Kreiranje kriptovalute korišćenjem blockchain tehnologije

VASILJE M. CVIJIC, Univerzitet Adriatik, Bar,

Fakultet za saobraćaj, komunikacije i logistiku, Budva, Crna Gora

NATAŠA GOSPIĆ, Univerzitet Adriatik, Bar,

Fakultet za saobraćaj, komunikacije i logistiku, Budva, Crna Gora

Pregledni rad

UDC: 336.7:004

DOI: DOI: 10.5937/tehnika2105655C

Glavni nosilac kriptovalutnog sistema je blockchain. Rad će pojasniti razlike između token-a i coin-a, ulogu rudara u kriptovalutnom sistemu, fork-ove, kako se postiže konsenzus mehanizam. Takođe će se diskutovati protokoli koji su u upotrebi. Zbog tehničkih sličnosti, urađena je komparacija blockchain-a s Bitcoin-om, koji pruža odličnu referentnu tačku. U radu se daje i prikaz praktične primjene blockchain-a u vidu pametnih ugovora. Rad će pružiti predlog faza razvoja sopstvene kripto valute, od samog početka, gdje se definiše svrha postojanja, kroz odabire tehničkih rješenja, pa sve do finalizacije gdje presudnu ulogu za uspjeh igraju marketing i komercijalni aspekti, uz smjernice za pridržavanje pravnih aspekata.

Ključne riječi: blockchain, konsenzus, pametni ugovori, nodovi, wallet

1. UVOD

Broj korisnika koji vide budućnost u kriptovalutama je u konstantnom porastu. Do septembra 2020. broj korisnika wallet-a (novčanika) blockchain-a porastao je na više od 50 miliona, prema istraživanju koje je objavila „Statista“-a [1] Bitcoin ima više od 70 miliona aktivnih korisnika. Različite vrste kriptovaluta generalno spadaju u jednu od dvije kategorije: koini ili tokeni. Do aprila 2021. godine postojalo je više od 10.000 različitih vrsta kriptovaluta.

Cilj ovog rada je da pruži jasniji uvid u svrhe postojanja i principe funkcionisanja kripto valuta, radi jednostavnijeg razlikovanja različitih vrsta i namjena kriptovaluta. Blockchain je termin koji se koristi za knjigu transakcija koje su podijeljene u blokove, koji su lančano i hronološki vezani. Blockchain se direktno oslanja na konsenzus mehanizam, i on je najvažniji parametar u ovoj tehnologiji. Odabir konsenzus mehanizma direktno utiče na dizajn nodova, potrošnju energije, memorije, aritmetičko logičke i ostale resurse. Kad je riječ o tehničkim aspektima, pored odabira konsenzus mehanizma, važan je odabir željenje blockchain platforme, a time i dizajn nodova, utemeljenje unu-

trašnje strukture blockchain-a, izrada API-ja, dizajn wallet-a i dizajn interfejsa, koji će biti obrađeni u daljem tekstu.

2. DEFINISANJE KRIPTOVALUTE

Kriptovaluta je decentralizovani, enkriptovani niz podataka koji označava novčanu jedinicu. Prati ga i organizuje P2P (peer-to-peer) mreža koja je poznata pod nazivom blockchain. Za razliku od fizičkog novca, kriptovalute su decentralizovane, što znači da ih ne izdaju vlade ili druge finansijske institucije.

Kriptovalute se stvaraju (i osiguravaju) pomoću kriptografskih algoritama koji se održavaju i potvrđuju u procesu koji se naziva rudarenje (eng. mining), gdje mreža računara ili specijalizovani hardver, poput integralnih kola za specifične za aplikacije (Application-Specific Integrated Circuits ASIC), obrađuju i potvrđuju transakcije. Proces stimuliše rudare koji vode mrežu s kriptovalutom, tako što im daje nagrade u malim iznosima kriptovalute.

Neke od poznatih kriptovaluta su: Bitcoin, Ethereum, Litecoin, Tether i Monero.

Kriptovaluta je postala oblik plaćanja koji se može online razmijeniti za robu i usluge. Mnoge kompanije su izdale vlastite valute, koje se često nazivaju tokenima, a njima se može trgovati isključivo za robu ili usluge koje ta kompanija pruža. Mogu se zamisliti kao čipovi za kazino. To zahtjeva da se zamijeni stvarna valuta (novac), za kriptovalutne token-e kako bi njima platili robu ili usluge.

