# Blockchain tehnologija u svijetu kriptovaluta

**Farkaš, Luka**

**PRIRODOSLOVNO-MATEMATIČKI FAKULTET U SPLITU**

ZAVRŠNI RAD

# BLOCKCHAIN TEHNOLOGIJA U SVIJETU KRIPTOVALUTA

Mentor: Dr. sc. Saša Mladenović

Student: Luka Farkaš

Split, rujan 2021. godine

# Temeljna dokumentacijska kartica

Završni rad

Sveučilište u Splitu

Prirodoslovno-matematički fakultet

Odjel za politehniku

Ruđera Boškovića 33, 21000 Split, Hrvatska

# BLOCKCHAIN TEHNOLOGIJA U SVIJETU KRIPTOVALUTA

Luka Farkaš

## SAŽETAK

Blockchain tehnologija u svijetu kriptovaluta donosi sustav decentraliziranog načina poslovanja. Bitcoin kao predstavnik u kriptovaluta donosi izvršavanje transakcija bez centralnog autoriteta. Takvo poslovanje postiže se određenim mehanizmima uz točno određena pravila i algoritme koji moraju zadovoljiti sve uvjete ispravnosti. Štoviše, velik broj ljudi mora provjeriti ispravnost transakcija kako bi bile valjane što donosi čvrstu i sigurnu provjeru i povezanost. Blockchain tehnologija i kriptovalute objašnjene su pomoću Bitcoina, izrađenog simulatora i Ethereuma. Dodatno je navedena primjena blockchain tehnologije u zdravstvenoj industriji i pri glasanju na izborima kao moguće rješenje za opisane probleme. Blockchain tehnologija ima priliku za napredak i razvoj primjenom umjetne inteligencije.

**Ključne riječi**: Blockchain tehnologija, blok, Bitcoin, kriptovalute, rudarenje, transakcije, dokaz o radu, Ethereum, Ether, pametni ugovori

Rad je pohranjen u knjižnici Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu

**Rad sadrži:** 30 stranica, 18 grafičkih prikaza, 1 tablicu i 21 literaturni navod.

Izvornik je na hrvatskom jeziku.

**Mentor:** **Dr. sc. Saša Mladenović,** *izvanredni profesor Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu*

**Ocjenjivači:** **Dr. sc. Saša Mladenović,** *izvanredni profesor Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu*

**Dr. sc. Divna Krpan,** *viši predavač redoviti profesor Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu*

**Dr. sc. Goran Zaharija,** *docent Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu*

Rad prihvaćen: **rujan 2021**

# Basic documentation card

Thesis

University of Split

Faculty of Science

Department of polytechnics

Ruđera Boškovića 33, 21000 Split, Croatia

# BLOCKCHAIN TECHNOLOGY IN THE CRYPTOCURRENCY WORLD

Luka Farkaš

## ABSTRACT

Blockchain technology in the cryptocurrency world brings a system of decentralized way of doing business. Bitcoin as a representative in cryptocurrencies brings the execution of transactions without central authority. Such business is achieved by certain mechanisms with precisely defined rules and algorithms that must meet all the conditions of correctness. Moreover, a large number of people have to check the correctness of transactions in order to be valid which brings a firm and secure check and connection. Blockchain technology and cryptocurrencies are explained by using Bitcoin, a simulator and Ethereum. Additionally, the application of blockchain technology in the healthcare industry and in elections is mentioned as a possible solution to the described problems. Blockchain technology has an opportunity for advancement and development with the application of artificial intelligence.

**Key words**: Blockchain Technology, block, Bitcoin, cryptocurrencies, mining, transactions, proof of work, Ethereum, Ether, smart contracts

Undergraduate thesis deposited in library of Faculty of science, University of Split

**Thesis consists of:** 30 pages, 18 figures, 1 tables and 21 references

Original language: Croatian

**Mentor:** **Saša Mladenović Ph.D.** *Associate Professor Professor of Faculty of Science, University of Split*

**Reviewers:** **Saša Mladenović Ph.D.** *Associate Professor Professor of Faculty of Science, University of Split*

**Divna Krpan, Ph.D.** *Senior Lecturer of Faculty of Science, University of Split*

**Goran Zaharija, Ph.D.** *Assistant Professor, University of Split*

Thesis accepted: **September 2021**

# IZJAVA

kojom izjavljujem s punom materijalnom i moralnom odgovornošću da sam završni rad s naslovom BLOCKCHAIN TEHNOLOGIJA U SVIJETU KRIPTOVALUTA izradio samostalno pod voditeljstvom izvanrednog profesora dr. sc. Saše Mladenovića. U radu sam primijenio metodologiju znanstvenoistraživačkog rada i koristio literaturu koja je navedena na kraju završnog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo/ u diplomskom radu na uobičajen, standardan način citirao/la sam i povezao/la s fusnotama s korištenim bibliografskim jedinicama. Rad je pisan u duhu hrvatskog jezika.

Student

Luka Farkaš

## Sadržaj

# Uvod

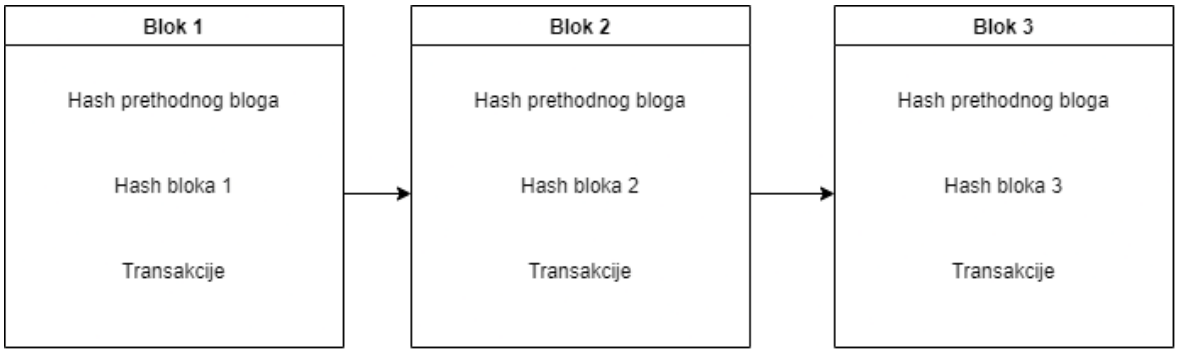
Suvremeni život je nezamisliv bez interneta, koji sa sobom nosi razne tehnologije. Jedna od njih je blockchain (*hrv. lanac blokova*) tehnologija. Stuart Haber i Scott Stornetta su početkom devedesetih godina prošlog stoljeća stvorili ideju o blockchain tehnologiji kakvu mi danas poznajemo. Njihov prvi rad temeljio se na kriptografski osiguranom lancu blokova kojem nitko nije mogao mijenjati vremensku oznaku dokumenata. Kasnije su svoj rad unaprijedili sa strukturom Merkle stabla kako bi mogli pohraniti što više dokumenata u jednom bloku. Zatim se pojavljuje Bitcoin kao digitalna kriptovaluta čija je osnova blockchain tehnologija. Bitcoin je danas prihvaćen u svijetu i blockchain tehnologija je pronašla primjenu u mnogim područjima djelatnosti kao što su: lanci opskrbe, zdravstvena industrija, digitalne umjetnine i drugo. Ovaj rad nastoji opisati glavne principe djelovanja blockchain tehnologije i kriptovaluta kroz istu. Bitcoin, kao glavni predstavnik kriptovaluta i blockchain tehnologije, okupio je mrežu ljudi koji rudarenjem pokušavaju osigurati transakcije, bez centralnog autoriteta. Par godina kasnije, pojavljuje se Ethereum. Ethereum predstavlja decentraliziranu mrežu koja je nadopunila nedostatke Bitcoina koje je uvidio Vitalik Buterin. Glavna razlika je u tome što Ethereum iza sebe ima cijelu mrežu kriptovaluta koje obavljaju različite funkcije, pruža mogućnost programiranja raznih aplikacija i konstantno razvija nove alate u kripto svijetu. Bitcoin služi samo kao digitalna vrijednost koja se često naziva i digitalno zlato. Zbog svoje popularnosti, Bitcoin se koristi kao platno sredstvo u mnogim primjerima svakodnevnog života: piće u kafiću, kupovina automobila, valuta države i drugo. Danas, svatko tko ima računalo i internet može postati sudionik blockchain tehnologije i kriptovaluta. Dovoljno je samo educirati se i odabrati kriptovalutu jer postoji velik broj kriptovaluta koje pružaju vrlo slične usluge. Nakon što su pojašnjene glavne karakteristike Bitcoina i Ethereuma, prikazana je problematika zdravstvene industrije čije je kvalitetno rješenje blockchain tehnologija i Ethereum mreža, koja pruža specifikacije i blockchain prikladan za rad poduzeća. Blockchain tehnologija bi također osigurala kvalitetno i sigurno glasanje na izborima, a „suradnja“ s umjetnom inteligencijom bi dodatno povećala efikasnost blockchain tehnologije [13]

# Motivacija

Bitcoin je 2008. godine donio promjene u svijetu financija putem blockchain tehnologije. Mnogi s Bitcoinom povezuju nagli skok vrijednosti Bitcoina s nekoliko centi do nekoliko dolara, pa danas i nekoliko desetaka tisuća dolara. U ekonomskom smislu Bitcoin se može kupiti, čuvati ili prodati i ostvariti ekonomsku dobit te se može trošiti kao običan novac. S druge strane, blockchain tehnologija je puno zanimljivija te je do danas (2021. godina) na temelju Bitcoina i blockchain tehnologije stvoreno više od 11 600 kriptovaluta. Najveća posebnost blockchain tehnologije je u tome što za obradu transakcija nije potreban centralni autoritet već se transakcije verificiraju rudarenjem. Rudari pružaju svoju računalnu snagu kako bi se verificirale transakcije i dobivaju nagradu u kriptovaluti, za čiju mrežu verificiraju transakcije. Nakon Bitcoina pojavio se Ethereum koji sa sobom donosi cijelu mrežu kriptovaluta i blockchaina. Ethereum blockchain sadrži pametne ugovore koji se izvršavaju automatski, također bez centralnog autoriteta. Bitno je naglasiti kako su i Bitcoin i Ethereum otvorenog koda (*eng. open source*) što ulijeva povjerenje korisnicima koji ulažu svoj novac, vrijeme i rad u kriptovalute. U početku se kriptovalutama moglo samo trgovati, dok se danas na blockchain stavljaju i autorska prava digitalnih umjetnina i glazbe. Postoje igrice čijim se igranjem može zaraditi kriptovaluta, a nogometni klubovi imaju svoje „fan tokene“ s kojima navijači i ljubitelji određenog kluba mogu trgovati, kupovati ulaznice i slično. Glavna prepreka kriptovalutama je djelovanje banaka koje predstavljaju centralni autoritet u svijetu financija. Prednost Bitcoina nad bankama je ta što za transakcije s Bitcoinom nije potrebno posjedovati nikakve posebne račune. Primatelj i pošiljatelj ne moraju biti u istoj državi i pri izvršavanju transakcije i nigdje ne moraju priložiti svoje osobne podatke. Bitcoinom se može trgovati svuda u svijetu uz male naknade za transakciju. Naravno, kriptovalute i blockchain tehnologija imaju negativne strane, ali je potrebno usavršavati tehnologije u skladu s vremenom i mogućnostima na internetu.

