treća će biti lokalna. Prvo će se prikazati stajalište Međunarodnog udruženja odvjetničkih komora.

Sigurno će doći do značajne promjene kako se obavlja pravni posao. Dugoročno gledano, određene će prakse postati automatizirane kao što su prijenosi, oporuke i registracija imanja. Odvjetnici koji se bave transakcijama morat će se pomiriti da se veliki dio posla koji oni obavljaju može automatizirati pametnim ugovorima. No, ovo nije kraj za odvjetnike zato što se automatizacija primjenjuje na obveze koje su repetitivne i zahtijevaju puno vremena za njihovo izvršenje. Korištenje pametnih ugovora imat će pozitivan učinak na odvjetnike jer će imati više vremena posvetiti se pravnim pitanjima. Zbog toga će odvjetnici moći uzeti veće portfelje poslova dok će algoritam izvršavati poslove s niskim rizikom i velikim volumenom. Posao koji je nekoć bio skup postat će isplativ. Odvjetnici će također morati naučiti nove vještine kako bi mogli zadovoljiti potražnju i interese svojih klijenata. Već postoji potražnja za odvjetnicima koji imaju vještine programiranja i kodiranja tako da ćemo vidjeti diplomirane pravnike koji imaju znanje iz STEM (engl. *Science Tehnology Engineering and Mathematics*) područja. Najvjerojatnije će odvjetnici s vještinama kodiranja postati sastavni dio prilikom sastavljanja ugovora po mjeri i njihove dubinske analize. Kako budu klijenti imali interakciju s blockchainom, nužni će im biti odvjetnici koji imaju potrebno znanje i stručnost u upravljanju s relevantnim pravnim kodeksima i regulatornim pitanjima. Odvjetnička će društva morati prihvatit nove tehnologije i inovacije kako bi ostale kompetitivne u dinamičnom tržištu i morat će zadovoljiti rastući interes i zahtjeve svojih klijenata [50].

Međunarodno udruženje odvjetničkih komora ne vidi pametne ugovore kao prijetnju za odvjetnike nego kao priliku da se odvjetnici rasterete od zamornih poslova te im pruža da povećaju svoj portfelj poslova. Također će im omogućiti da postanu profitabilniji što će imati za posljedicu zapošljavanje veće broja ljudi koji mogu obaviti veći opseg poslova što bi za klijente značilo niže cijene usluga.

Nakon upoznavanja s stavom koje ima jedno međunarodno udruženje objasnit će se državna razina na primjeru stava Američke odvjetničke komore.

Tehnologija pametnih ugovora je postigla značajna unapređenja, ali je još u ranim fazama razvoja. Problemi koji se moraju riješiti kako bi vidjeli širu primjenu pametnih ugovora su:

- Proširivost
- Rizici od centralizacije
- Uporabljivost.

Problem s proširivošću nastaje zbog toga što je tehnologija ovisna o brzini rada same mreže. Složene transakcije zahtijevaju veću brzinu rada mreže, a njima mogu pristupiti samo entiteti koji to mogu priuštiti. Rizik od centralizacije može se pojaviti ako je procesorska moć mreže koncentrirana na mali broj ljudi. Ako je grupa zlonamjerna, a ima većinu, oni se mogu dogovoriti da provode nezakonite i zlonamjerne transakcije. Budući da su pametni ugovori primarno napisani u kodu i nisu čitljivi za prosječnog odvjetnika, nužni su programi koji će olakšati njihovo pisanje i čitanje [51].

Rješenja za probleme s proširivošću i uporabljivosti već su obrazložena, ali nije rješenje za problem centralizacije. Problem centralizacije može se riješiti na dva načina. Prvi je način da država sklopi dogovor s više (što više to bolje jer će time blockchain biti sigurniji) vanjskih pružatelja infrastrukture koji će imati ravnopravni udio u mreži dok će država biti zadužena za održavanje i unapređenja mreže. Prednost je što država neće kontrolirati sve aspekte, infrastrukturu će održavati profesionalci dok će se država moći fokusirati na razvoj platforme. Nedostatak ovakvog rješenja je potencijalno udruženje vanjskih suradnika za izvođenje nezakonitih radnji i njihov nagli prestanka rada zbog izvanrednih situacija zbog čega će blockchaina biti manje sigurnijim. Drugo je rješenje da infrastruktura bude ravnopravno raspodijeljena na tri čvora između države, vanjskih pružatelja i opće populacije dok bi se validator bloka odabirao slučajnim odabirom. Prednost je ovog rješenja teže postizanje većine u uključene strane i povjerenje u sustav koji bi bio veći jer svi koji koriste sustav također sudjeluju u njegovom radu te će svima biti u cilju da sustav radi na što pravedniji način. Nedostatak ovog rješenja su veći troškovi vođenja sustava zbog ulaganja noviju opremu i potencijalno udruženje dviju strana da izvrše napad na mrežu. Na lokalnoj razini prikazat će se kakvo stajalište imaju sami odvjetnici na pametne ugovore. Izložit će se stajalište odvjetničke tvrtke Freshfields Bruckhaus Deringer sa sjedištem u Londonu i koja pripada među najstarije odvjetničke urede na svijetu.