Adresa autora: Vasilje Cvijic, Univerzitet Adriatik, Bar, Fakultet za saobraćaj, komunikacije i logistiku, Budva, Žrtava fašizma 56, Crna Gora

e-mail: vasiljecvijic@gmail.com

Rad primljen: 28.09.2021.

Rad prihvaćen: 08.10.2021.

Kriptovalute su pravi proizvod digitalnog doba, i postoje bez učešća banaka, vlada ili bilo kojeg posrednika. Međutim, u većini slučajeva za kupovinu i prodaju digitalne imovine mora se koristiti berza za razmjenu digitalnih valuta. Ono što pruža bezbjednost jeste da su kriptovalute enkriptovane specijalizovanim računarskim kodiranjem koji se naziva kriptografija. Namjerno su dizajnirane kao komplikovana zagonetka tako da ih je teško razbiti odnosno hakovati. Različite vrste kriptovaluta generalno spadaju u jednu od dvije kategorije: koini ili tTokeni

3. TIPOVI TEHNOLOGIJA KOJI SE KORISTE ZA KRIPTOVALUTE

Kao što je rečeno, kriptovalute rade utemeljene na tehnologiji koja se naziva blockchain.

Blockchain protokol je skup:

- determinističko logičkih pravila;
- kriptografije i enkripcije kao osnov za bezbjednost;

Sem blockchain-a, koji predstavlja knjigu transakcija, za funkcionisanje kriptovalute, ključan je odabir konsenzusnog mehanizma. Konsenzus je sporazum koji zadovoljava svaku od uključenih strana. Ovo je ključ demokratije i decentralizacije uopšte, a posebno tehnologije distribuiranog registra. Na primjer iako je [2] Satoshi Nakamoto njegov misteriozni osnivač, on (ili ona) nema moć nad zajednicom.

U užem smislu, koji se koristi u kriptografiji, konsenzus je postupak donošenja odluka. Njegov cilj je osigurati da se svi učesnici na mreži slože o svom trenutnom statusu nakon dodavanja novih informacija, bloka podataka ili grupe transakcija. Drugim riječima, protokol konsenzusa osigurava da je lanac ispravan i daje podsticaj da ostanu poštenu učesnici. Ovo je važna struktura za spriječavanje situacije u kojoj neko sam kontroliše cio sistem i osigurava da se svi pridržavaju pravila mreže.

Zastupljeni protokoli konsenzusnih mehanizama su:

- Dokaz o radu (PoW - Proof of Work),
- Dokaz o ulogu (PoS - Proof of Stake),
- Delegirani dokaz o ulogu (DPoS - Delegated Proof of Stake),
- Dokaz o aktivnosti (PoA - Proof of Activity),
- Dokaz lokacije (PoL - Proof of Location),
- Dokaz o važnosti (PoI - Proof of Importance),
- Dokaz o proteklom vremenu (PoET - Proof of Elapsed Time),
- Dokaz o ovlaštenju (PoA - Proof of Authority),
- Dokaz o sagorevanju (PoB - Proof of Burn),
- Dokaz kapaciteta (PoC - Proof of Capacity) ili dokaz prostora (PoS - Proof of Space),

- Dokaz o ulozenom vremenu (PoST - Proof of Stake Time),
- Dokaz mozga (Proof of Brain),
- Dokaz fizičke adrese (PoPA - Proof of Physical Address) / Dokaz bankovnog naloga (PoBA - Proof of Bank Account).

U radu će se detaljnije dati protokoli PoW, PoS i PoSt. PoW i PoS su najzastupljeniji, a značaj PoSt-a je u kompromisu koji pruža.

4. DEFINISANJE BLOCKCHAIN-A

Blockchain je decentralizovana tehnologija rasprostranjena na mnogim računarima koja upravlja i bilježi transakcije. Bitan aspekt koji privlači korisnike ove tehnologije je i njena bezbjednost.

„Blockchain“, tehnologija vođenja evidencije stoji i iza Bitcoin mreže, kao i mreža mnogih drugih kriptovaluta).

Blockchain je specifična vrsta baze podataka. Razlikuje se od tipične baze podataka po načinu na koji čuva informacije. Blockchain skladišti podatke u blokovima koji su zatim povezani lancima. Kako novi podaci pristižu, oni se unose u novi blok. Jednom kada se blok napuni podacima, on se „lančano“ vezuje za prethodni blok, što čini podatke lančano sortiranim zajedno, u definisanom hronološkom redoslijedu. Na blockchain-u se mogu čuvati različite vrste informacija, ali najčešća upotreba do sada bila je u vidu „knjige za transakcije“.