# 1. Blockchain tehnologija

Blockchain predstavlja javnu knjigu (*eng. ledger*) ili skup zapisa svih digitalnih transakcija i događaja koji su izvršeni i podijeljeni među sudionicima blockchain sustava. Podatak koji se jednom unese u blockchain nikada se ne može brisati ili mijenjati. Blok se sastoji od informacija izvršenih transakcija koje su provjerene od strane validatora. Svaki blok povezan je sa svojim prethodnim i sljedećim blokom. Bitna stavka u svakom bloku je *hash*. *Hash* je matematička funkcija koja ulaz podataka neodređene duljine pretvara u zapis fiksne duljine. Jednom izračunati podatci pretvoreni u *hash* ne mogu se ponovno preračunati u početne podatke. Ukoliko bi se samo jedan ulazni podatak promijenio, izračunati *hash* bio bi potpuno drugačiji od onog „pravog“. Algoritam kojim se u Bitcoin blockchainu izračunavaju *hashevi* naziva se SHA-256. Svaki blok u blockchain sustavu sadrži *hash* prethodnog bloka, što omogućava čvrstu i sigurnu povezanost blokova. Pojednostavljen prikaz blokova u blockchain tehnologiji prikazan je na slici 1. [1] [2] [3]




Slika 1 Pojednostavljeni prikaz blokova u blockchain tehnologiji

## 1.1. Bitcoin

Bitcoin je najpopularniji primjer koji je izravno vezan za blockchain tehnologiju. Stvoren je 2009. godine kao digitalna kriptovaluta. Grupa ili pojedinac (i dalje se ne zna tko je tvorac Bitcoina) pod imenom Satoshi Nakamoto 2008. godine objavila je u svom članku, pod nazivom “Bitcoin: A Peer-To-Peer Electronic Cash System”, bijeli papir (*eng. whitepaper*) Bitcoina. Whitepaper je opisivao tehnologiju kojom će Bitcoin funkcionirati gdje se, između ostalog, opisuje kako će transakcije Bitcoinom imati male iznose naknada

te će se transakcije izvršavati bez centralnog autoriteta - banke. Nakon objavljivanja whitepapera stvoren je i prvi blok (*eng. genesis block*) u blockchain sustavu, koji je sadržavao 50 od ukupnih 21 000 000 Bitcoina. Protokol za funkcioniranje Bitcoin blockchaina bio je otvorenog koda i svatko ga je mogao preuzeti i pokrenuti na svom računalu. Bitcoin ne postoji u fizičkom smislu kao kovanica ili papirnati novac, već se podatci o količini Bitcoina čuvaju na blockchainu. Simbol Bitcoina je kovanica narančaste boje koja u sredini ima slovo „B“, koje izgleda slično kao oznaka valute dolar ($). Postoji više vrsta simbola za Bitcoin i jedna od njih prikazana je na slici 2.

Slika 2 Jedan od simbola Bitcoina

(izvor https://hr.m.wikipedia.org/wiki/Datoteka:BTC_Logo.svg)

Takvi podatci javno su dostupni i transparentni. Svatko tko želi posjedovati Bitcoin mora posjedovati i digitalni kripto novčanik. Postoje razne vrste digitalnih kripto novčanika i svaki novčanik mora imati jedinstvenu adresu pomoću koje uplatitelj šalje, a primatelj prima Bitcoin. Kripto novčanik se može napraviti putem interneta, preuzeti s interneta kao desktop aplikacija ili se može kupiti u fizičkom obliku koji je sličan izgledu USB-a. Takav pristup slanju Bitcoina u potpunosti je anoniman jer adresa ne sadržava nikakve podatke iz kojih bi se moglo pročitati tko „stoji“ iza transakcije. Dakle, svaka transakcija je javna i vidljiva na blockchainu, ali ujedno je i anonimna. [1] [2] [3]

## 1.2. Rudarenje Bitcoina

Rudarenje se u svijetu kriptovaluta koristi kao termin za stvaranje novih digitalnih kovanica. Postoje i drugi načini stvaranja digitalnih kriptovaluta, ali Bitcoin nastaje rudarenjem. Bitcoin se rudari uz pomoć posebnih računala koja koriste svoju snagu kako bi riješili složene matematičke probleme potrebne za stvaranje novog bloka transakcija. Rudarem se naziva onog koji pruža svoju računalnu snagu Bitcoin mreži. Rudar, odnosno

njegova računalna snaga, koji prvi uspješno riješi zadani matematički problem, stvara određeni dio Bitcoina na način da ga dobije kao nagradu u svoj kripto novčanik. Bitna karakteristika pri rudarenju Bitcoina težina je rudarenja na Bitcoin mreži (*eng. network difficulty*). Težina mreže određuje koliko je računalne snage potrebno da bi se stvorio novi blok. U početku je težina mreže bila niska i Bitcoin se mogao stvarati snagom iz grafičkih kartica i procesora, dok su danas potrebna ASIC računala. Težina mreže od početka postojanja Bitcoina do danas (22.7.2021.) prikazana je na slici 3.

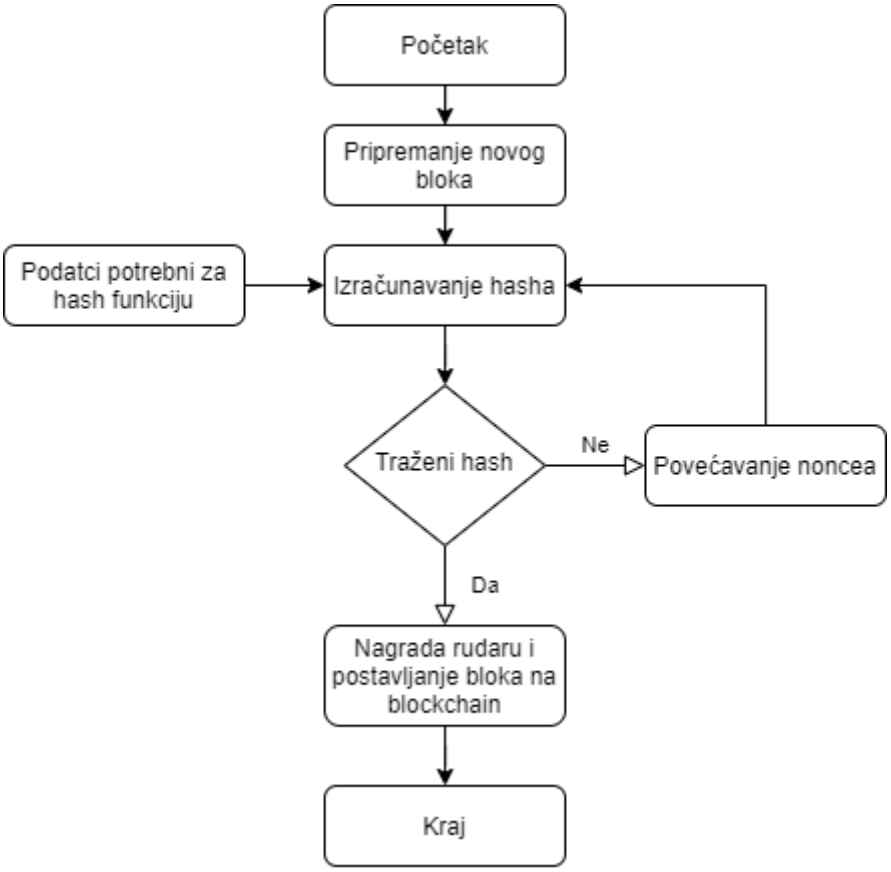

Slika 3 Grafički prikaz težine rudarenja na Bitcoin mreži (slika je prerađena po uzoru na sliku https://api.blockchain.info/charts/preview/difficulty.png?timespan=all&h=600&w=1200 )

Početna nagrada za uspješno stvaranje novog bloka iznosila je 50 Bitcoina. Svake četiri godine nagrada se smanjuje za pola *(eng. halving)*. Danas (23.7.2021.) se za uspješno stvoren blok dobiva 6.25 Bitcoina, a idući halving će se dogoditi 2024. godine i nagrada za jedan blok će biti 3.125 Bitcoina. Predviđa se da će zadnji Bitcoin biti stvoren 2140. godine (21 000 000 Bitcoina će biti u opticaju 2140.) te će se tada rudari nagrađivati s naknadom za transakciju (*eng. transaction fee*). Postoji i mogućnost da se početni Bitcoin protokol promijeni što bi utjecalo na način nagrađivanja rudara. [3], [4]

## 1.3. Verifikacija transakcija (proof of work)

Verifikaciju Bitcoin transakcija izvršavaju rudari. Rudar najprije mora provjeriti transakcije veličine jedan megabajt neovisno o tome koliko transakcija sačinjava toliku količinu podataka. Veličina transakcije ovisi o tome koliko podataka pohranjuje određena transakcija. Uglavnom se u bloku nalazi po nekoliko tisuća transakcija. Zatim rudar mora

postaviti blok na blockchain rješavanjem složenog matematičkog problema. Opisan način verifikacije naziva se dokaz o radu (*eng. proof of work,* skraćenica PoW) kojim rudar pokušava pronaći *hash* koji je manji ili jednak ciljanom *hashu*. Potrebno je „imati sreće“ i biti prvi rudar na mreži koji je uspio verificirati sve transakcije i izračunati traženi *hash*. Dakle, velik broj rudara verificira transakcije, dok samo jedan uspijeva najbrže izračunati traženi *hash*. Slika 4 prikazuje dijagram toka PoW algoritma za postizanje konsenzusa.