Pametni ugovori dolaze i s nedostacima. Primjer, namjerna dvosmislenost nije moguća pa tako klauzule koje sadrže termine kao što su *dobra namjera, s najboljom namjerom* ili *u mjeri u kojoj je to moguće* ne mogu se implementirati u računalni kod i zbog toga ne mogu biti dio pametnih ugovora. Izazov s kojim će se morati baviti je ništetni ugovori jer jednom, kada je ugovor izvršen, on se ne može pravno poništiti. Stranke se mogu dogovoriti oko buduće transakcije koja će vratiti rezultat na početno stanje, ali će ništetna transakcija biti zabilježena na blockchainu. Najznačajniji

problem za odvjetnike bit će usklađivanje pravnog sloja, tj. dogovor između strankama s tehničkim slojem, odnosno rastavljanje dijelove dogovora računalnim kodom koristeći naredbu *if – else*. Ako ta dva sloja nisu ispravno usklađena, tada bi pametni ugovori mogli stvoriti više problema nego što bi ih riješili [52].

Nedostatak o namjernoj dvosmislenosti odnosi se na Contra proferentem pravilo, a ono je pravilo tumačenja ugovora prema kojemu se ugovorna odredba tumači u smislu koji je najpovoljniji za sugovaratelja osobe koja je sastavila ugovor. U Hrvatskom je zakonu to pravilo definirano Zakonom o zaštiti potrošača prema čl.54. st.1. prema kojem se *Dvojbene ili nerazumljive ugovorne odredbe tumače u smislu koji je povoljniji za potrošača* [53].

Dok je tumačenje spornih odredbi definirano Zakonom o obaveznim prema čl.319.st.2. gdje *Pri tumačenju spornih odredbi ne treba se držati doslovnog značenja pojedinih izričaja, već treba istraživati namjeru ugovaratelja i odredbu tako razumjeti kako to odgovara načelima obaveznog prava utvrđenim ovim Zakonom*, i čl.320.st.1 *U slučaju kad je ugovor sklopljen prema unaprijed otisnutom sadržaju, ili kad je ugovor na drugi način pripremila i predložila jedna ugovorna strana, nejasne odredbe tumačiti će se u korist druge strane.*[56].

Dok se pojave hibridni ugovori kod kojih se može umetnuti klauzule s namjernom dvosmislenošću treba primjenjivati tradicionalne ugovore za takvu vrstu klauzul.. Problem s ništetnim ugovorima može se riješiti tako da se stranke unaprijed dogovore oko rezervnog ugovora koji bi poništio prvotni ugovor u slučaju da on postane ništetan. Ovo se rješenje može primjenjivati dok se ne dođe do prihvatljivog rješenja koje će omogućiti poništavanje ugovora i brisanje s blockchaina. Usklađivanje pravnog i tehničkog dijela zahtijevat će vremena kako bi se došlo na željenu razinu. Brzog rješenja nema nego će se problemi rješavati u hodu.

