Blockchain i kriptovaluta Etherum i Litecoin

Malbašić, Rino

Sveučilište Jurja Dobrile u Puli
Fakultet Informatike u Puli

Rino Malbašić

Blockchain i kriptovalute Ethereum i Litecoin

Blockchain and cryptocurrency Ethereum and Litecoin

Pula, rujan, 2023. godine

Završni radSveučilište Jurja Dobrile u Puli
Fakultet Informatike u Puli

Rino Malbašić

Blockchain i kriptovalute Ethereum i Litecoin

Blockchain and cryptocurrency Ethereum and Litecoin

Završni rad

JMBAG: 0303082500, redoviti student

Studijski smjer: Informatika

Kolegij: Informacijska Tehnologija i društvo

Znanstveno polje: Informacijske i komunikacijske znanosti Znanstvena grana: Informacijski sustavi i informatologija

MENTOR: doc. dr. sc. Snježana Babić

Pula, rujan, 2023. godine

Sadržaj

UVOD

Predmet istraživanja

Prve transakcije svih oblika pojavile su se s pojavom čovjeka. Zamjena robe za robu iznjedrila je određene predmete koji su bili poželjnije platežno sredstvo od drugih. Vremenom su plemeniti metali preuzeli ulogu platežnog sredstva te oblikovanjem istih u kovanice, njihova se realna vrijednost mogla mijenjati za vrijednost robe. Razvojem trgovine, pojavile su se i prve novčanice koje su imale nominalnu vrijednost i predstavljale su zamjenu za realnu vrijednost zlata. Na taj su način ljudi preuzeli sustav plaćanja roba i usluga temeljen na uzajamnom dogovoru i prihvaćanju nominalnih vrijednosti novčanica. Zahvaljujući sve razvijenijoj trgovini, bankarstvo je pratilo zahtjeve vremena te je efektivni novac ustupao mjesto knjižnom novcu dok se pravi novac sve više povlačio iz opticaja. Pojava interneta rezultirala je i razvojem elektroničkog novca koji se temelji na raznim karticama s ugrađenim čipovima i softverskom podlogom te postoji samo kao elektronski zapis.

Blockchainovi i kriptovalute su iduća nova razina razvoja bilježenja financijskih transakcija. Za razliku od dosadašnjeg centraliziranog načina plaćanja transakcija putem raznih financijskih institucija koje podliježu kontroli središnje banke i države, kriptovalute predstavljaju decentralizirani način bilježenja transakcija koji ne ovisi i ne podliježe kontroli niti jedne institucije već se temelji na jedinstvenom bilježenju svih prošlih transakcija koje se povezuju u jedinstveni nepromjenjivi niz.

Cilj rada

Cilj ovog rada je prikazati okolnosti u kojima je nastao koncept blockchaina i povijesni razvoj, njegovu strukturu, tehnologiju i osobine te uvjete postojanja. Blockchain tehnologiju koristi velik broj raznih kriptovaluta, ali prvu primjenu imala je pojavom Bitcoina. U radu je opisan razvoj kriptovalute Litecoin koja je nastala kao težnja za uklanjanjem tadašnjih nedostataka Bitcoina i pojava Ethereuma koji je nastao iz iste težnje za uklanjanjem nedostataka tadašnjih *peer-to-peer* tehnologija, ali koji je osuvremenio i proširio primjenu blockchaina pametnim ugovorima. Osim navedenog, cilj ovog rada je i usporedba Litecoina i Ethereuma koja se neminovno provlači kroz čitav rad i koja će se sumirati u zadnjem dijelu rada.

Blockchain se može poistovjetiti s lancem što „chain“ zapravo i znači. Umjesto metalnih karika koje se povezuju, u blockchainu su povezane baze podataka ili podatkovni blokovi. Lanac je jednosmjeran i svaka sljedeća veza ovisi o prijašnjoj, nadovezuje se na nju i postaje njen nepromjenjivi sastavni dio.

Neki ga nazivaju i digitalnom knjigom transakcija koja se multiplicira i distribuira po cijeloj mreži računalnih sustava na blockchainu. To znači da se svaki put nakon nove transakcije na blockchainu, u knjigama svih sudionika dodaje zapis te transakcije. Sustav blockchainova se dalje ubrzano razvija. Pojedine su kriptovalute ostale na temeljnoj tehnologiji dok su nove digitalne valute dodatno ojačale i razvile blockchainove na način da se, osim transakcija, mogu bilježiti i drugi podaci i aplikacije.

Cilj ovog rada je prikazati razvoj i način djelovanja blockchaina te usporediti Litecoin i Ethereum, njihove sličnosti, prednosti i nedostatke.