Slika 4 PoW opisan dijagramom toka

Zbog težine na  Bitcoin mreži pojedincu treba ogromna količina računalne snage kako bi prvi izračunao ciljani *hash*, pa se rudari udružuju u rudarski bazen (*eng. mining pool*). *Mining pool* funkcionira tako da više rudara međusobno udružuje svoje računalne snage i time imaju veće šanse za stvoriti blok i postaviti ga na blockchain. Dobivena nagrada ravnomjerno se dijeli među rudarima. Transakcije je moguće provjeriti bez pokretanja cijelog mrežnog čvora. Korisnik treba imati samo kopiju zaglavlja najdužeg PoW lanca u blockchainu. Najduži PoW lanac dobiva se slanjem upita mrežnom čvoru dok se ne utvrdi da je to zaista najduži lanac. Zatim korisnik može dobiti popis transakcija povezujući transakciju s blokom koji sadrži vremensku oznaku. Korisnik ne može validirati svoju

transakciju, ali može provjeriti mjesto u lancu na kojem se transakcija nalazi i vidjeti je li prihvaćena od strane mrežnog čvora [2], [3], [6]

## 1.4. Validacija bloka

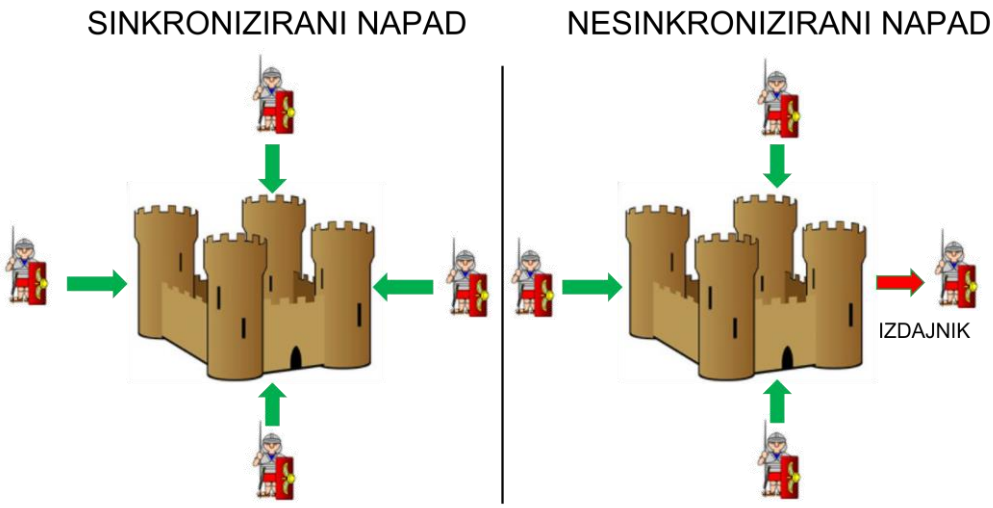
Stalnim generiranjem novih blokova na Bitcoin mreži, lanac blokova se konstantno povećava te je potrebno ažurirati posljednje stanje Bitcoin ledgera. Validacija bloka izvršava se u sljedećim koracima:

1. Provjerava se validnost i postojanje prethodnog bloka na koji se trenutni blok referencira.
2. Provjera se je li vremenska oznaka veća od prethodnog bloka i manja od 2 sata u budućnost.
3. Provjerava se validnost PoW algoritma trenutnog bloka.
4. Postavlja se `S[0]` za zadnje stanje prethodnog bloka. Stanje označava kolekciju Bitcoin novčića koji su stvoreni rudarenjem, ali još nisu potrošeni.
5. Pretpostavimo da je `TX` popis transakcija bloka s n transakcija. Za svaki `i` u `0 ... n-1` postavite `S[i+1] = Apply (S[i], TX [i])`. Apply funkcija provjerava nepotrošene novčiće, poklapaju li se sa stanjem bloka i provjerava odgovara li navedeni potpis vlasniku nepotrošenih novčića. Radi lakšeg razumijevanja pojma „nepotrošeni novčići“ slijedi pojašnjenje: Transakcije na Bitcoinovom blockchainu funkcioniraju tako da uplatitelj pošalje na blockchain cijeli svoj iznos Bitcoina koji posjeduje te dio šalje primatelju, a ostatak „šalje“ samom sebi. Ostatak su nepotrošeni novčići koje funkcija provjerava.
6. Ukoliko je sve prošlo bez pogreške, `S[n]` se postavlja kao posljednje stanje bloka.

Bitno je kojim redom rudar unosi transakcije u blok. Ukoliko postoje dvije transakcije A i B u bloku tako da B transakcija troši nepotrošene novčiće od transakcije A, od velike je važnosti da se transakcije A prva unese u blok kako bi blok bio ispravan. [9]

## 1.5. Problem bizantskih generala

Problem bizantskih generala najčešći je problem s kojim se suočavaju decentralizirani sustavi. Generali su predstavljeni kao Bitcoin čvorovi (*eng. node*), odnosno rudari. Glavna ideja ovog problema je sljedeća: kako osigurati da peer-to-peer, decentralizirana Bitcoin mreža, donosi ispravne odluke i verificira transakcije, čak i ako dio rudara pokuša namjerno donositi krive, odnosno neispravne odluke? Zamislimo dvorac koji su generali odlučili napasti kao na slici 5.




Slika 5 Grafički prikaza problema bizantskih generala (slika je prerađena po uzoru na sliku https://www.flickr.com/photos/166102838@N03/31024022797)

Generali su sa svojim vojskama okružili dvorac i moraju se dogovoriti za napad s drugim generalima. Dvorac također ima vojsku koja je utvrđena i odana kralju. Generali se dogovaraju za napad na način da jedni drugima prenose poruke putem glasnika. Dvorac je dobro utvrđen pa je generalima važno da napad izvedu sinkronizirano. Slanje poruka može izazvati neke od sljedećih problema:

1. Glasnik može biti izdajnik te će prenijeti krivu poruku drugom generalu i napad neće uspjeti.
2. Neprijatelj može zarobiti glasnika i generali neće znati kada točno trebaju napasti
3. Problem može biti i u generalima koji se mogu namjerno povući kako bi drugi generali neuspješno napali kralja.
4. General ne može znati koji od preostalih generala neće izvršiti napad na kralja nego će ga braniti .

„Napad“ na Bitcoin mreži bi također morao biti sinkroniziran i većina rudara bi morala u tome sudjelovati (minimalno 51% rudara). Kao primjer napada uzet ćemo dvostruku potrošnju (*eng. double spending*). Kupac bi u tom slučaju mogao kupiti Bitcoin dva puta s istim iznosom novca. Obje transakcije dolaze na verifikaciju i rudari primijete da takvo nešto nije moguće te prvu verificiraju, a drugu označavaju kao neispravnu. Ukoliko se transakcije izvrše simultano, ispravna će biti ona koja ima više potvrda od validatora. [5]

## 1.6. Nonce

*Nonce* je skraćenica za „Broj koji se koristi samo jednom“ (*eng. number only used once*). Koristi se u blockchain tehnologiji kao dodatak *hashu* bloka kako bi se zadovoljili uvjeti težine na Bitcoin mreži. Prethodno stvorenom *hashu* dodaje se *nonce* te se ponovno izvršava *hash* funkcija. Rudari moraju pronaći odgovarajući *nonce* kako bi bili nagrađeni Bitcoinom. Podatci o rudaru, *nonceu*, transakcijama i drugim podatcima vezano za stvoren blok mogu se pronaći na Bitcoin blockchain istraživačima (*eng. blockchain explorer*). Slika 6 prikazuje dio podataka za blok broj 699 599 sa blockchain explorera.

| | |
|---|---|
| Rudar | Poolin |
| Broj transakcija | 2,110 |
| Težina | 18,415,156,832,118.24 |
| Merkle korijen | 218662b29fd73a242ec680ef52c86b9ce4741af8fc9beadfd735a39e7aa76f79 |
| Nonce | **2,716,998,054** |

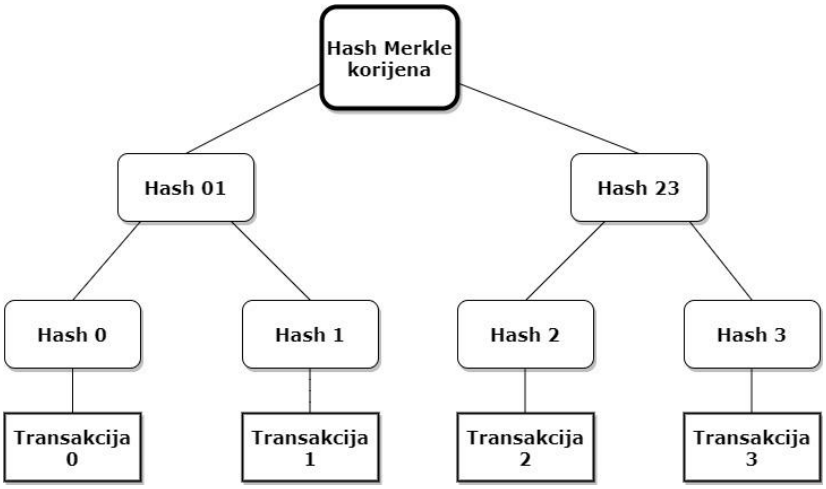
Slika 6 Podatci bloka 699 599 na Bitcoin mreži (slika je prerađena po uzoru na podatke sa stranice https://www.blockchain.com/btc/block/000000000000000000d41c37450e08ce4b20723ebf3edfc27ce3a7684d89a25)

Ukoliko *hash* zadovoljava sve uvjete za stvaranje novog bloka, a *nonce* je manji od traženog, takav *nonce* nazivamo zlatni *nonce* (*eng. golden nonce*). Rudari moraju pogoditi *nonce*, dodati ga u *hash* i provesti usporedbu s traženim *hashem*. Vrlo je mala šansa za pronalazak *noncea* u prvom pokušaju, a povećanje težine na Bitcoin mreži otežava pronalazak traženog *noncea*. Težina mreže za sve je rudare jednaka, što osigurava svima istu mogućnost pronalaska traženog *noncea*. Bitcoin mreža unaprijed zna koliko bi se novih blokova trebalo izgenerirati tijekom određenog vremena. Manji broj izgeneriranih blokova rezultira smanjenjem težine na mreži i obratno. Smanjenjem težine, smanjit će se

vrijeme potrebno za pronalazak traženog *noncea* i stvaranje ciljanog *hasha* te će se postići predodređeni broj novih blokova na mreži. [3]

## 1.7. Pohranjivanje transakcija u bloku

Prethodno je navedeno kako blok može sadržavati i do nekoliko tisuća transakcija te bi validacija svake transakcije zasebno, pri postavljanju novog bloka na blockchain, trošilo više vremena i računalne snage. Transakcije se spremaju u strukturu binarnog stabla i *hashiraju*. *Hash* transakcije ostaje u tijelu bloka i stavlja se u strukturu binarnog stabla koja se naziva Merkleovo stablo (*eng. Merkle tree)*. Grafički prikaz strukture Merkle stabla prikazan je na slici 7 radi lakšeg predočavanja strukture.