9. ZAKLJUČAK

Blockchain tehnologija i pametni ugovori sigurno će promijeniti kreiranje, obrađivanje i korištenje podatke u budućnosti. Kao i svaka nova tehnologija ona dolazi sa svojim prednostima i nedostacima, rješava neke probleme, ali ne i sve prilikom sklapanja ugovora. Blockchain tehnologija još je u stanju razvoja i iz dana u dan napreduje te stalno dolaze novi projekti koji osiguraju višemilijunsko financiranje. Kako bude vrijeme prolazilo, tako će se vidjeti sve više proizvoda koje nam se nude, a baziraju se na blockchain tehnologiji. Nažalost postoje pojedinci i grupe koji koriste nove tehnologije kako bi izvodili prevare te stekli financijsku korist. U 2021. godini ukupna šteta koja je nastala zbog prevara povezanim s kriptovalutama koje koriste blockchain tehnologiju je iznosila 1.000,000.000 dolara. Stoga je bitno provesti kvalitetno istraživanje i konzultirati se sa stručnjacima koji imaju više iskustva u tome pri nego se uloži novac u željeni projekt. Nova tehnologija predstavlja prilika za sve one koji žele raditi s njom zato što postoji velika potreba za dobrim i kvalitetnim projektima. Vlade diljem svijeta rade na istraživanjima na temu blockchain tehnologije te bi se u skorašnje vrijeme mogli vidjeti prijedlozi za njenu regulaciju.

Pametni su ugovori još u ranom stanju razvoja. Iako se zovu *pametnim* ugovorima, oni to zapravo nisu jer se radi o računalnim programima koji su *pametni* onoliko koliko i osoba koja ih je programirala. Oni se trenutačno koriste za jednostavne transakcije kao što je prijenos vrijednosti s jednog računa na drugi u decentraliziranim financijama. Njihovo korištenje zna biti skupo zbog toga što Ethereum blockchain na kojem se izvode koristi konsenzusni mehanizam PoW i Sloj 1 blockchain. Taj se nedostatak planira riješiti prelaženjem na konsenzusni mehanizam PoS i Sloj 2 blockchain. Korištenjem konsenzusnog mehanizma PoS planira se smanjiti potrošnja struje za 99.95 posto. Ovo je ozbiljan energetski problem zato što je Ethereum blockchain u jednom trenutku trošio struje u iznosu od 112 teravatsati za usporedbu toliku potrošnju struje ima Nizozemska koja prema zadnjem popisu stanovništva ima 17 440 000 stanovnika. Prelazak na Sloj 2 blockchain bi riješio problem skupih transakcija i povećao bi broj transakcija u satu. Pravni izazovi su zahtjevniji za rješavanje jer svaka država ima svoja zakonska rješenja. Pravna rješenja za pametne ugovore su u procesu istraživanja. Ako pametni ugovori postanu pravno obvezujući ugovori, treba očekivati da će se koristiti u situacijama koje su jako jednostavne za prenošenje u računalni kod. Pametni

ugovori neće ugroziti radna mjesta odvjetnika i posrednika nego će im pomoći da automatiziraju dio poslova koji im nisu bili dovoljno profitabilni te im omogućiti da postanu produktivniji i profitabilniji. Mogućnosti pametnih ugovora nisu još istražene, ali je sigurno da će se njihovim korištenjem povećati transparentnost, sigurnost i brzina prilikom sklapanja ugovora.

LITERATURA I POPIS PROPISA S IZVORIMA

[1] Bashir I. Mastering Blockchain *Second Edition* Distributed ledger technology, decentralization, and smart contracts explained. London: Packt Publishin; 2018 [Pristupljeno: lipanj 2021]

[2] National Archives and Records Administration. Blockchain White Paper, Maryland, 2019. Preuzeto sa: https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf [Pristupljeno: liapnj 2021]

[3] lamport L, Shostak R, Pease M. The Byzantine Generals Problem. ACM Transactions on Programming Languages and System. 1982;4(3):382-401. [Pristupljeno: Lipanj 2021]

[4] Hozjan, D. (2017) *Blockchain*. Diplomski rad. Zagreb: Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet [Pristupljeno: lipanj 2021]

[5] Antonopoulos A.M. Mastering Bitcoin Unlocking Digital Crypto - Currencies . Sebastopol: O'Reilly; 2015 [Pristupljeno: Srpanj 2021]

[6] J. Golosova and A. Romanovs. The Advantages and Disadvantages of the Blockchain Technology. 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018, pp. 1-6, doi: 10.1109/AIEEE.2018.8592253. https://www.researchgate.net/publication/330028734_The_Advantages_and_Disadvantages_of_the_Blockchain_Technology

[7] Solomakha S., Blockchain – Hot or Not?, (2021), Softengi. https://softengi.com/blog/blockchain-hot-or-not/ [Pristupljeno: Kolovoz 2021]

[8] Hands J., Mining vs. Farming, the Dana Behind Being Green, (2021),Chia.net . Preuzeto sa: https://www.chia.net/2021/10/20/mining-vs-farming.en.html[Pristupljeno: kolovoz 2021]