1. Blockchain

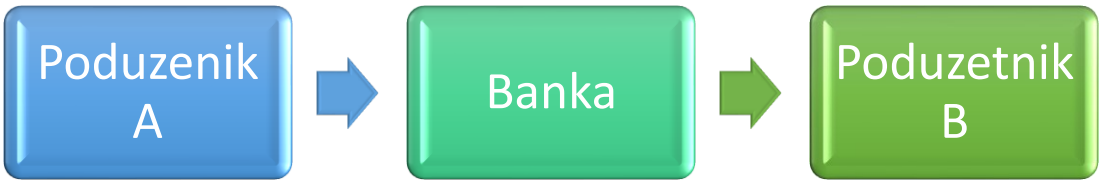
Termin blockchain može se na hrvatski jezik prevesti kao lanac blokova. Blokovi su organizirani skupovi podataka i predstavljaju zaokruženu cjelinu. Ti se blokovi međusobno spajaju u dugi neprekinuti lanac. Svaki novi blok nadovezuje se na posljednji blok u lancu te postaje njegova nova karika čija vrijednost ovisi o vrijednosti posljednjeg bloka u lancu na kojeg se nadovezao. Kako bi se podaci u blokovima, a time i čitav lanac, sigurnosno zaštitili, primjenjuje se kriptografija kao metoda prijevoda razumljivog i čitjivog teksta u kriptirani tj. šifrirani tekst kojeg je moguće opet vratiti u prvobitno čitljivo stanje ukoliko se posjeduje ključ za odgonetanje šifri. Taj se postupak naziva dekriptiranje ili dešifriranje. Prošlost obiluje primjerima kriptiranja poruka među kojima se ističu pisma koja je Julije Cezar slao Ciceronu i *Enigma* – elektromehanički stroj za šifriranje poruka kojeg je izumio inženjer elektrotehnike dr. Arthur Scherbius i kojeg je njemačka tvrtka *Scherbius & Ritter* patentirala davne 1919. godine (Čavrak, n.d.).

Radovi o kriptografski povezanim blokovima pojavili su se još početkom 90-tih godina. Prvi rad u kojem je opisan koncept blockchaina objavljen je 2008. godine na mrežnoj stranici *bitcoin.org* pod nazivom “Bitcoin: A Peer-to-Peer Electronic Cash System”. Autor ili autori stranice bio je pojedinac ili grupa pod pseudonimom Satoshi Nakamoto. Sve istrage koje su

provedene s ciljem utvrđivanja je li Satoshi prava osoba, skupina ili organizacija, završile su neuspjehom (Arunović, 2018.).

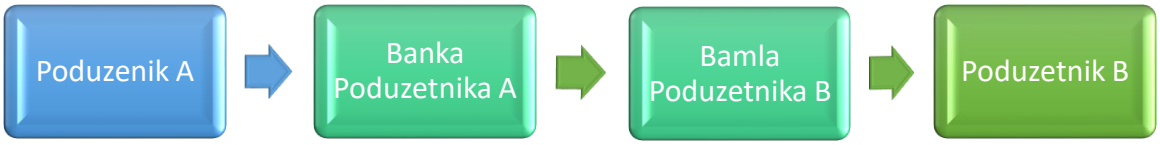
Blockchain je tehnologija koju možemo nazvati i digitalnim knjigovodstvom. Blockchain je distribuirana baza podataka ili knjiga transakcija koja se dijeli između čvorova računalne mreže. Čvor može biti bilo koji uređaj koji može primati, slati ili prosljeđivati informacije poput računala ili mobilnog telefonskog uređaja. Čvorovi računalne mreže mogu biti redistribucijske točke ili krajnje komunikacijske točke. Njihova definicija ovisi o mreži i sloju protokola o kojem se govori. Kao baza podataka, blockchain pohranjuje informacije elektronički u digitalnom formatu. Blockchaini su najpoznatiji po svojoj ključnoj ulozi u sustavima kriptovaluta, kao što je Bitcoin, za održavanje sigurne i decentralizirane evidencije transakcija. Inovacija blockchaina jamči točnost i sigurnost zapisa podataka.

Način funkcioniranja blockchaina može se objasniti na primjeru jednostavne novčane transakcije. Poduzetnik A želi podmiriti dugovanje bezgotovinskom transakcijom Poduzetniku B. Kako bi to učinio, Poduzetnik A mora dati nalog vlastitoj banci u kojoj ima otvoren račun i dovoljno financijskih sredstava na njemu da odobri odnosno izvrši prijenos određenog iznosa na račun Poduzetnika B čiji račun može biti u istoj ili nekoj drugoj banci. Nakon što je Poduzetnik A dao nalog, transakciju će izvršiti jedna banka u prvom slučaju (Slika 1), odnosno dvije banke u drugom (Slika 2) i o tome obavijestiti vlasnike računa.



Slika 1. *Primjer transakcije u slučaju kada oba poduzetnika imaju račun u istoj banci (prikaz autora rada)*

Poduzetnik A daje nalog banci da na njegov teret izvrši transakciju u korist Poduzetnika B. U izvršenju transakcije pojavljuje se jedna banka kao posrednik.

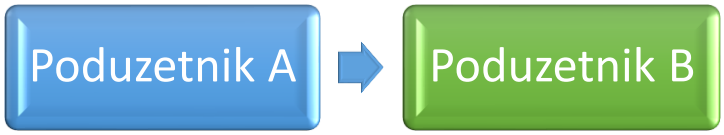


Slika 2. *Primjer transakcije u slučaju kada poduzetnici imaju račun u različitim bankama (prikaz autora rada)*

Poduzetnik A daje nalog vlastitoj banci da izvrši transakciju prema Poduzetniku B koji ima račun u drugoj banci. U tom se slučaju pojavljuju dva posrednika odnosno dvije banke koje sudjeluju u izvršenju transakcija.

U oba primjera, poduzetnici moraju koristiti usluge banke i imati povjerenja da će banke izvršiti njihove naloge. Banka ili banke pojavljuju se u ulozi posrednika u izvršavanju transakcija te odlučuju kako i po kojoj cijeni će izvršiti naloge što im osigurava veliku moć i izvor zarade.