Bitcoin, kao i blockchain, potpuno je transparentan i otvoren, a svako čvorište (eng. node) je u ovoj mreži jednako ravnopravno.

U slučaju Bitcoin-a, blockchain se koristi na decentralizovan način tako da nijedna osoba ili grupa nemaju kontrolu - već svi korisnici kolektivno zadržavaju kontrolu.

Decentralizovani blockchain-i su nepromenljivi, što znači da su unijeti podaci nepovratni. Za Bitcoin to znači da su transakcije trajno evidentirane i svima vidljive.

4.1. Struktura skladišta

Poređenje dato u [3] jasno oslikava razliku između blockchain-a i baze podataka. Baza podataka svoje podatke strukturira u tabele, dok blockchain, kao što mu i samo ime kaže, strukturira svoje podatke u djelove (blokove) koji su povezani lančano. To čini tako da su svi blockchain-i baze podataka, ali nisu sve baze podataka blockchain-i. Blokovi imaju određene kapacitete za skladištenje i kada se napune lančano se vežu za prethodno ispunjeni blok, čineći lanac podataka poznat kao „block-chain“. Sve nove informacije će biti dodate u novi blok koji će se takođe dodati lancu kada se popuni.

Ovaj sistem takođe inherentno čini nepovratan vremenski okvir podataka kada se primenjuje u decentralizovanoj prirodi. Kad se blok napuni, postavlja se fiksirano u vremenskoj liniji. Svaki blok u lancu dobija tačnu vremensku oznaku kada se doda u lanac.

Osim kao nosioc kriptovalutnih coin-a, blockchain tehnologija može služiti kao platforma za pametne ugovore. Pametni ugovor je jedna od kriptovalutnih formi, koja nije ugovor u pravnom smislu, već program koji se izvodi na blockchain-u. Pametni ugovor je ugovor koji se samostalno izvršava, a uslovi ugovora između kupca i prodavca su direktno zapisani u redove koda. Pametni ugovori imaju dvije bitne karakteristike: mogu primati i slati transakcije i nepromjenjivi su. Praktični primjeri pametnih ugovora u svijetu digitalne umjetnosti su u vidu NFT (Non fungible token), gdje se dokaz prava svojine nad određenom umjetninom dokazuje istim. U slučaju promjene vlasništva, vrši se transfer NFT-a. U zdravstvu bi bilo moguće objediniti decentralizovanu bazu za COVID pasoše, te bi se u svega nekoliko sekundi, skeniranjem QR koda mogla utvrditi vjerodostojnost potvrda. U transportnoj industriji, je moguće pratiti putanju proizvoda, od proizvođača do krajnjih potrošača. Ovo je posebno značajno u prehrambenoj industriji, gdje u slučaju neispravnosti, može brzo biti utvrđeno u kom skladištu su sve boravili proizvodi. Automobilaska industrija bi mogla ostvariti benefite, obilježavanjem bitnijih komponenti vozila QR kodovima, koji bi imali aritmetičku povezanost s čeksumom identifikacijskog broja vozila (Vehicle Identification Number - VIN). U slučajevima krađe vozila i prodaje komponenti na crnom tržištu, s lakoćom bi se utvrdilo da iste potiču s ukradenog vozila. Ovo direktno destimuliše krađu vozila, i podstiče veći profit proizvođača, koji prodaju nove automobilske djelove.

5. PREDLOG RAZVOJA KRIPTOVALTE

U procesu kreiranja nove kriptovalute, potrebno je uraditi sljedeće:

- Definirati svrhu razvoja predmetne kriptovalute, kao i način „brendiranja“.
- Definirati odgovarajuće tehničke protokole po kojima će funkcionisati.
- Definirati zahtjevani nivo bezbjednosti kriptovalute.
- Odlučiti da li će funkcionisati kao koin ili kao token.
- Riješiti i definisati pravne aspekte.
- Prikupiti investitore (moguće i kroz Initial Coin Offering - ICO i/ili Initial Exchange Offering - IEO), „lansiranje“ proizvoda,
- Razrada kriptovalute u komercijalnom i ekonomskom aspektu.