[9] Iredale G., Top Disadvantages of Blockchain Tehnology, (2020), 101blockchains.com. Preuzeto sa: https://101blockchains.com/disadvantages-of-blockchain/ [Pristupljeno: kolovoz 2021]

[10] Walenza E., 51% Attack, (2022), Iotone.com, Preuzeto sa: https://www.iotone.com/term/51-attack/t762 [Pristupljeno: rujan 2021]

[11] Walenza E., Double Spending, (2022), Iotone.com, Preuzeto sa: https://www.iotone.com/term/double-spending/t779 [Pristupljeno: rujan 2021]

[12] CARNet CERT, DDoS napad, 2008, Cis.hr, Preuzeto sa: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-09-240.pdf [Pristupljeno: Rujan 2021]

[13] Longchamp Y., Are blockhains that safe? How to attack and prevent attacks, (2020), Seba swiss. Preuzeto sa: https://www.seba.swiss/research/are-blockchains-safe-how-to-attack-them-and-prevent-attacks [Pristupljeno: rujan 2021]

[14] Kumar N, Aggarwal S, Raj P. Advances in Computers Volume123. The Blockchain Technology for Secure and Smart Applications across Industry Verticals. 2021;121(1);399-410.

[15] Keselj M. (2015) Bitcoin. Diplomski rad. Osijek. Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku [Pristupljeno: rujan 2021]

[16] Radošević S. (2018) Bitcoin algoritam. Diplomski rad. Osijek. Sveučilište Josipa Jurja Strossmayera u Osijeku. Fakultet elektrotehnike, računarstva i informacijskih tehnologija [Pristupljeno: rujan 2021]

[17] Eshmadeva, AMD Ryzen 9 3900x CPU in AM4 socket close up, (2020), Dreamtime.com, Preuzeto sa: https://www.dreamstime.com/photos-images/amd-ryzen.html [Pristupljeno: studeni 2021]

[18] Nana Dua, RTX vs GTX Seson One Episode One, (2020), Unsplash.com, Preuzeto sa: https://unsplash.com/s/photos/graphics-card [Pristupljeno: studeni 2021]

[19] mandjelo, Field – programmable Gate Array Xilinx Electronics Micron Technology Flash Memory PNG, (2018), IMGBIN.com, Preuzeto sa: https://imgbin.com/png/ZRS6thMR/field-programmable-gate-array-xilinx-electronics-micron-technology-flash-memory-png [Pristupljeno: studeni 2021]

[20] Alexlmx, ASIC miner 3D rendering isolated on white background, (2021), Dreamstime.com Preuzeto sa: https://www.dreamstime.com/asic-miner-d-rendering-isolated-white-background-image210827359[Pristupljeno: studeni 2021]

[21] Antonopoulos A.M, Wood Dr.Gavin. Mastering Ethereum Building Smart Contracts and DApps. Sebastopol. O'Reilly: 2019 [Pristupljeno: Studeni 2021]

[22] Juviler J., What is GitHub? (And What Is It Used For?), (2021), blog.hubspot.com. Preuzeto sa : https://blog.hubspot.com/website/what-is-github-used-for [Pristupljeno: travanj 2022]

[23] chrome.google.com. Preuzeto sa: https://chrome.google.com/webstore/search/metamask?hl=en [Pristupljeno: travanj 2022]

[24] chrome.google.com. Preuzeto sa: https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn?hl=en [Pristupljeno: travanj 2022]

[25] Cross T., The Morden proof-of-work testnet for Ethereum Classic, (2021), github.com Preuzeto sa: https://github.com/eth-classic/morden [Pristupljeno: svibanj 2022]

[26] Red Hat, What is an IDE, (2019), redhat.com. Preuzeto sa: https://www.redhat.com/en/topics/middleware/what-is-ide [Pristupljeno: svibanj 2022]

[27] remix-ide.readthedocs.io. Preuzeto sa: https://remix-ide.readthedocs.io/en/latest/ [Pristupljeno: svibanj 2022]

[28] remix.ethereum.org Preuzeto sa: https://remix.ethereum.org/ [Pristupljeno: svibanj 2022]

[29] Law Commission, Smart legal Contracts Summary, 2021, s3-eu-west-2.amazonaws.com, Preuzeto sa: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/6.7776_LC_Smart_Legal_Contracts_2021_Final.pdf [Pristupljeno: svibanj 2022]

[30] ethereum.org, Decentralized autonomous organizatio (DAOs), (2022), ethereum.org. Preuzeto sa: https://ethereum.org/en/dao/ [Pristupljeno: svibanj 2022]

[31] SIMBA CHAIN, What are the Three Types of Smart Contracts?, (2021), Blog.simbachain.com. Preuzeto sa: https://blog.simbachain.com/blog/types-of-smart-contracts [Pristupljeno: svibanj 2022]

[32] Zheng Z, Xie S, Dai H-Ning, Chen W, Chen X, Weng J, Imran M. An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems. 2020;105(1): 475-491.