Blockchain tehnologija omogućava izostavljanje trećih osoba u izvršavanju transakcija te se zbog toga smatra u potpunosti decentraliziranim načinom bilježenja transakcija. Izostavimo li banke iz prethodnog primjera, blockchain tehnologiju možemo prikazati na sljedeći način (Slika 3):



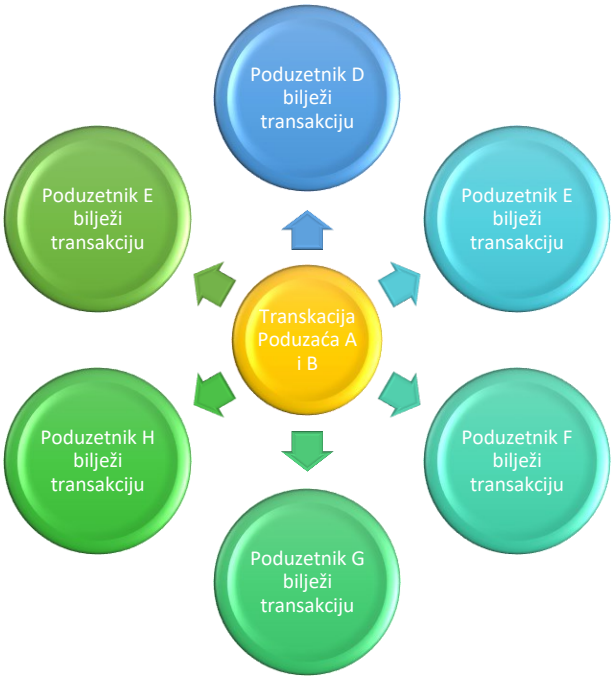
Slika 3. *Prikaz direktnog izvršenja transakcija bez posrednika (prikaz autora rada)*

Transakcija se izvršava na teret Poduzetnika A odobravanjem računa Poduzetnika B bez ikakvih institucija ili drugih subjekata koji preuzimaju ulogu posrednika u izvršavanju transakcija.

Postavlja se pitanje sigurnosti transakcija koje se provode bez posrednika koji jamče sigurnost, zakonitost i istinitost događaja. U navedenom slučaju poduzetnici moraju povjerenje preusmjeriti s banke na drugog poduzetnika, a to isto povjerenje se može lako izigrati. Banke su igrale ulogu svjedoka u transakcijama. U blockchain tehnologiji ulogu banaka-svjedoka preuzimaju drugi „poduzetnici“ ili sudionici u procesu stvaranja i trgovanja kriptovalutama.

Uvedemo li u naš prikaz još četiri poduzetnika C, D, E i F koji će u vlastitim sustavim bilježiti spomenutu transakciju, krug bilježenja provedene transakcije, a time i krug povjerenja širi se na veći broj sudionika (Slika 4). U takvim okolnostima nemoguće je falsificirati ili na bilo koji način malverzirati transakciju jer je ona zabilježena na četiri računala. Želi li jedan sudionik lažirati transakciju morao bi to učiniti na sva četiri računala što je gotovo nemoguće. Uvedemo li u naš primjer stotine ili tisuće poduzetnika koji koriste blockchain tehnologiju i na čijim se računalima, govorimo o tisućama računala, bilježe sve njihove međusobne transakcije, nemoguće je izvršiti bilo kakvu istu malverzaciju na svim tim računalima.

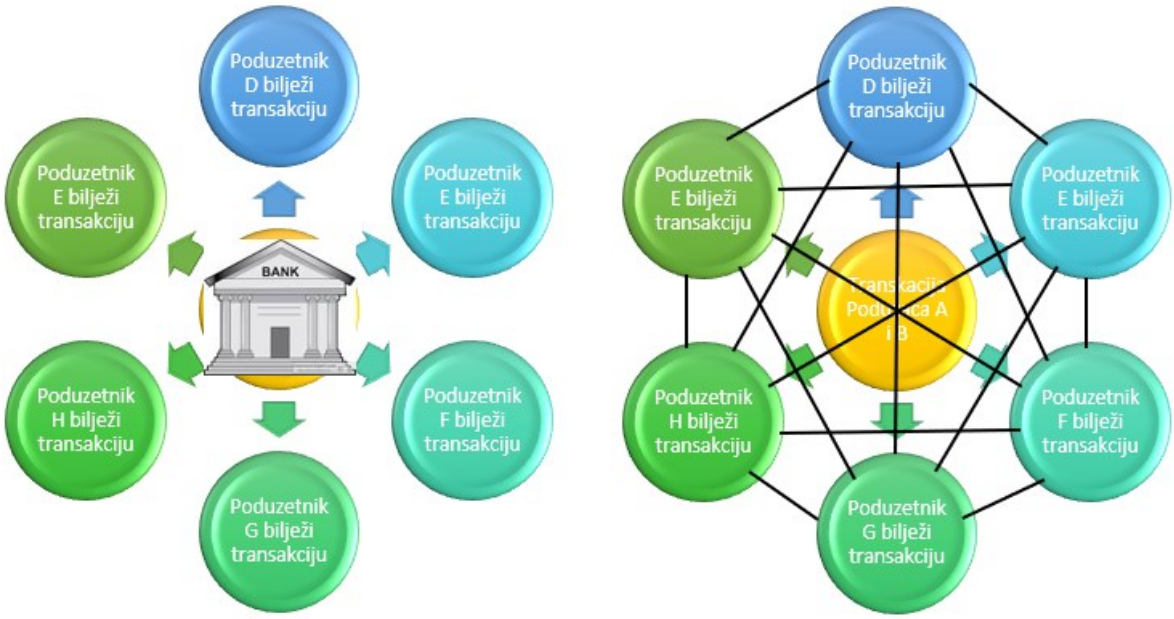
Što je veći broj sudionika u neposrednom izvršavanju transakcija to je manja mogućnost malverziranja transakcija.