5.1. Definisanje svrhe postojanja

Identifikovanjem problema ili neispunjenog zahtjeva na tržištu i stvara se prostor za kreiranje nove kriptovalute. Važno je napomenuti da većina kriptovaluta nema suštinsku vrijednost i da ih ne podržava nijedna državna institucija. Njihova novčana vrijednost dolazi od ljudi koji ih osnažuju. Što se tiče ljudi koji profesionalno finansijski ulažu u kriptovalute, razlikujemo dvije glavne vrste: investitore i špekulante. Da bi kriptovaluta komercijalno osnažila, adekvatnim brendiranjem i marketing kampanjama je neophodno privući korisnike spremne da ulože novac u istu.

5.2. Definisanje tehničkih protokola

Preporuka je da se koriste open source rješenja, jer pružaju veći stepen povjerenja i korisnicima, i potencijalnim investitorima. Postoji više opcija. Moguće je preuzeti postojeća rješenja, kao jedna opcija. Kao druga opcija može biti postojeće rješenje koje se nadograđuje (jeftinija opcija), i treća opcija je kreiranje sopstvene (skuplja opcija). U daljem tekstu za tehničko rješenje diskutovana je treća opcija. Za ovu opciju potrebno je:

- Odabrati željeni konsenzus mehanizam
- Odabrati željenu blockchain platformu
- Dizajnirati node-ove
- Utemeljiti unutrašnju strukturu blockchain-a
- Definirati API-je (Application Program Interface)
- Kreirati sistem wallet-a za korisnike
- Dizajnirati interfejs

5.3. Izbor konsenzus mehanizama

Najzastupljeniji protokoli konsenzus mehanizama su: PoW i PoS. Obzirom da PoW algoritam vrši preveliku potrošnju električne energije, da PoS algoritam ima problem monopola, budućnost je u hibridnim rješenjima, kao što je PoSt.

PoSt se razlikuje po tome što omogućuje učesnicima mreže da pokažu kako su skladištili podatke tokom određenog vremenskog perioda. Isto se dokazuje tako što će nasumično odabrani rudari biti odabrani i njihovi će se podaci pročitati radi provjere. Prema tvorcima, Talu Moranu i Ilanu Orlovu [3], to se naziva „racionalnim dokazima prostora i vremena“ jer su stvarni troškovi skladištenja proporcionalni proizvodu skladišnog kapaciteta i vremena koje je podatak bio uskladišten. Imajući u vidu analizu iz [4] ukratko se može reći da je PoSt povoljnije rešenje u odnosu na PoW, jer je otporan na ASIC (Application Specific Integrated Circuits), pa u rudarenju može da učestvuje bilo ko, ima manju potrošnju električne energije, dosljedna vremena bloka transakcija i manje je podložan zlonamjernim rudarskim napadima. I ovaj protokol ima svoje nedostatke. Hardver je opšte namjene, te se napadači mogu prebacivati između: rudarenja,

napadanja i korištenja za skladištenje podataka, što povećava broj napadača. Takođe je i veća složenost zbog podslotova i VDF (Verifiable Delay Function).

Ako se izvrši poređenje PoSt i PoS dolazi se do sljedećih zaključaka [5]. Prednosti PoSt u odnosu na PoS su:

- Napadač može prenijeti svoj ulog na nekoga drugog, ali račva lanac neposredno prije nego što se njegov ulog prenese. U ovom alternativnom lancu napadač još uvijek ima sav svoj ulog pa može nastaviti lanac. Situacija „ništa se ne rizikuje“ razlikuje se u PoS-u jer stvaranje PoSt-a zahtijeva fizički resurs (memoriju na disku), dok je za stvaranje PoS-a potreban samo ključ.
- Napadač može zagarantovati svoj udio, ulažući svoje nagrade (bogati postaju bogatiji), budući da je ukupan broj coin-a ograničen.
- Mogu postojati situacije u kojima napadač može usitniti različite načine prenosa udjela.
- Nije potrebna registracija, a u PoS se ne može se učestvovati bez prijave, što povećava privatnost.

Kod PoSt postoji veća prepreka za ulazak. Sigurnosni depoziti i slashing otežavaju učešće manjih korisnika. PoS mehanizam može oduzeti ulog od korisnika, kako bi kaznio neočekivana ponašanja rudara na nodovima, dok PoSt ima manju kaznenu efikasnost, jer bi se hard diskovi u slučaju slashing-a mogli koristiti u druge svrhe. [5]

Iako najsloženiji, PoSt pruža najbolji kompromis, i ima perspektivu da se daljim razvijanjem i usvajanjem unaprijedi.