Slika 7 Grafički prikaz Merkle stabla

Na primjer, potrebno validirati ima velik broj transakcija, podatke od prve dvije transakcije provest će se kroz *hash* funkciju. Podatci transakcije su djeca, a *hash* ostaje kao roditelj dviju transakcija. Taj korak ponovi se za sve parove transakcija. Zatim dobivene *hasheve*, također u parovima, provedemo kroz *hash* funkciju i dobivamo nove roditelje od parova *hasheva*. Korak se ponavlja sve dok se ne dobije korijen Merkle stabla, odnosno samo jedan *hash*, koji je nastao od svih transakcija i njihovih *hasheva*. Korijen *hasheva* sprema se u zaglavlje bloka. Uzimajući u obzir da je za stvaranje novog bloka potrebno deset minuta, blokovi bi godišnje zauzimali oko 4.2 megabajta prostora. Prema Mooreovom zakonu, radna memorija računala svake bi se godine povećavala za 1.2 gigabajt. Dakle, pohrana blokova ne bi trebala predstavljati problem čak i ako bi se blokovi morali čuvati u radnoj memoriji. [2]

# 2. Implementacija – Blockchain simulator

Nakon opisanih glavnih karakteristika blockchain strukture i principa rada, slijedi simulacija stvaranja novih blokova na mreži uz pomoć simulatora. Simulator će tražiti određene *hasheve* uz pomoć računalne snage koja će biti višestruko manja od potrebne za stvaranje novih Bitcoin blokova.

## 2.1. Korištene tehnologije

Simulator predstavljen kao konzolska aplikacija programirana u Microsoft Visual Studio 2019. okruženju u programskom jeziku C#. Sličan je programskom jeziku C, C++, Java i JavaScript. C# objektno je orijentiran programski jezik koji omogućuje programerima izradu raznovrsnih aplikacija (web aplikacija, mobilnih aplikacija, desktop aplikacija…). Programski kod izvršava se u .NET okruženju, virtualnom sustavu za izvršavanje koji se naziva common language runtime (CLR) i skupu biblioteka klasa. CLR je Microsoftova implementacija common language infrastructure (CLI). CLI je osnova za stvaranje okruženja za izvršavanje i razvoj u kojima jezici i biblioteke besprijekorno rade zajedno. Izvorni kod se kompajlira u intermediate langugage (IL) koji je u skladu s CLI zahtjevima. IL se pohranjuje u assembly koji sadrži popis informacija o assembly tipovima i verziji. Nakon izvršavanja C# programskog koda, assembly se učitava u CLR koji izvodi kompajliranje za pretvaranje IL koda u strojne upute točno na vrijeme *(eng. Just-In-Time*, JIT). CLR pruža i druge usluge kao što su: automatsko prikupljanje smeća (*eng. garbage collection*), upravljanje iznimkama i upravljanje resursima. Dakle, C# kod se ne kompajlira direktno u strojni jezik za određenu platformu već to radi pomoću IL kako bi se bez problema izvršavao na različitim platformama. [7]

## 2.2. Klase i imenski prostori

Imenski prostori u C# služe za organiziranje i grupiranje klasa. Klasa je tip podatka koji manipulira podatcima preko objekta, instance klase. Klasa `Program` sadrži glavnu metodu `Main()` koja postavlja početne parametre i poziva metodu za stvaranje blokova. Početni parametri u ovom su slučaju težina na mreži i konačan broj blokova koje će

simulator izgenerirati. `Blockchain` klasa u svom konstruktoru sadrži poziv metode za stvaranje genesis bloka. Blokovi će se pohranjivati u listu nakon što se izgeneriraju. Klasa `Block` sadrži glavne parametre potrebne za izračunavanje *hasha*. Parametri se u konstruktoru spremaju u određene tipove podataka i pripremaju za *hash* funkciju. Algoritam kojim se provodi *hash* funkcija naziva se SHA256 i za njega nam je potreban kriptografski imenski prostor `using System.Security.Cryptography.` Kriptografske funkcije koriste se kada je podatke potrebno zaštititi od „treće strane“. Zaštićene podatke zna pročitati samo krajnji primatelj koji će podatke dešifrirati određenim algoritmom. Ukoliko podatci budu ukradeni ili završe kod pogrešnog primatelja, bit će ih teško dešifrirati i pročitati. Imenski prostor `using Newtonsoft.Json` koristimo za pretvaranje podataka o transakciji iz tekstualnog oblika u JSON oblik. Posljednja klasa `BlockTransactionData` sadrži podatke o transakciji: prodavač, kupac i iznos. Podatci će se u klasi `Block` pretvarati u JSON oblik te koristiti u *hash* funkciji kao parametri. Dijagram klasa prikazan je na slici 8. [8]

Slika 8 Dijagram klasa blockchain simulatora

## 2.3. Metode

Metoda u C# programskom jeziku predstavlja blok koda koji sadrži niz izraza. Može sadržavati ulazne parametre te se izvršava pozivanjem u kodu. Metoda `Main()` je početna točka za svaku C# aplikaciju, a poziva se CLR-om pri pokretanju programa. Sada će se opisati metode u klasama blockchain simulatora

- Klasa `Program` sadrži samo metodu `Main()`, za koju je već napisano kako sadrži početne parametre i poziva metodu `StartMining()`. Metoda kao ulaz sadržava konačan broj blokova koje će simulator generirati i težinu na mreži koja se proizvoljno odabire. Težina na mreži postavljena je na vrijednost 5 kao i broj blokova koje će simulator generirati.

```
const int difficulty = 5;
const int numberOfBlockToBeMined = 5;
```

  Nakon što se stvore svi blokovi, pozvat će se metoda `ChainValidator()` koja će provjeriti sve blokove i njihovu povezanost *hashevima*.

- Klasa `Block` sadrži metodu `ClaculateHash()` za izračunavanje *hasha* koja sadrži instancu klase SHA256.

```
using var sha256Hash = SHA256.Create();
```

  *Hash* se računa uz pomoć potrebnih podataka koji se kodiraju UTF-8 (Unicode Transformation Format) standardom. Znak u UTF-8 standardu može biti prikazan duljinom od jednog do četiri bajta te je moguće prikazati bilo koji znak u Unicode standardu. Unicode standardom može se prikazati bilo koja riječ, simbol, oznaka, broj bez obzira na platformu, jezik, aplikaciju ili uređaj. UTF-8 je „unatrag“ kompatibilan s ASCII zapisom. Nakon što metoda `ComputeHash()` izračuna *hash* i vrati niz bajtova, svaki cijeli broj (*eng. integer*) sprema se u instancu klase `StringBuilder` u heksadecimalnom formatu kao što je prikazano u kodu ispod.

```
var hashedData = new StringBuilder();
            foreach (var b in bytes)
            {
                hashedData.Append(b.ToString("x2"));
            }
```

  Nakon što se svi bajtove pretvore u heksadecimalne znakove, metoda završava s vraćanjem *hasha* u obliku niza znakova (*eng. string*). [13], [14]

  Metoda `MineBlock()` postavlja početni dio *hasha* na odgovarajući broj nula, što odgovara parametru `Difficulty`. Nakon određivanja prvog dijela *hasha*, pozivanje metode `CalculateHash()` poziva se dok se prvi dio *hasha* ne „poklopi“ s traženim prvim dijelom *hasha*. *Nonce* se povećava nakon svakog neuspjelog pokušaja traženja *hasha*. Kod ispod prikazuje petlju koja povećava *nonce* dok se ne pronađe traženi *hash*, odnosno u ovom slučaju prvi dio *hasha*.

```
while (Hash.Substring(0, Difficulty) != target)
                {
                    this.Nonce++;
                    this.Hash = this.CalculateHash();
                }
```

Nakon uspješnog pronalaska prvog dijela *hasha*, poziva se metoda `PrintMinedHashInfo()` koja ispisuje detaljne podatke o uspješno stvorenom bloku.

- Klasa `Blockchain` sadrži metodu `CreateGenesisBlock()` za stvaranje prvog bloka na mreži. Podatci za transakciju unaprijed su postavljeni, a *hash* prethodnog bloka je 0. Podatci o pošiljatelju, primatelju i količini poslanog Bitcoina spremaju se pomoću instance klase `BlockTransactionData`.

  ```
  var data = new BlockTransactionData() { Amount = 0, Seller =
  "Genesis Block", Buyer = "Genesis Block" };
  ```

  Metoda u sebi sadrži instancu klase `Block` u koju šalje podatke prvog bloka na mreži. Nakon dobivenih podataka, klasa `Block` u konstruktoru poziva metodu `CalculateHash()`, kojom se dobiva *hash* prvog bloka na mreži. Jednostavna metoda `GetLatestBlock()` koristi se za dohvaćanje zadnjeg bloka u lancu. Dohvaćanje zadnjeg bloka koristi se kako bi se dohvatio njegov *hash* i postavio kao prethodni *hash* za trenutni blok. `AddNewBlock()` metoda je koja uz pomoć instance klase `Block` postavlja `PreviousHash`, poziva rudarenje bloka i nakon svega dodaje blok u lanac. Metoda `AddNewBlock()` prikazana je u kodu ispod.

  ```
  private void AddNewBlock(Block newBLock)
          { newBLock.PreviousHash = this.GetLatestBlock().Hash;
            newBLock.MineBlock();
            this.Chain.Add(newBLock);}
  ```

  Ulazni parametri metode `StartMining()` su konačan broj blokova koji će simulator izgenerirati i težina na mreži. For petlja ponavlja se onoliko puta koliki je konačan broj blokova. Poziva se metoda `AddNewBlock()` koja je prethodno objašnjena. `AddNewBlock()` metoda za ulazne parametre prima instancu klase `Block`, pa je potrebno poslati i tražene podatke. Kod koji slijedi prikazuje dodavanje bloka u lanac uz stvaranje nove instance klase `Block`.

```
this.AddNewBlock
                (
new Block(difficulty: difficulty,index: i, timeStamp:
DateTime.Now.ToString("dd.MM.yyyy HH:mm:ss") + "." +
DateTime.Now.Ticks,
                        data: new BlockTransactionData()
                        {
                            Seller = RandomString(5),
                            Buyer = RandomString(5),
                            Amount = new Random().Next(1, 50)
} ) );
```