Slika 4. *Prikaz bilježenja transakcije na svim računalima sudionika blockchaina (prikaz autora rada)*

U ovom primjeru transakciju između Poduzetnika A i Poduzetnika B provjerava i potvrđuje 4 poduzetnika (C, D, E, F). Time se smanjuje mogućnost malverziranja transakcijama jer bi se morao imati pristup računalima preostalih četiri poduzetnika i izvršiti malverzaciju što je nemoguće. Što je veći broj korisnika u sustavu, mogućnost malverziranja se smanjuje, a samim time se povećava sigurnost izvršenja transakcija.

Usporedimo li centralizirani bankovni sustav bilježenja transakcija i blockchain tehnologiju, možemo zaključiti da je blockchain istisnuo posrednika jer više nije potreban s obzirom da svi sudionici (čvorovi) ravnopravno sudjeluju u bilježenju transakcija.



Slika 5. *Usporedba centraliziranog i decentraliziranog načina bilježenja transakcija (prikaz autora rada)*

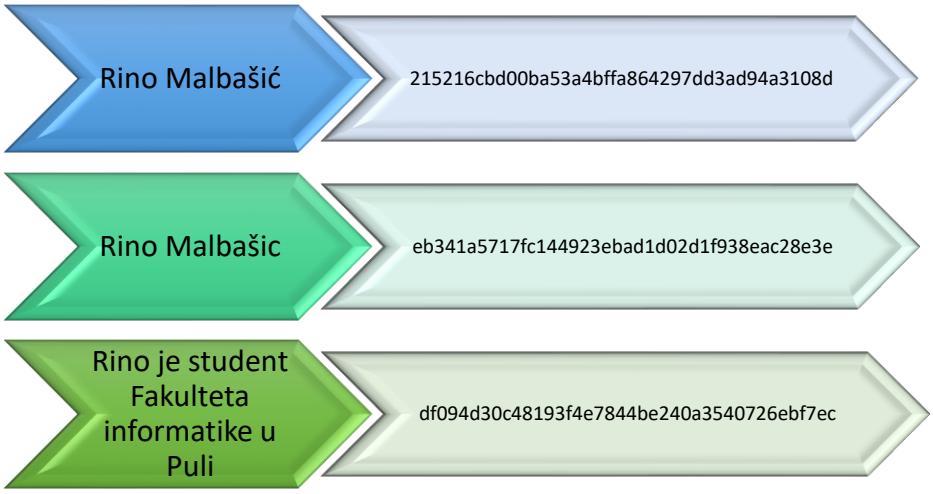
Lijeva slika prikazuje centralizirani način izvršenja transakcija. Banka bilježi transakcije poduzetnika i bez nje, transakcije se ne bi mogle izvršiti. Desna slika prikazuje decentralizirani način izvršenja u kojem je banka izostavljena i sudionici sami provjeravaju je li moguće izvršiti transakciju. Ukoliko utvrde da je moguće, potvrđuju je.

Jedna od ključnih razlika između tipične baze podataka i blockchaina je način na koji su podaci strukturirani. Baza podataka strukturira svoje podatke u tablice, poput Excel tablice dok blockchain ili blok lanac prikuplja informacije koje su postavljene u blokove odnosno grupe koje čine blockchain. Unutar blokova spremaju se skupovi informacija.

1.1. Blok

Blockchain se sastoji od skupa zaštićenih informacijskih blokova lančano povezanih jedan za drugi. Ujedno je to i decentralizirana digitalna knjiga transakcija koja je distribuirana među svim računalima koja ih koriste. Knjiga se sastoji od zapisa koje nazivamo blokovima i koriste se za bilježenje transakcija na mnogim računalima.

Osnovna sastavnica blockchaina je blok ili podatkovni paket koji se sastoji od podataka, oznake vremena, *hash* bloka i *hash* prethodnog bloka. "Hash" ili hash funkcija je funkcija koja se može koristiti za pretvaranje podataka proizvoljne veličine u vrijednosti fiksne veličine. Koristi se za indeksiranje i pronalaženje podataka u bazama podataka, a moguće ju je koristiti i za šifriranje. Iz sljedećeg primjera (Slika 6) vidljivo je da promjena bilo kojeg ulaznog znaka rezultira potpuno novim hashom. Isto tako, vidljivo je da ulazni podaci mogu biti različite veličine, ali hash je uvijek iste veličine.