[33] Grasso A., Smart Contracts: Real-Life Use Cases, (2019), ResearchGate.net. Preuzeto sa: https://www.researchgate.net/publication/343152377_Smart_Contracts_Real-Life_Use_Cases [Pristupljeno: svibanj 2022]

[34] Mohanta B.Kumar., An Overview of Smart Contracts and Use Cases in Blockchain Techology, (2018), ResearchGate.net Preuzeto sa: https://www.researchgate.net/publication/328581609_An_Overview_of_Smart_Contract_and_Use_Cases_in_Blockchain_Technology [Pristupljeno: svibanj 2022]

[35] IBM, What is blockchain technology?, (2019), ibm.com. Preuzeto sa: https://www.ibm.com/topics/what-is-blockchain [Pristupljeno: ožujak 2022]

[36] Douglas J., INTRO TO ETHEREUM, (2022), ethereum.org Preuzeto sa: https://ethereum.org/en/developers/docs/intro-to-ethereum/#what-is-a-blockchain [Pristupljeno: ožujak 2022]

[37] Organzation for Economic Co-operation and Development, OECD Blockchain Primer, (2022), oecd.org. Preuzeto sa: https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf [Pristupljeno: ožujak 2022]

[38] Sultan K, Ruhi U, Lakhani R. CONCEPTUALIZING BLOCKCHAINS: CHARACTERISTICS & APPLICATIONS. 11th IADIS International Conference Information Systems 2018, University of Ottawa, Canada, 2018

[39] Zoltu M., INTRDUCTION TO SMART CONTRACTS, (2022), ethereum.org. Preuzeto sa: https://ethereum.org/en/developers/docs/smart-contracts/ [Pristupljeno: ožujak 2022]

[40] Law Commission, Smart contracts, (2021), lawcom.gov.uk. Preuzeto sa: https://www.lawcom.gov.uk/project/smart-contracts/ [Pristupljeno: ožujak 2022]

[41] National Archives and Records Administration. Blockchain White Paper, Maryland, 2019. Preuzeto sa: https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf [Pristupljeno: travanj 2022]

[42] Dangi S. Are Smart Contracts the Future of Contracts ?. PM World Jurnal. 2019;8(9):10-11. Preuzeto sa: https://pmworldlibrary.net/wp-content/uploads/2019/10/pmwj86-Oct2019-Dangli-are-smart-contracts-the-future-of-contracts.pdf [Pristupljeno: 10.6.2022]

[43] ethereum.org., Ethereum for everyone Scaling Ethereum without compromising on security or decentralization, (2022)ethereum.org Preuzeto sa: https://ethereum.org/en/layer-2/ [Pristupljeno: lipanj 2022]

[44] Boissay F, Cornelli G, Doerr S, Frost J. Blockchain scalability and the fragmentation of crypto, BIS Bulletin No 56, Basel, 2022., p. 2-4. Preuzeto sa: https://www.bis.org/publ/bisbull56.pdf [Pristupljeno: 14.6.2022]

[45] Smith C., SCALING, (2022), ethereum.org. Preuzeto sa: https://ethereum.org/en/developers/docs/scaling/

[46] THE EUROPEAN UNION BLOCKHAIN OBSERVATORY AND FORUM. Legal and regulatory framework of blockchains and smart contracts, Pariz, 2019. Preuzeto sa: https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf [Pristupljeno: lipanj 2022]

[47] Law Commission., About us, (2022), lawcom.gov.uk. Preuzeto sa: https://www.lawcom.gov.uk/about/ [Pristupljeno: lipanj 2022]

[48] Artzt Dr.M, Hsu L, D.Palley S, Luis Sombra T, Tinianow A, Van Der Laan J, D.Weingarten G. THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW. 2021; 1: 4-11 [Pristupljeno: lipanj 2022]