5.4. Razvoj API-ja

Application Program Interface - API će omogućiti interkonekciju kreirane kriptovalute s raznim platformama, aplikacijama uz pojednostavljenje razmjene podataka. Neke blockchain platforme dolaze s unaprijed izrađenim API-jima, dok neke ne. Glavne karakteristike API -ja potrebne u kreiranju kriptovalute su:

- Generisanje parova ključeva i adresa
 - Obavljanje funkcija vezanih za reviziju
 - Autentifikacija podataka kroz digitalne potpise i hešve
 - Skladištenje i povratak podataka
 - Upravljanje životnim ciklusom pametne imovine: izdavanje, plaćanje, razmjena, escrow i arhiviranje
 - Pametni ugovori
- Izabran API treba da:
- Na jednostavan način omogući web stranicama da primaju plaćanja u Bitcoin-u.
 - Pruži uslugu wallet-a povezanu s blockchain-om
 - Pruži API-je za primanje i plaćanje iz samog blockchain novčanika

- Podrži JSON (JavaScript Object Notation) za zahtjeve podataka po bloku i transakciji
- Podrži web socket-e: streaming socket s niskom latencijom, koji pružaju podatke o novim blokovima i transakcijama.

Iz navedenog proističe da u slučaju razvoja sopstvene blockchain platforme, neophodno je razviti i odgovarajuće API-je. Glavni fokus mora biti na omogućenju interkonekcije s platformama, radi efikasnije primjene koja srazmjerno pruža bolje šanse komercijalnog uspjeha.

5.5. Kreiranje sistema wallet (novčanika) kriptovalute:

U ovom procesu neophodno je da se konfiguriše API novčanika za upravljanje dozvolama za koje se kod može dobiti sa platformi poput GitHub -a. Nadalje, postavlja se lozinka za novčanik koju ne treba dijeliti ni sa kim, kao i postavljeni privatni ključ.

Nakon toga se generiše nova adresa novčanika, testira korisnički interfejs i ostavljaju na čuvanje određena sredstva.

Sljedeći postupci se predlažu u slučaju kreiranja sopstvenog wallet-a:

- Koristiti gotove template.
- Koristiti standardne open source biblioteke poput Chain-Java.
- Instalirati API sa web lokacije.
- Navesti naziv novčanika i podesiti dozvole za transakcije.
- Izabrati programe i integrisati ih u wallet.
- Napisati kod i integrisati ga u svoju bazu podataka.
- Dizajnirati korisnički interfejs.
- Obaviti testiranje prije zvaničnog pokretanja wallet-a.

6. PRAVNI ASPEKTI

Usled nedostatka centralnog autoriteta koji vodi računa o svim korisnicima, kao i usled značajno većeg stepena slobode i anonimnosti koje kriptovalute pružaju, pojam kriptovaluta je često bio vezane i za ilegalne transakcije.

Osim ilegalnih trgovina na Dark Web-u, kriptovalute mogu biti zloupotrijebljene za globalne transakcije većih količina prljavog novca van kontrola vlada, pranje novca, finansiranje terorizma, i razne druge oblike ilegalnih aktivnosti.

Jedno od prva načela prava je: „Sve što zakonom nije izričito zabranjeno, smatra se dozvoljenim i legalnim“. Otuda i potreba da se uvedu „pravne stege“ i koliko-toliko nametnu pravila, propisi i prakse u ovoj oblasti.

Potrebno je razumjeti da razne zemlje svijeta, ima-

ju različite stavove o kriptovalutama, i da iz tih stavova proizilaze i različiti pravni propisi. Nije moguće kreirati kriptovalutu, koja će istovremeno zadovoljiti pravne propise svih zemalja, i tog razloga se praktikuje pridržavanje generalnih smjernica u borbi protiv pranja novca (Anti Money Laundering - AML), a berze za razmjenu kriptovaluta, praktikuju i KYC (Know Your Client) procedure.

7. ZAKLJUČAK

Obzirom na ne stabilnu geopolitičku situaciju, npr. trgovinski rat između USA i Kine, političkih i praktičnih promjena od početka pandemije COVID 19 virusa, kao i inflaciju valuta, kriptovalute imaju sve veću budućnost. Problem inflacije je trenutno globalan jer se usljed pandemije COVID 19 doštampavao i USD [6] i EUR [7] kako bi vlade zemalja izvršile bailout tj. otkup dugova svojih nacionalnih avio, brodskih i drugih kompanija. Time su kompanije mogle da nastave s radom, a stotine hiljada radnika sačuvali radna mjesta, i ekonomija tih zemalja nije stala. Negativan efekat je pad vrijednosti novca, tj inflacija. Nasuprot tome, Bitcoin ima ograničen ukupan broj coin-a (21 milion), te je problem inflacije kod njega eliminisan.