Data su podatci koji će biti nasumično izgenerirani pomoću metode `Random()` i metode `RandomString()` koja na ulazu prima broj koji određuje duljinu izgenerirane riječi. `ChainValidator()` metoda provjerava povezanost blokova u lancu. Provjerava se svaki blok sa svojim prethodnim blokom na način da se provode tri provjere.

```
if (currentBlock.Hash != currentBlock.CalculateHash())
                { return false; }

if (currentBlock.PreviousHash != previousBlock.Hash)
                { return false; }

if (previousBlock.Hash!=previousBlock.CalculateHash())
                { return false; }
```

*Hash* trenutnog bloka mora biti isti ako se ponovo izračunava. Trenutni blok mora sadržavati *hash* prethodnog bloka koji je ispravan te se taj isti *hash* prethodnog bloka mora podudarati s ponovno izračunatim *hashem*, ako ga se računa s podatcima za prethodni blok. Metoda `RandomString()` nije od velike važnosti za funkcioniranje simulatora, već samo generira podatke za transakciju u obliku stringa. [8]

## 2.4. Pokretanje simulatora i rezultati

Simulator se jednostavno pokrene klikom na „Blockchain“ gumb za izvršavanje koda ili pritiskom tipke „F5“ na tipkovnici. Slika 9 prikazuje isječak iz konzolske aplikacije nakon pokrenutog programskog koda.

```
Index         : 0
Difficulty    : 0
Nonce         : 0
TimeStamp     : 13.09.2021 00:08:56.637670885363617015
Data          : {"Seller":"Genesis Block","Buyer":"Genesis Block","Amount":0}
Previous Hash: 0
Hash          : 901fad544e5a0d120d8b1b61452fb03cccd463b71e33a2d725bcdae3628b6091
Block Mined   : (0)

----------------------------------------------------------------
Mining new block......
Index         : 1
Difficulty    : 3
Nonce         : 816
TimeStamp     : 13.09.2021 00:08:56.637670885368947465
Data          : {"Seller":"UNQSK","Buyer":"IDGNA","Amount":14}
Previous Hash: 901fad544e5a0d120d8b1b61452fb03cccd463b71e33a2d725bcdae3628b6091
Hash          : 000ca97c6888a4696b7fc456b366b1b1aa65173a4ccffa07baf8c1b4fe657feb
Block Mined   : (1)

----------------------------------------------------------------
Mining new block......
Index         : 2
Difficulty    : 3
Nonce         : 2939
TimeStamp     : 13.09.2021 00:08:56.637670885369180954
Data          : {"Seller":"RCXEV","Buyer":"IMYOX","Amount":18}
Previous Hash: 000ca97c6888a4696b7fc456b366b1b1aa65173a4ccffa07baf8c1b4fe657feb
Hash          : 0002d1596e5e49f315a8a96d8cef3e1b9ece0c8192261185a57b2f4e12ee6e09
Block Mined   : (2)

----------------------------------------------------------------
Chain Validation: True
```

Slika 9 Isječak rezultata nakon pokretanja simulatora

Kako bi se bolje shvatio parametar težine na Bitcoin mreži, može se povećati vrijednost parametra Difficulty i pokrenuti simulator. Zatim se isto napravi s manjom vrijednošću za parametar Difficulty.

Postavit će se da simulator generira dva bloka i rezultate ćemo prikazati tablicom 1.

Tablica 1 Prikaz *noncea* povećanjem težine na mreži simulatora

| Difficulty | Blok | Nonce |
|---|---|---|
| | | |
| 1 | 1 | 16 |
| | 2 | 11 |
| | | |
| 3 | 1 | 829 |
| | 2 | 219 |
| | | |
| 5 | 1 | 1 573 522 |
| | 2 | 6 231 |

Rezultati prikazuju kako malim povećanjem težine na mreži *nonce* prikazuje višestruko veće vrijednosti. *Nonce* u simulatoru prikazuje vrijednost izračunatih *hasheva* koji nisu zadovoljili uvjete traženog *hasha*. Jednoznamenkasta vrijednost težine na mreži zahtjeva čak 7-znamenkastu vrijednost pokušaja generiranja prema rezultatima simulatora. Uzimajući u obzir rezultate simulatora, jasno je kako za rudarenje na Bitcoin mreži prema trenutnoj težini nije dovoljno koristiti obično računalo pa čak i više njih. Simulator je preuzet s linka koji je naveden u literaturi pod oznakom [21].

# 3. Ethereum

Ethereum je tehnologija koja omogućava izgradnju decentraliziranih aplikacija. Stvorio ga je Vitalik Buterin 2015. godine zajedno sa svojim timom blockchain razvojnih inženjera. Ethereum se često naziva kriptovalutom, što nije u potpunosti točno. Kriptovaluta koja stoji iza Ethereuma je Ether (ETH) i Etherom se plaćaju naknade za transakcije na Ethereum mreži. Simbol Ethereuma, ujedno i Ethera prikazan je na slici 10.

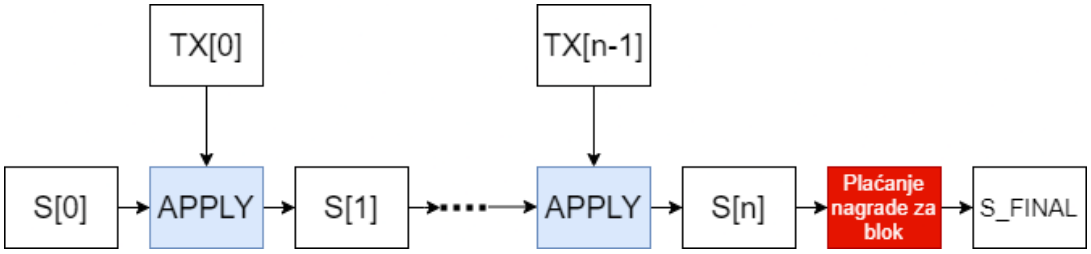
Slika 10 Simbol Ethereuma i kriptovalute Ether (izvor: https://hr.wikipedia.org/wiki/Ethereum#/media/Datoteka:Ethereum_logo_2014.svg)

Također, kao i kod Bitcoina, potrebna je računalna snaga kako bi se verificirale transakcije na Ethereum mreži i postavile na blockchain. Tehnologija koju pruža Ethereum temelji se na decentralizaciji, odnosno izradi pametnih ugovora i decentraliziranih aplikacija. Sve to omogućava blockchain s ugrađenim Turingovim programskim jezikom *(eng. Turing-complete programming language)*. Turing-complete programming language onaj je programski jezik na kojem se može izvršiti bilo koji algoritam. Aplikacije na Ethereum mreži izgrađuju se programskim jezikom Solidity. Izrada aplikacija i kriptovaluta na Ethereum mreži zamišljena je tako da bude što jednostavnija programerima i drugim korisnicima. Za razliku od Bitcoina, Ethereum nema ograničenu količinu Ethera koja se može stvoriti rudarenjem, već je ta količina neograničena. [9], [10], [11]

## 3.1. Ethereum blockchain i rudarenje

Blockchain Ethereuma vrlo je sličan Bitcoinovom blockchainu iako postoje razlike. Glavna razlika je u arhitekturi blockchaina. Blockchain Bitcoina sadrži samo kopiju svih transakcija dok Ethereum blockchain uz kopiju svih transakcija sadrži i trenutno, odnosno

najnovije stanje bloka. Osim toga, blok u Ethereum blockchainu sadrži i vrijednosti za broj bloka i težinu na mreži. Vrijeme potrebno za stvaranje bloka na Bitcoin blockchainu je otprilike 10 minuta dok se blokovi na Ethereum blockchainu generiraju svakih 15 sekundi. Kratko vrijeme generiranja novih blokova znači i brže izvršavanje transakcija što je od velike važnosti za kriptovalutu ukoliko bi postala platno sredstvo za što više korisnika. Algoritam za validaciju bloka na Ethereum blockchainu grafički je prikazan na slici 11.




Slika 11 Grafički prikaz algoritma za validaciju bloka na Ethereum blockchainu (slika je napravljena po uzoru na sliku sa web stranice https://ethereum.org/en/whitepaper/#philosophy, poglavlje: „Blockchain and Mining“)

Slijedi i detaljniji opis algoritma koji se izvršava u sljedećim koracima:

1. Provjerava se postoji li prethodno referencirani blok i je li ispravan.
2. Provjerava se vremenska oznaka prethodnog bloka koja mora biti manje od trenutne, a vremenska oznaka trenutnog bloka ne smije biti veća od 15 minuta u budućnost
3. Zatim se provjeravaju transakcije, broj bloka, korijen transakcije (*eng. transaction root)* i rodbinski korijen (*eng. uncle root* ) limit goriva za transakciju. Uncle root je korijen bloka koji nastaje kada dva rudara u isto vrijeme pripreme blok za validaciju. Uzrok tome je kašnjenje u postavljanju bloka na blockchain te samo jedan blok prolazi validaciju i postavlja se na blockchain.
4. Provjerava se validnost PoW algoritma
5. Ukoliko je sve do sada bilo ispravno, postavlja se zadnje stanje prethodnog bloka na varijablu `S[0]`.
6. Varijabla `TX` označava transakcije u bloku s `n` transakcija. Potrebno je provesti sljedeću provjeru: `za svaki i od 0 do n-1, postavi S[i+1] = APPLY(S[i],TX[i])`. „Apply“ je funkcija prijelaza stanja koja provjerava valjanost transakcije i podudaranje *noncea* kod pošiljatelja i primatelja te izračunava vrijednost naknade za transakciju. Ukoliko bilo koja provjera funkcije

vrati pogrešku ili ukupna naknada za transakciju ne prijeđe limit goriva, algoritam vraća pogrešku. Pojam „goriva“ na Ethereum mreži detaljnije je pojašnjen u odlomku 3.2

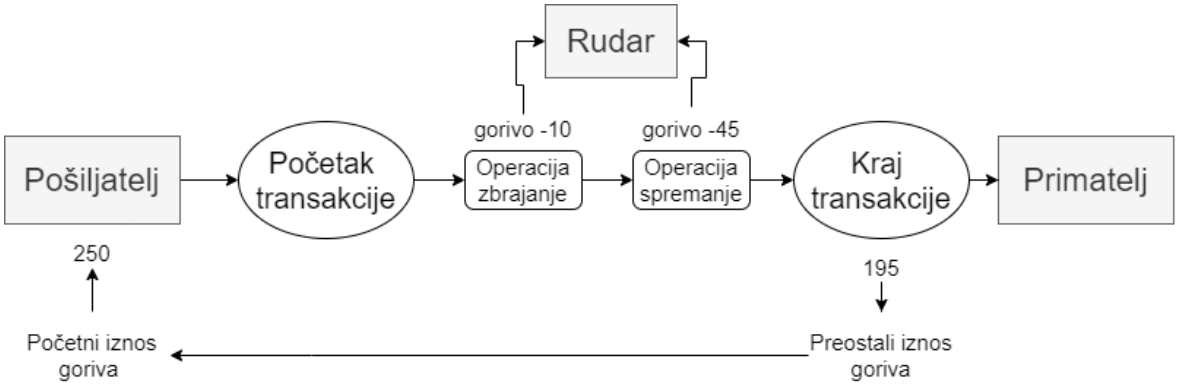
7. Zadnje stanje transakcija je `S[n]`, nakon kojeg slijedi nagrada za rudara te posljednje stanje bloka – `S_FINAL`.
8. Provjerava se korijen Merkle stabla koji mora biti jednak korijenu konačnog stanja, koji se nalazi u zaglavlju bloka. Ukoliko su jednaki, blok je valjan, u suprotnosti nije.