[49] U.S. SECURITIES AND EXCHANGE COMMISSION., Ponzi Scheme, (2022), investor.gov. Preuzeto sa: https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme [Pristupljeno: lipanj 2022]

[50] Sherborne A. Blockchain, Smart Contracts and Lawyers. Internacional Bar Association. 2017 Preuzeto sa: https://theblockchaintest.com/uploads/resources/International%20Bar%20Association%20%20Blockchain%20smart%20contracts%20and%20lawyers%20-%202017%20-%20Dec.pdf [Pristupljeno: lipanj 2022]

[51] Tsui S. Ng., Blockchain and Beyond: Smart Contracts, (2017), americanbar.org. Preuzeto sa: https://www.americanbar.org/groups/business_law/publications/blt/2017/09/09_ng/ [Pristupljeno: lipanj 2022]

[52] Fritz G., What's in a smart contract?, (2022), freshfields.com. Preuzeto sa: https://www.freshfields.com/en-gb/our-thinking/campaigns/technology-quotient/fintech/whats-in/whats-in-a-smart-contract/ [Pristupljeno: lipanj 2022]

[53] struna.ihjj.hr. Preuzeto sa: http://struna.ihjj.hr/naziv/lt-i-gt-contra-proferentem-lt-i-gt-pravilo/9531/ [Pristupljeno: lipanj 2022]

[54] Domazet N., U EU raste strah od nestašica električne energije, (2022), energetika-net.com Preuzeto sa: http://www.energetika-net.com/vijesti/energetsko-gospodarstvo/u-eu-raste-strah-od-nestasica-elektricne-energije-35086 [Pristupljeno: rujan 2022]

[55] Vojković, G. (2022) Electronic Office Management of Public Administration in Croatia. U: Skala. K,ur. MIPRO 2022 45th Jubilee International Convention Proceedings. Rijeka: MIPRO, 1387-1391.

[56] Zakon o obaveznim odnosima (pročišćeni tekst, Narodne novine, br. 126/21).

Popis kratica

ABI (Application Binary Interface) aplikacijsko binarno sučelje

ASIC (Application Specific Integrated Circuit) integrirani krugovi za specifičnu primjenu

CA (Contract Accounts) ugovorni račun

DAO (Decentralized autonomous organizations) Decentralizirane autonomne organizacije

DPoS (Delegated Proof of Stake) Delegirani dokaz udjela

ECDSA (Elliptic Curve Digital Signature Algorithm) algoritam za digitalni potpis poruke koji koristi eliptične krivulje i njihova svojstva

eIDAS (electronic Identification Authentication and Signature) elektronička identifikacija i usluge povjerenja

EOA (Externally Owned Accounts) računi u vanjskom vlasništuvu

EVM (Ethereum virtual machina) Ethereum virtualni stroj

FPGA (Field Programmable Gate Array) programabilna polja logičkih sklopova

IBM (Internacional Business Machines) Međunarodni poslovni strojevi

IDE (Integrated Development Environments) integrirano razvojno okruženje

IoT (Internet of Things) Internet stvari

LLL (Lisp Like Language) jezik poput Lisp

NARA (National Archives and Records Administration) Državni arhiv i uprava za evidencije

NASAA (North American Securities Administrators Association) sjevernoamerička udruga upravitelja vrijednosnih papira

NFT (Non-fungible token) nezamjenjivi token

OECD (Organization fro Economic Co-operation and Development) Organizacija za ekonomsku suradnju i razvoj

PoA (Proof of Authority) dokaz autoriteta

PoS (Proof of Space) dokaz o prostoru

PoS (Proof of Stake) dokaz udjela

PoW (Proof of Work) dokaz o radu

ROM (Read Only Memory) memorija samo za čitanje

RPC (Remote Procedure Call) poziv udaljene procedure

SEC (Securities and Exchange Commission) Američka komisija za reguliranje i trgovinu vrijednosnim papirima

SHA (Secure Hash Algoritam) algoritam za sigurno hashiranje

STEM (Science, Tehnology, Engineering and Mathematics) znanost tehnologija inžinjerstvo i matematika

SQL (Structured Query Language) strukturirani upitni jezik

TSP (Trust Service Providers) Pružatelji usluga povjerenja

WIF (Wallet Import Fromat) format za unos novčanika

Popis korištenih slika

Popis korištenih tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Tehnološki i pravni izazovi pametnih ugovora , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 14.9.2022.

Vladimir Babić
(ime i prezime, *potpis*)