Komparativna analiza PoW, PoS i PoSt konsenzus mehanizama pokazuje da je PoSt (proof of space and time) najperspektivniji izbor konsenzus mehanizma.

Nov konsenzus mehanizam zahtjeva i razvoj nove blockchain platforme.

Dizajn nodova bi, zahvaljujući odabranom konsenzus mehanizmu trebao da pruži veći nivo decentralizacije. Porastom mreže, i brojem nodova, značajno bi rastao i stepen bezbjednosti, jer bi takva mreža postala otpornija na hakerske napade.

U unutrašnjoj strukturu blockchain-a, digitalno potpisivanje blokova najoptimalnije je vršiti „BLS“ (Boneh–Lynn–Shacham) algoritmom jer nema nasumičnosti kao kod „ECDSA“ (Elliptic Curve Digital Signature Algorithm) algoritma, a potpisi su 50% manji nego kod „Schnorr“ algoritma, što pruža bolju optimizaciju [8].

API-ji treba da pruže visok stepen interkonekcije s ostalim platformama i tehnologijama, jer od toga drastično zavisi mogućnost šire primjene kripto valute.

Kripto valuta treba da podrži sve tipove wallet-a, jer je odabir stvar preference korisnika.

Korisnički interfejsi moraju biti dizajnirani na jednostavan i prihvatljiv način, tako da onemogućavaju

duple transakcije, pruže korisniku knjugu kontakata, i maksimalno pojednostave upotrebu. Administratorski interfejsi, moraju što jasnije pružiti uvid u detektovane anomalije unutar sistema, kako bi administrator jasnije mogao obraditi informacije i donijeti odluku.

Snaga potencijalnog blockchain rješenja može se uveliko poboljšati integracijom vještačke inteligencije (AI), biometrije, robota, klauda, kognitivnih usluga, kontejnera, analitike podataka, interneta stvari i mašinskog učenja.

Preporučuje se pridržavanje generalnih smjernica za pravne aspekte.

LITERATURA

- [1] *Number of Blockchain wallet users worldwide from November 2011 to September 13*, Dostupno na: <https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/> 2021.
- [2] *What Is the Nakamoto Consensus?* Dostupno na: <https://coinmarketcap.com/alexandria/article/what-is-the-nakamoto-consensus>
- [3] Tal Moran & Ilan Orlov, *Simple Proofs of Space-Time and Rational Proofs of Storage*. Dostupno na: <https://eprint.iacr.org/2016/035.pdf>
- [4] Luke Conway, *Blockchain explained*. Dostupno na: <https://www.investopedia.com/terms/b/blockchain.asp>
- [5] Roy Natan, *Consensus Algorithm Summary*. Dostupno na: <https://github-wiki-see.page/m/Chia-Network/chia-blockchain/wiki/Consensus-Algorithm-Summary>
- [6] Vivek Kaul, *Lessons from the Fed's \$3 trillion money printing*. Dostupno na: <https://www.livemint.com/industry/banking/lessons-from-the-fed-s-3-trillion-money-printing-11592322603528.html>
- [7] Balazs Koranyi, Francesco Canepa *ECB to print 1 trillion euro this year to stem coronavirus*. Dostupno na: <https://www.reuters.com/article/us-health-coronavirus-ecb-idUSKBN21543D>
- [8] *ECDSA VS Schnorr signature VS BLS signature*. Dostupno na: <https://blog.csdn.net/mutourend/article/details/106796297>

SUMMARY

THE ROLE OF BLOCKCHAIN IN CREATING CRYPTOCURRENCY

The main carrier of the cryptocurrency system is blockchain. The paper will explain the differences between tokens and coins, the role of miners in the cryptocurrency system, forks, how a consensus mechanism is achieved. The protocols in use will also be discussed. Due to technical similarities, a blockchain was compared with Bitcoin, which provides an excellent reference point. The paper also presents the practical application of blockchain in the form of smart contracts. The paper will propose the stages of development of own cryptocurrency, from the very beginning, where the purpose of existence is defined, through the selection of technical solutions, until the finalization where marketing and commercial aspects play a crucial role for success, with guidelines for legal aspects.

Key words: *blockchain, consensus, smart contracts, nodes, wallet*