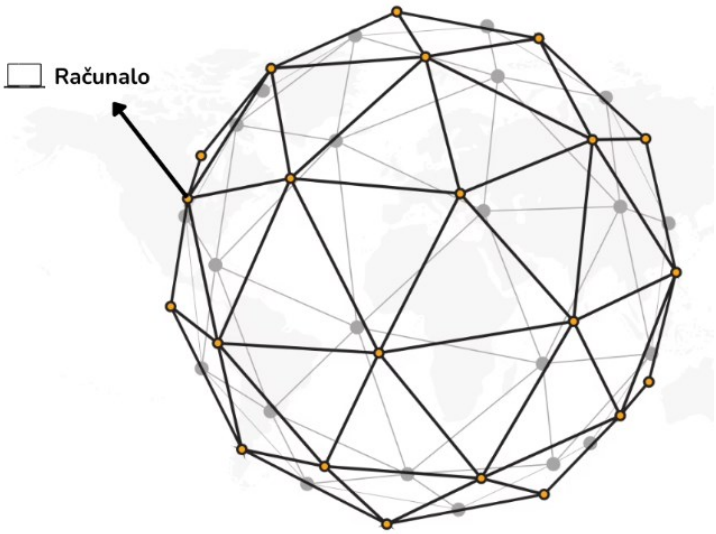


Slika 6. *primjer pretvaranja podataka pomoću algoritma SHA-256 (prikaz autora rada)*

Algoritam pretvara ulazne podatke različite duljine (vrijednosti) u izlazne šifre fiksne duljine. Prvi i drugi ulazni podatak razlikuju se u jednom slovu: Ć i C. Izlazni hashevi su iste duljine, ali s potpuno drugačijim redoslijedom slova i brojeva. U trećem primjeru ulazni podatak ima više znakova od prethodna dva, ali izlazni hash je iste duljine kao u prethodna dva primjera.

Blokovi u sebi sadrže transakcije koje su ostvarene u određenom vremenu i njihove informacije. Valjanost transakcije provjeravaju i potvrđuju svi sudionici odnosno računala koja pokreću blockchain. S obzirom da svako računalo može provjeriti povijest svih transakcija koje su zabilježene u blokovima, a time i u blockchainu, provjera valjanosti je vrlo jednostavna. Nakon što sva računala provjere i odobre transakciju, ona se pohranjuje u blok. Jednom zabilježena transakcija više se nikada ne može izmijeniti.

Računala koja su ravnopravno povezana u mrežu i koja mogu dijeliti resurse bez središnjeg poslužitelja nazivaju se *peer to peer* računala (Slika 7). Računala moraju imati istu programsku podršku kako bi izravno mogla pristupiti datotekama koje se nalaze na disku ostalih umreženih računala.



Slika 7. *Prikaz mreže računala*

Mreža računala pokreće blockchain. Za njihove sastavne elemente - računala koristi se izraz "čvor" (engl. node) (Izvor: https://www.bitcoin-store.hr/blog/sto-je-blockchain-i-kako-funkcionira/, pristupljeno 4.8.2023.)

Računala mogu biti vezom ad hoc, slučajnom vezom koja je kratkotrajna. Oblik povezivanja s osobinama *peer to peer* veze mogu biti i računala u jednom uredu koji su povezani fizičkom vezom (kablovima). Isto tako, može biti mreža mnogo većih razmjera u kojoj posebni protokoli i aplikacije uspostavljaju izravne odnose među korisnicima preko Interneta.

U takvom obliku povezivanja računala, korištenje blockchaina isključuje mogućnost beskonačnog umnožavanja digitalnog materijala. Time se potvrđuje da se svaka jedinica prenosi samo jednom transakciju.

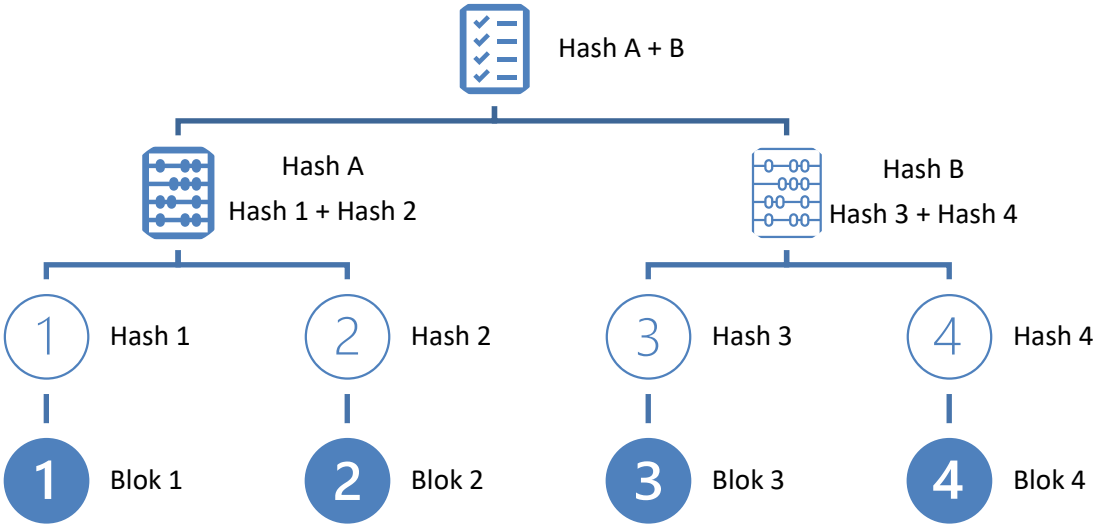
Transakcije koje su provjerene, prihvaćene tj. konvalidirane pohranjuju se u blokove čija je struktura prikaza u nastavku (Slika 8).