Pohranjivanje svih stanja u bloku ne čini se toliko učinkovitim, ali stanja bloka su također pohranjena u strukturu stabla. Nakon svakog bloka potrebno je promijeniti samo mali dio stabla jer su stanja između dva susjedna bloka u većini stabla jednaka. Stoga stanja mogu biti spremljena jednom, a pristupiti im se može dva puta korištenjem pokazivača odnosno *hasha* podstabla. Zbog toga se koristi posebna vrsta stabla – Patricia stablo. Patricia stablo je modifikacija Merkle stabla koja omogućava umetanje i brisanje čvorova, a ne samo njihovo mijenjanje. Stanja čine dio posljednjeg bloka pa nije potrebno pohranjivati cijelu povijest blockchaina.[9]

## 3.2. Ether

Ether je glavna kriptovaluta u Ethereum mreži kojom se plaćaju naknade za transakciju i nagrađuju rudari na mreži. Osim toga, Ether se može čuvati kao digitalna vrijednost, davati u zajam uz određenu kamatu, koristi se kao sredstvo plaćanja u određenim trgovinama i drugo. Kako bi shvatili način rada Ethereum mreže nužno je razumjeti pojam „goriva“ (*eng. fuel)* i pojam Ethereum virtualni stroj (*eng. Ethereum Virtual Machine*, skraćenica EVM) koji je pokrenut na svakom Ethereum mrežnom čvoru. EVM je emulacija računalnog sistema, odnosno računalni sistem u našem računalnom sistemu koji zauzima dio naših računalnih resursa (memorija, procesor, radna memorija i drugo). Operacije na EVM-u stoga je potrebno i platiti rudaru koji je na svoje računalo instalirao Ethereum čvor te pokrenuo EVM kako bi verificirao transakcije. Količina goriva određuje koliko će se minimalno morati platiti rudaru kako bi se uspjeli pokriti troškovi obrade transakcije. Svaka operacija na EVM-u troši određenu količinu resursa, stoga svaka operacija ima određenu cijenu. Složenije operacije svakako zahtijevaju više goriva. Korisnik Ethereum mreže može proizvoljno odabrati količinu goriva koju je spreman platiti ukoliko želi da se

njegova transakcija što brže izvrši. Rudar će u tom slučaju biti spreman verificirati najprije transakcije za koje će biti najviše plaćen. Slijed operacija i izvršavanje transakcija na Ethereum mreži prikazano je na slici 12.




Slika 12 Dijagram toka goriva tijekom izvršavanja transakcije na Ethereum mreži (slika je napravljena po uzoru na sliku sa web stranice https://preethikasireddy.medium.com/how-does-ethereum-work-anyway-22d1df506369)

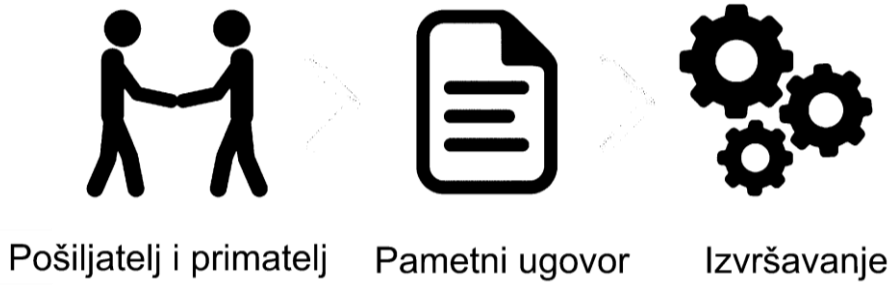
Vrijednost goriva izražava se u najmanjoj jedinici Ethera koja se naziva „wei“. Vrijednost jednog Ethera jednaka je 1 000 000 000 (bilijun) giga wei-a. Slika 13 prikazuje količinu goriva na Ethereum mreži potrebnu za izvršavanje transakcija.


Slika 13 Vrijednost goriva potrebna za transakcije na Ethereum mreži (podatci su preuzeti sa web stranice www.coinmarketcap.com 5.9.2021.)

Ovakav prikaz često se može vidjeti na stranicama koje pružaju informacije o kripto tržištu. Ukoliko želimo poslati Ether s jednog računa na drugi, moramo platiti 21 000 jedinica goriva. Kada bi cijena goriva bila jednaka 1 Gwei, iznos transakcije bi bio 0.000021 Ethera, odnosno 75 puta više s cijenom goriva od 75 Gwei. Plaćanje manjeg iznosa goriva nego što je potrebno dovodi do neuspjele transakcije. Dodatno se plaća i naknada za transakciju, koja je jednaka razlici količine početnog i preostalog goriva, multiplicirana za vrijednost cijene goriva. [12]

## 3.3. Pametni ugovori

Kriptograf Nick Szabo je devedesetih godina definirao pojam „Pametni ugovor“ kao: „skup obećanja, navedenih u digitalnom obliku, uključujući protokole u okviru kojih stranke izvršavaju druga obećanja“. Pojavom Bitcoina i decentraliziranih blockchain platformi taj izraz je evoluirao. Pametni ugovor (*eng. smart contract*) na Ethereum mreži unaprijed je programiran ugovor koji se samostalno izvršava, bez centralnog autoriteta. Ugovor kao takav nije niti pravni niti je „pametan“, ali je izraz ostao kao takav. Uvjeti ugovora napisani su u linijama koda programskim jezikom Solidity i javno su dostupni. Jednom implementiran ugovor ne može se više promijeniti. Ishod izvršavanja pametnog ugovora jednak je za svakoga tko ga pokrene, s obzirom na kontekst transakcije koja je započela njegovo izvršavanje i stanje Ethereum blockchaina u trenutku izvršavanja. Slika 14 ilustrira proces „sklapanja“ i izvršavanja pametnog ugovora.




Slika 14 Pojednostavljen prikaz procesa sklapanja i izvršavanja pametnog ugovora (slika je prerađena po uzoru na sliku https://www.forex.academy/the-top-5-smart-contracts-platforms/)

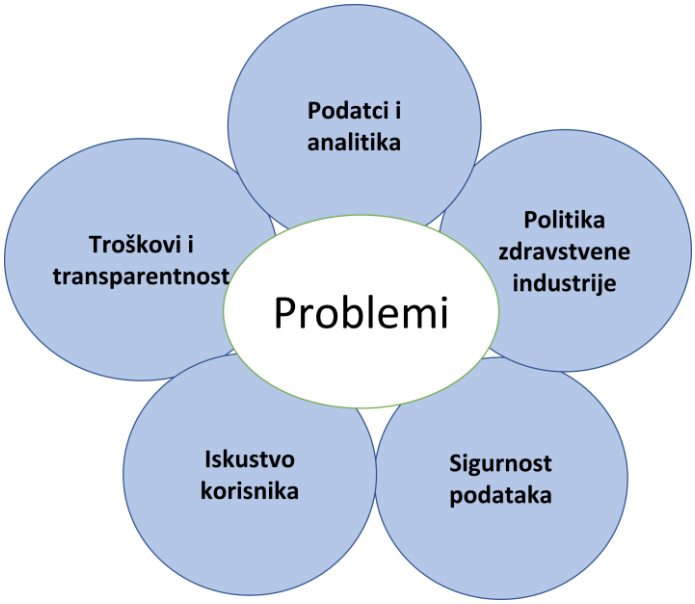
Pošiljatelj proizvoljno odabire iznos kriptovalute koju želi poslati primatelju te dobiva prijedlog o iznosu naknade za transakciju, goriva i vremenu u kojem će se transakcija izvršiti. Nakon toga primatelj klikom „potpisuje“ pametni ugovor i podatci se nakon validacije, koja je opisana u poglavlju 3.2, šalju na blockchain. Podatci o pametnom ugovoru također su javni na blockchainu i jednom izvršen ugovor nepovratan je. Pametni ugovori funkcioniraju s vrlo ograničenim kontekstom izvršavanja. Mogu pristupiti vlastitom stanju, kontekstu transakcije koja ih je pozvala na izvršavanje i nekim podacima o najnovijim blokovima. Softver koji izvršava pametne ugovore na Ethereum mreži je Ethereum Virtual Machine. EVM radi kao lokalna instanca na svakom Ethereum čvoru, ali budući da sve instance EVM-a rade na istom početnom stanju i proizvode isto završno stanje, sustav u cjelini djeluje kao jedno "svjetsko računalo". [9], [10], [20]

# 4. Druge primjene blockchain tehnologije

Blockchain tehnologija, zbog svojih karakteristika, pronalazi primjenu i u mnogim drugim primjerima. Velike količine podataka predstavljaju sve veći problem te je potrebno primijeniti tehnologiju koja brzo i efikasno izvršava rad s velikim količinama podataka. Također, ti isti podatci trebaju biti na sigurnom mjestu i dostupni određenim pojedincima ili skupinama korisnika.

## 4.1. Blockchain tehnologija u zdravstvenoj industriji

Posljednjih 30 godina zdravstvena industrija je pogođena pojavom centraliziranih podatkovnih sustava, regulacijom zdravstvenih podataka i mandatom da se usredotoči na digitalizaciju medicinskih podataka s različitim pružateljima usluga elektroničkih zdravstvenih kartona (*eng. electronical medical record*, skraćenica EMR). Problemi s kojima se suočava zdravstvena industrija prikazani su na slici 15.