Slika 8. *Prikaz strukture bloka (prikaz autora rada)*

Svaki blok sastoji se od Hasha prijašnjeg bloka na kojeg se nadovezuje, od popisa izvršenih i potvrđenih transakcija, od oznake vremena i vlastitog hasha kojeg će preuzeti budući blok koji će se nadovezati na ovaj posljednji u blockchainu

Transakcije koje su sadržane u bloku raspršene su i kodirane u stablo nazvano „Merkle".

Merkleovo stablo je baza podataka temeljena na *hash* funkciji. Struktura nalikuje na stablo u kojem je svaki list (čvor) *hash* bloka. Svaki čvor koji nije list postaje *hash* podređenog čvora tj. njegovog djeteta. Merkleova stabla imaju faktor grananja 2, što znači da svaki čvor ima dvoje djece (Slika 9). Svaki blok sadrži kriptografski raspršene kodove prijašnjih blokova u blockchainu, povezujući ih poput grana stabla. Ti povezani blokovi tvore lanac. Ovaj ponavljajući proces, sve unazad do početnog bloka, potvrđuje cjelovitost prethodnog bloka, koji je poznat kao „blok podrijetla".



Slika 9. *Prikaz Merkleovog stabla (prikaz autora rada)*

Svaki list (čvor) stabla je hash bloka. Svaki čvor koji nije list postaje hash podređenog čvora tj. njegovog djeteta. Merkleova stabla imaju faktor grananja 2, što znači da svaki čvor ima dvoje djece.

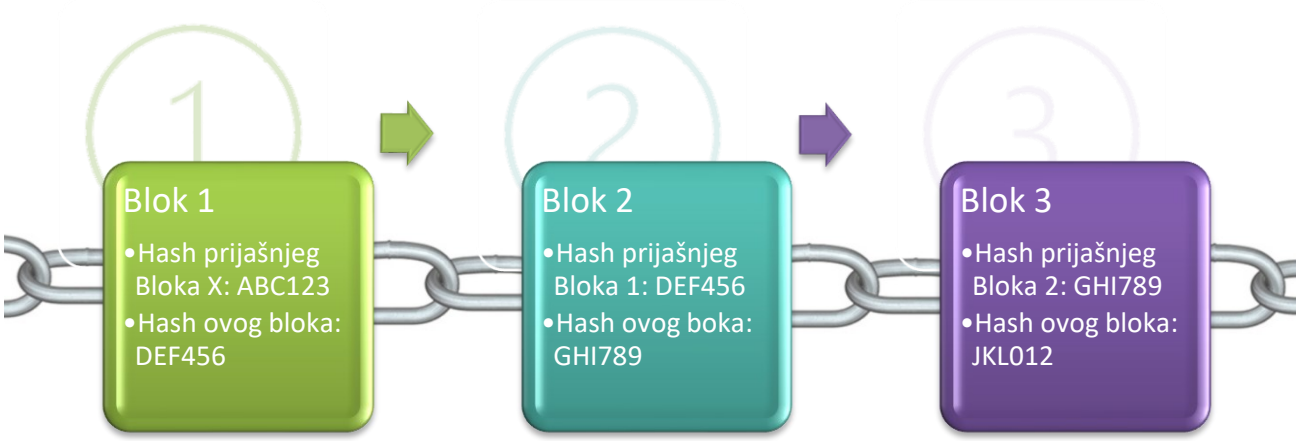
Kako bi se osigurala cjelovitost bloka i podataka koji su sadržani u njemu, blok je najčešće digitalno potpisan. Digitalni potpis je matematička shema za provjeru autentičnosti digitalnih poruka ili dokumenata. Valjani digitalni potpis, gdje su preduvjeti zadovoljeni, daje primatelju vrlo visoku sigurnost da je poruku kreirao poznati pošiljatelj (autentičnost) i da poruka nije mijenjana u prijenosu (integritet).

1.2. Struktura Blockchaina

Blokovi pohranjuju popis transakcija. S obzirom da imaju ograničenu mogućnost pohranjivanja, popunjavanje bloka popisom transakcija znači i njegovo zatvaranje.

Svaka daljnja transakcija popisuje se u novonastalom bloku koji se na postojeći veže putem hasha. Vezivanjem jednog bloka na drugi nastaje lanac blokova ili blockchain. Na taj način nastaje „digitalna knjiga“ u kojoj su informacije kronološki poredane i kriptografski zaštićene.

U nastavku je prikaz vezivanja blokova u lanac (Slika 10).



Slika 10. *Prikaz vezivanja blokova u lanac (prikaz autora rada)*

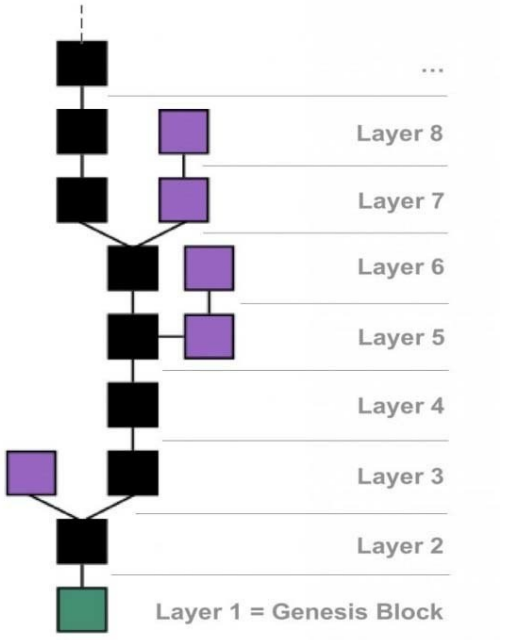
Blokovi se povezuju u lanac putem hash funkcije. Blok 2, nakon što je ispunjen njegov kapacitet pohrane transakcija, vezao se na blok 1 putem njegovog hasha, u ovom primjeru DEF456. Nakon što se vezao, Blok 2 stvara vlastiti hash, u ovom primjeru GHI789. Idući blok koji će se vezati na njega, moći će to učiniti pomoću hasha Bloka 2 na isti način na koji se Blok 2 vezao na Blok 1. Svaki idući novonastali i popunjeni blok nadovezat će se na blockchain na isti način.

Svaki blok u lancu vezuje se na prethodni blok pomoću hash funkcije odnosno kriptografskog algoritma koji preuzima jedinstveni podatkovni zapis prethodnog bloka (na slici zeleni Blok 1 i njegov Hash DEF456) i stvara novi izlazni niz znakova (na slici plavi Blok 2 i njegov hash GHI789. Taj izlazni hash ujedno je i ulazna vrijednost novog bloka koji će se nadovezati na lanac.

U nekim slučajevima može se dogoditi istodobna proizvodnja različitih blokova zbog kojih se može stvoriti privremeno grananje (eng. *fork*) samog lanca. Grananje predstavlja situaciju u kojoj se blockchain razdvaja u dva potencijalna smjera. Osim povijesti temeljenoj na hashu, svaki blockchain ima neki vlastiti određeni algoritam. Svaki algoritam služi za bodovanje različitih verzija povijesti blockchaina te se u konačnici odabire onaj algoritam s većim brojem

bodova u odnosu na ostale. Za one blokove koji nisu odabrani za uključivanje u blockchain, dodjeljuje im se naziv blokovi „siročad“.

Neki blokovi s istom vremenskom oznakom (vršnjaci) ponekad imaju različite verzije povijesti. Ti blokovi sadrže trenutnu najbolju verziju podataka. Kada u bilo kakvom trenutku vršnjak primi verziju s većim brojem bodova (najčešće staru verziju s nekim novim dodanim blokom), oni se proširuju ili prepisuju preko vlastite baze podataka i ponovno prenose poboljšanu verziju ostalim blokovima u lancu. Ne postoji slučaj ili trenutak u kojem je zagarantirano kako će zapis zauvijek ostati u najboljoj verziji u povijesti.



Slika 11. *Prikaz grananja blockchaina (Izvor: https://www.researchgate.net/figure/Formation-of-Blockchain-6_fig1_338651863 pristupljeno 4.8.2023., , pristupljeno 4.8.2023.)*

U nekim je slučajevima (primjer Razina 3, 5 i 6) moguće istovremeno spajanje dva različita bloka na jedan blockchain pri čemu nastaju dva paralelna lanca. Korisnici će odlučiti koji će od njih ostati, a kojeg će odbaciti.

Slika 11. prikazuje je kako blockchain izgleda kada su blokovi spojeni u lanac. Prvi sloj je prvi blok koji se naziva *Genesis Block.* Prvi blok se u drugom sloju grana na dva dijela od kojih će jedan postati stalni sljedbenik, a drugi će se »izgubiti«. Zbog konsenzusa zajednice koji određuje da se u trenutku nadogradnje bloka isti mora vezati na duži lanac i zbog male vjerojatnosti da će oba lanca opstajati kroz vrijeme u jednakoj dužini, duži će lanac opstati, a kraći će se izgubiti. To vrijedi za sve sljedeće blokove u lancu. Preostaju samo oni koji se nadovezuju sa sljedećim blokom.

Umjesto kreiranja prijepisa starih blokova, blockchaini nadovezuju nove blokove na stare i omogućuju proširenje lanca pomoću tih novih blokova. Zbog tog se razloga vjerojatnost zamjene unosa eksponencijalno smanjuje kako se na njima gradi i povezuje više blokova. Na primjer, Bitcoin koristi sustav „dokaza o radu“, gdje se lanac s najviše kumulativnih dokaza o radu smatra važećim po mreži.