Slika 15 Problemi u zdravstvenoj industriji prikazani Vennovim dijagramom (slika je prerađena po uzoru na sliku sa web stranice: https://www.slideshare.net/aryausa/healthcare-industry-237321061, slajd 3)

Većina spremišta u vlasništvu je pružatelja zdravstvenih usluga, farmaceutskih tvrtki i drugih sudionika u zdravstvenom i medicinskom sustavu koji uglavnom nisu međusobno povezani. Manjak komunikacije i povezanosti u sistemu koje sadrži zdravstvene podatke

na razini pojedinca i stanovništva (javno zdravstvo) nailazi na prepreke u sljedećim situacijama:

- Kada se pacijenti žele posavjetovati ili zatražiti medicinske usluge od drugih pružatelja zdravstvene zaštite.
- Kada administratori kliničkog ispitivanja žele potvrditi ogromne količine podataka sudionika.
- Kada farmaceutske tvrtke žele osigurati autentičnost lijekova koji cirkuliraju svjetskim tržištima.

Ponekad zbog nemogućnosti sigurne razmjene podataka i privremenog upravljanja medicinskom dokumentacijom, pacijenti troše vrijeme i resurse tražeći suvišnu medicinsku skrb (npr. ponovno obavljanje krvnih pretraga). U hitnim situacijama, liječnici i drugi zdravstveni djelatnici koji pružaju njegu možda neće imati potpunu preglednost povijesti bolesti pacijenta (npr. dokumentacija za alergije pacijenta, prethodna zdravstvena stanja itd.) te može doći do nepravilnog liječenja. Potrebno je i sigurno praćenje lanca opskrbe lijekova kako bi se spriječila distribucija zabranjenih ili neautentičnih lijekova. Blockchain tehnologija predstavlja priliku za sigurno praćenje, označavanje kronologije i isticanje identifikacijskih podataka tvari u nepromjenjivom zapisu. [15]

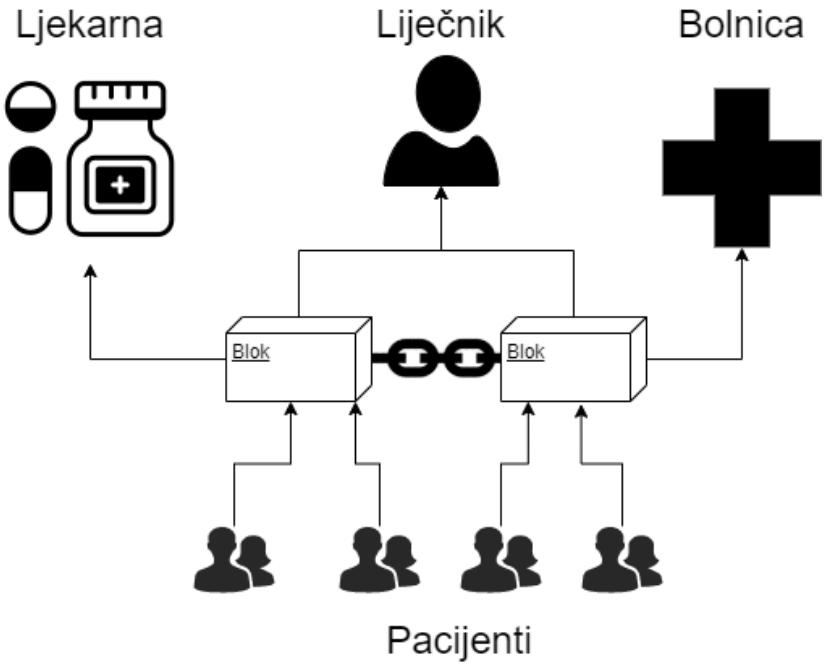
### 4.1.1. Enterprise Ethereum

Ethereum za poduzetnike (*eng. Enterprise Ethereum*) odnosi se na definirani skup smjernica i tehničkih specifikacija za ubrzanje usvajanja blockchain tehnologije među poduzećima. Specifikacije pružaju tvrtkama mogućnost iskorištavanja privatnih lanaca zasnovanih na Ethereumu i glavnoj javnoj mreži. Privatni lanac na Ethereumu zahtjeva posebno odobrenje da bi se pristupilo podatcima. Enterprise Ethereum specifikaciju održava Enterprise Ethereum Alliance (EEA), članica blockchaina i postojećih tvrtki iz cijelog svijeta. Quorum je Enterprise Ethereum rješenje tvrtke ConsenSys. Koristeći smjernice i specifikacije Enterprise Ethereuma koje je odredio EEA, ConsenSys Quorum izgrađen je kako bi zadovoljio potrebe poduzeća za rješenjima i aplikacijama temeljenim na blockchainu. Pomoću protokola Enterprise Ethereum otvorenog koda ConsenSys Quorum, tvrtke mogu izgraditi visokoučinkovita rješenja s nizom prilagodljivih modula

proizvoda. ConsenSys Solutions radi s nizom blockchain proizvoda koji se mogu prilagoditi različitim zdravstvenim aplikacijama, uključujući sljedeće:

- Sigurno upravljanje elektroničkim zdravstvenim kartonima
- Upravljanje pristankom pacijenata
- Utvrđivanje podrijetla i provjera lijekova.
- Sigurnost podataka u kliničkim ispitivanjima
- Poticaji putem mikroplaćanja

Sigurnost elektroničkih zdravstvenih kartona tijekom razmjene među zdravstvenim ustanovama i djelatnicima će osigurati decentralizirane baze podataka. Takve strukture rade na zaštiti podataka i privatnosti pacijenata, omogućuju liječnicima uvid u povijest bolesti njihovih pacijenata, te osnažuju istraživače da koriste zajedničke podatke za poticanje znanstvenog napretka. Slika 16 prikazuje povezanost zdravstvenih djelatnika i ustanova s pacijentima pomoću blockchain tehnologije.




Slika 16 Povezanost zdravstvenih institucija i pacijenata blockchain tehnologijom

Blockchain rješenja omogućuju vlasništvo strukturiranih podataka putem slojeva privatnosti i dopuštenja ugrađenih u Ethereumu. Iako pacijenti ne mogu promijeniti ili izbrisati određene medicinske podatke koje liječnici unesu na svoje profile, oni mogu kontrolirati pristup dajući potpunu ili djelomičnu vidljivost različitim sudionicima u sustavu zdravstvene zaštite. Na primjer, pacijenti mogu podijeliti svoju potpunu evidenciju

sa liječnikom specijalistom, ali mogu odlučiti podijeliti samo podatke koji se ne mogu identificirati sa znanstvenim istraživačkim tvrtkama ili drugim većim zdravstvenim organizacijama. Upravljanje lancem opskrbe lijekovima postaje sigurnije i odgovornije uz transparentnost, nepromjenjivost i interoperabilnost koju je uveo Enterprise Ethereum. Interoperabilnost između mreža osigurava da različite blockchain aplikacije i sustavi duž opskrbnog lanca mogu koherentno međusobno djelovati. Stoga farmaceutske tvrtke mogu registrirati svoje proizvode na blockchainu i pratiti kretanje od izvorne točke do krajnjeg potrošača. Enterprise Ethereum smanjuje rizik od lažnih podataka svojim mehanizmom konsenzusa i decentraliziranom strukturom koja štiti od hakiranja ili manipulacije. Dokumentima se može dati dokaz o postojanju i provjera autentičnosti na blockchainu. Većina čvorova tada postiže konsenzus za odobravanje novih transakcija i sprječavanje izmjene podataka. Time se štiti integritet podataka, promiču pouzdani rezultati ispitivanja i potiče suradnja među istraživačkom zajednicom. Pametni ugovori na Enterprise Ethereumu omogućuju uvođenje mikroplaćanja kako bi se potaknulo specifično ponašanje pacijenata. Ovi se ugovori mogu programirati za nagrađivanje pacijenata koji slijede određeni plan liječenja ili dijele svoje podatke za klinička istraživanja. [15], [16]

## 4.2. Glasanje pomoću blockchain tehnologije

Većina država, izbore za predsjednika ili parlament održava javno, glasanjem biračkim mjestima koja su predodređena građanima. Pri glasanju potrebno je priložiti odgovarajući dokument i potvrditi svoj identitet. Zatim se dobije olovka i papir te se zaokruži broj željenog kandidata. Osoba koja se ne nalazi u mjestu prebivališta po kojemu se dodjeljuje biračko mjesto mora preuzeti poseban dokument kako bi promijenila svoje biračko mjesto. Nakon isteka vremena za glasanje, glasovi se moraju prebrojati i provjeriti valjanost glasačkih listića. Posao brojanja odrađuju ljudi koji moraju biti iz različitih stranaka te moraju biti nadgledani od strane određenog državnog tijela za provjeru glasačkih mjesta. Sve navedeno su zastarjele tehnike koje se mogu zamijeniti elektroničkim glasanjem. Na primjer, istraživanje u Brazilu pokazalo je da je usvajanje elektroničkog glasanja povećala izlaznost ljudi na izbore što je kao rezultat dovelo do povećanja državnog proračuna za zdravstvene usluge. Strahovi od velikih manipulacija glasanjem putem interneta spriječili su napredak u donošenju promjena. Vrlo mali broj zemalja uopće koristi glasanje putem interneta, a većina njih koristi neku verziju elektroničkih glasačkih uređaja koja zahtijevaju od glasača da posjete na biračko mjesto i pokažu identifikacijski dokument prije nego što

unesu svoj glas na uređaj. Velika prednost glasanjem pomoću glasačkih uređaja je brzina brojanja glasova, posebno u velikim zemljama poput Indije i Brazila. Također, uređaji su dodatno smanjili troškove održavanja izbora. Iako su strojevi doveli poboljšanje i napredak tijekom izbora i dalje je potrebno otići na biračko mjesto gdje se nalazi uređaj za glasanje. Slika 17 prikazuje jedan takav glasački uređaj koji se sastoji od upravljačke jedinice za identifikaciju i jedinice za glasanje („glasački listić“).


Slika 17 Izgled elektroničkog stroja za glasanje (slika je prerađena po uzoru na sliku sa web stranice https://www.iitk.ac.in/gymkhanaGJ/?page_id=89)

Nasuprot tome, mnoge zrele demokracije nisu prihvatile glasanje na internetu zbog straha od hakiranja i prijevare. Neke su zemlje aktivno prestale koristiti (npr. Nizozemska 2005.). Jedno od mogućih rješenja je blockchain tehnologija. U travnju, 2019. godine u Sjedinjenim američkim državama pokrenut je probni projekt glasanja pomoću blockchain tehnologije. Projekt koristi sustav glasovanja u vlasništvu Službe za reformu izbora zajedno s projektom otvorenog koda „Verify My Vote“ za provjeru glasova. Blockchain tehnologija koja podržava ovu platformu omogućuje glasačima da provjere da li se njihovi glasovi prebrojavaju i da li su glasovi ispravno zabilježeni bez ugrožavanja vlastite anonimnosti. Štoviše, svatko može provjeriti je li prebrojavanje obavljeno ispravno bez ugrožavanja tajnosti glasačkih listića. Iako jedno tijelo (Civica) nadzire trenutni centralizirani sustav glasovanja na svojim izborima, sada je moguće raspodijeliti kontrolu izbora među nekoliko povjerenika, što bi moglo povećati povjerenje birača u rezultate. Način funkcioniranja blockchain tehnologije koji zahtjeva provjeru validnosti glasova od

strane više tijela znatno otežava manipulaciju na izborima. Više provjera validnosti glasova „povećava cijenu“ prijevare na izborima, odnosno velik broj sudionika bi se morao udružiti kako bi manipulirao podatcima. U ovlaštenom sustavu validatori (rudari) bi bili poznati biračima. Na primjer, predstavnici stranaka iz različitih stranaka osigurali bi povjerenje u sustav. Osim toga, sustav temeljen na blockchainu može omogućiti neovisnim tijelima za praćenje glasova reviziju prebrojanih glasova i kodova koji se koriste kako bi bili sigurni da je sustav bez prijevara - nešto što trenutni centralizirani sustavi ne nude. Blockchain tehnologija se može uključiti u arhitekturu glasanja već od faze registracije birača do pohrane i prebrojavanja glasova. U svakoj fazi sprječavaju jednog birača da izvrši izmjene bez dogovora među određenim podskupom cijele mreže ovlaštenih validatora. Nedostatak ovih dodatnih sigurnosnih provjera je trošak pokretanja dodatnih poslužitelja. Ipak, blockchain tehnologija ne može riješiti sve moguće vrste izbornih prijevara. Mreža ovlaštenih validatora ne može provjeriti dolaze li glasovi od pravih korisnika, ali može provjeriti druge ključne nedoumice: da je glasanje tehnički valjano, da se ne događa dvostruko prebrojavanje i da glasovanje dolazi s ovlaštenog mjesta. U Estoniji, na primjer, birači mogu glasati sa bilo kojeg mjesta u svijetu koristeći osobnu iskaznicu s mikročipom koji se može pročitati čitačem kartica. Također postoji mogućnost da je biračevo računalo izloženo zlonamjernom softveru. [18]

## 4.3. Blockchain i umjetna inteligencija

Blockchain tehnologija i umjetna inteligencija (*eng. Artificial Intelligence,* skraćenica AI) su dvije tehnologije u razvoju koje su sve popularnija tema današnjice. Blockchain tehnologija, kao raspodijeljeni decentralizirani sustav za čuvanje šifriranih podataka, imao bi koristi od „surađivanja“ s umjetnom inteligencijom. Umjetna inteligencija bi bila „mozak“ u situacijama kada je potrebno usmjeriti velike količine podataka i raditi s istima. Štoviše, umjetna inteligencija može poboljšati učinkovitost blockchaina daleko bolje od ljudi. Način na koji se blockchain tehnologija trenutno izvodi na standardnim računalima dokazuje to da je puno računalne snage potrebno za obavljanje čak i osnovnih zadataka. Umjetna inteligencija pruža nam mogućnost da se odmaknemo od toga i rješavamo zadatke na inteligentniji i učinkovitiji način. Na primjer, algoritmi za *hashiranje* koriste računalnu snagu kako bi provjerili sve potencijalne kandidate i zadovoljavaju li oni određene uvjete prije validacije transakcija. Algoritam baziran na strojnom učenju bi puno učinkovitije rješavao navedeni problem uz odgovarajuću „pripremu“. SinguarlityNET je posebno

usmjerena platforma za korištenje blockchain tehnologije za poticanje šire distribucije podataka i algoritama, pomažući u osiguravanju budućeg razvoja umjetne inteligencije i stvaranju „decentraliziranog AI-a“. Pogodnosti koje pruža SingularityNET prikazane su na slici 18.


Slika 18 Pogodnosti SingularityNET-a (slika je prerađena po uzoru na sliku s web stranice: https://singularitynet.io/)

SingularityNET kombinira blockchain i AI za stvaranje pametnijih, decentraliziranih AI blockchain mreža koje mogu zadržati različite skupove podataka. Napredak AI-a u potpunosti ovisi o unosu podataka. Putem podataka AI prima informacije o svijetu i stvarima koje se na njemu događaju. Zapravo, podaci hrane AI, te će se AI moći kontinuirano poboljšavati. S druge strane, blockchain kao tehnologija koja omogućuje šifrirano skladištenje podataka na distribuiranoj knjizi, omogućuje stvaranje potpuno zaštićenih baza podataka koje mogu pregledati stranke kojima je to odobreno. Kad kombiniramo blockchain tehnologiju s AI, imamo sigurnosni sustav za osjetljive i visoko vrijedne osobne podatke pojedinaca. [19]

# Zaključak

Proučavajući blockchain u kriptovalutama dolazimo do zaključka kako blockchain tehnologija osigurava privatnost, anonimnost, decentralizaciju, sigurnost, javnost transakcija te ono najbitnije: dobar temelj za izgradnju boljih protokola i tehnologija u svijetu kriptovaluta. Bitcoin kao prvi predstavnik kriptovaluta i blockchain tehnologija postaje sve popularniji i njegova vrijednost raste. Većih promjena u protokolu po kojem djeluje Bitcoin mreža nije utjecala na srž djelovanja blockchain tehnologije što ukazuje na dobru početnu ideju koja već 13 godina pokazuje kako nije samo jedna u nizu od prijevara na financijskom tržištu. Problem predstavlja što decentralizirani sustav, pojavom ASIC strojeva, gubi na decentralizaciji. Takvi strojevi su vrlo skupi što povlači činjenicu da će samo oni koji su se u prošlosti obogatili rudarenjem ili kupovinom Bitcoina biti još bogatiji. S druge strane, udruživanje rudara u mining poolove također smanjuje decentralizaciju mreže. Problemi nastaju i kod potrošnje električne energije potrebne za rudarenje Bitcoina, iako je ona nezanemariva s potrošnjom električne energije u sličnim sustavima koje bi Bitcoin ili slična mreža mogla zamijeniti (npr. potrošnja struje svih banaka i bankomata) često se prikazuje kao velik problem u medijima. S druge strane, Ethereum je stvoren kao mreža koja se može širiti, primati nove tehnologije, pruža razne usluge djelatnicima, omogućava izgradnju raznih aplikacija i drugo. Ideja Ethereuma da unaprijedi nedostatke Bitcoina i proširi djelovanje blockchaina je zasigurno uspjela. Ethereum je malim izmjenama u funkcioniranju blockchain tehnologije omogućio puno brže izvršavanje transakcija na mreži. Problem Ethereuma je prevelik promet mreže jer u slučaju kupovine drugih kriptovaluta na mreži naknada za transakcije poprima višestruko veće iznose. Ažuriranje protokola, koje se naziva Ethereum 2.0, pokušava riješiti problem velikih iznosa transakcija i sličnih stvari. Primjerom djelovanja blockchain tehnologije u zdravstvu i prilikom glasanja na izborima vidi se kako bi se takva tehnologija mogla upotrijebiti u raznim sektorima ljudske djelatnosti. Izraz „digitalizacija sustava“ je sve popularniji u svijetu te je potrebno osigurati da takvi sustavi funkcioniraju. Blockchain tehnologija može pronaći primjenu u mnogobrojnim sustavima i pružiti im kvalitetno i olakšano djelovanje pomoću umjetne inteligencije. Umjetna inteligencija može biti nevjerojatno revolucionarna, ali mora biti dizajnirana s najvećim mjerama opreza u čemu blockchain tehnologija u može uvelike pomoći.

# Literatura


[1] Berkeley, *Applied Innovation Review* Issue No. 2 June 2016, http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

[2] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://Bitcoin.org/bitcoin.pdf

[3] Investopedia, https://www.investopedia.com/terms/b/blockchain.asp

[4] Blockchain.Com, https://www.blockchain.com/charts/difficulty

[5] Ivan on tech academy, https://academy.ivanontech.com/blog/byzantine-generals-problem-an-introduction

[6] Alibaba Cloud, https://www.alibabacloud.com/blog/comprehensive-review-of-proof-of-work-consensus-in-blockchain_597042

[7] Microsoft – a tour of C# language https://docs.microsoft.com/en-us/dotnet/csharp/tour-of-csharp/

[8] Microsoft – Cryptographic Services, https://docs.microsoft.com/en-us/dotnet/standard/security/cryptographic-services

[9] Ethereum whitepaper, https://ethereum.org/en/whitepaper/#ethereum

[10] Investopedia, https://www.investopedia.com/terms/e/ethereum.asp

[11] DEV community, https://dev.to/gruhn/what-makes-a-programming-language-turing-complete-58fl

[12] EthHub, https://docs.ethhub.io/

[13] W3schools, https://www.w3schools.com/charsets/ref_html_utf8.asp

[14] General Information, https://unicode.org/standard/WhatIsUnicode.html

[15] Consensys, https://consensys.net/blockchain-use-cases/healthcare-and-the-life-sciences/

[16] Consensys, https://consensys.net/enterprise-ethereum/

[17] 101 Blockchains, https://101blockchains.com/history-of-blockchain-timeline/

[18] LSE Phelam US centre, https://blogs.lse.ac.uk/usappblog/2020/09/25/long-read-how-blockchain-can-make-electronic-voting-more-secure/

[19] BBVA Openmind, https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/

[20] Investopedia, https://www.investopedia.com/terms/s/smart-contracts.asp

[21] asecer79, *BlockChain Simulator*, https://github.com/asecer79/BlockChainSimulator

# Skraćenice

| | | |
|---|---|---|
| PoW | *Proof of work* | Dokaz o radu |
| USB | *Universal serial bus* | Univerzalna serijska sabirnica |
| ASIC | *Application-Specific Integrated Circuit* | Integrirani krug specifične primjene |
| JSON | *JavaScript Object Notation* | JavaScript notacijski objekt |
| EVM | *Ethereum Virtual Machine* | Ethereum virtualni stroj |
| UTF-8 | *Unicode Transformation Format – 8 bits* | Unicode format za transformaciju |
| EMR | *Electronical Medical Record* | Elektronički zdravstveni karton |
| EEA | *Enterprise Ethereum Alliance* | Enterprise Ethereum savez |
| AI | *Artifical Intelligence* | Umjetna inteligencija |