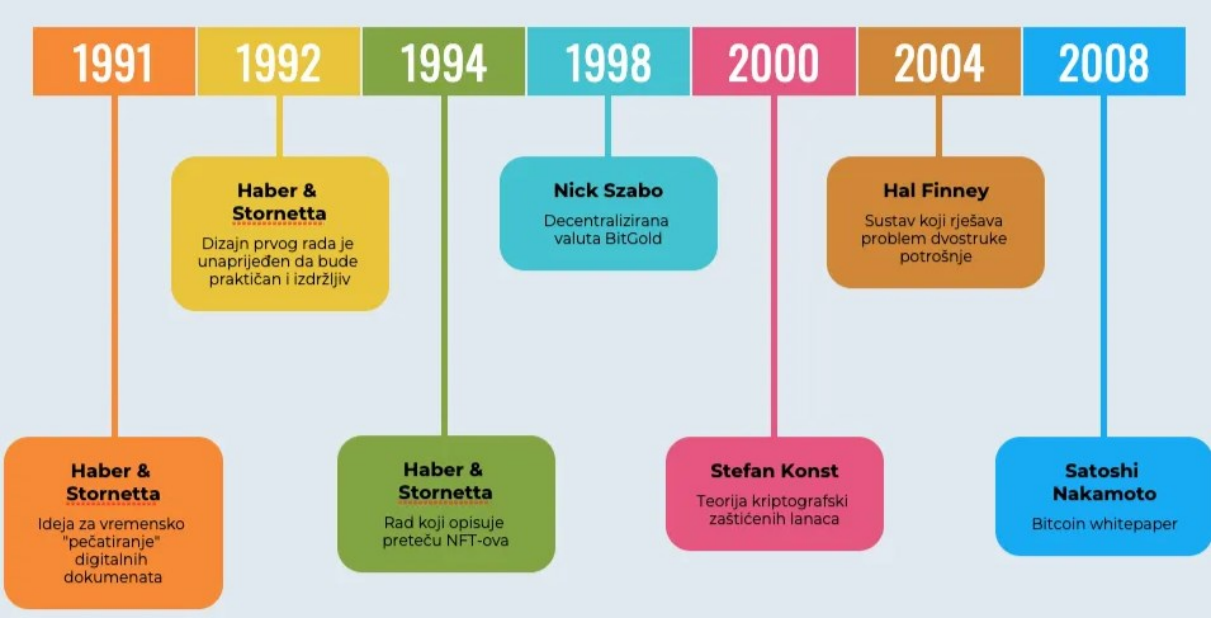
1.3. Povijesni razvoj blockchaina

Ranih 1990-tih grupa istraživača radila je na projektu razvoja distribuirane baze podataka koju bi dijelio veći broj sudionika bez potrebe za posrednikom. 1991. godine istraživači Stuart Haber i W. Scott Stornetta istraživali su mogućnost vremenskog „pečatiranja“ digitalnih dokumentata što bi osiguralo originalnost i točno datiranje istih. Dokumente su pohranjivali u lanac koji je bio sastavljen od blokova. Iduće godine nadogradili su sustav „pečaćenja“ Merkelovim stablom čime su povećali broj prikupljenih dokumenata po bloku. 1994. godine počinje prva komercijalizacija ideje (Slika 12).

1998. godine računalni znanstvenik Nick Szabo razvio je decentraliziranu valutu „Bit Gold“. Vrijednost se temeljila na cijeni računalnih resursa. Vrijednost „bitova“ se računala složenom matematičkom jednadžbom, ali sustav nije saživio.

2000. godine Stefan Konst predstavio je teoriju kriptografski zaštićenih lanaca prema kojoj su kutovi bilo kojeg grafa povezani s rubovima grafa kriptografskim metodama. Takve metode omogućavale su daljnje širenje kutova i rubova koji su se unosili u lanac. Osim toga, metoda je omogućili praćenje odnosa do samog nastanka čime se dokazivala autentičnost.

2008. godine predstavljen je već prethodno spomenuti rad Satoshia Nakamota, a naredne je godine izrudaren tj. Stvoren prvi blok Bitcoin blockchaina poznat kao „genesis blok“ .



Slika 12. *Povijest razvoja blockchain tehnologije od nastanka prvog „genesis“ bloka (Izvor: https://medium.com/@swarowski.eth/blockchain-tehnologija-povijest-933c77e1ecbf, pristupljeno 4.8.2023.)*

Nakon pojave Bitcoina, blockchain tehnologija imala je sve više pristaša te se ubrzano počela razvijati i nadograđivati.

Od 2010. do 2012. godine kriptovalute su se razvijale velikom brzinom. Započela su plaćanja i donacije u kriptovaluti, ali to je ujedno i razdoblje hakiranja istih te uvođenja novih sigurnijih rješenja (Sheldon, 2021).

Razdoblje između 2013. godine i 2015. godine može se opisati kao razdoblje velikih napredaka, ali ujedno i previranja i upitne legalnosti kriptovaluti. Dok su u nekim zemljama (Tajland i Kina) kriptovalute zabranjene, u drugima (Vancouver) je osposobljen bankomat za iste. Velika prekretnica tog razdoblja bila je objava Vitalika Buterina u kojoj predlaže decentraliziranu aplikacijsku platformu i stvaranje Zaklade Ethereum. 2014. godine uveo je pametne ugovore i mogućnost korištenja blockchain tehnologije i za druge vrijednosti osim kriptovaluti. 2015. godine pokrenuta je mreža Ethereum Frontier, a sama kriptovaluta postala je jedna od vodećih. Iste su se godine udružile velike investicijske banke kako bi proučile kripotvalute i blockchainove i implementirale ih u vlastito poslovanje.

2016. godine riječ blockchain postaje jedna riječ koja je u primjeni i danas. Ujedno je to godina velikih poznatih hakiranja sustava Ethereum iskorištavanjem greške u kodu i krađe mjenjačnice Bitfinexa tijekom koje je otuđeno 120.000 bitcoina (cca 66 milijuna dolara).

2017. godina označila je veliki zamah u korištenju kriptovaluti. Japan je priznao Bitcoin kao legalnu valutu dok je 15% svjetskih banaka implementiralo blockchain tehnologiju u nekim segmentima poslovanja.

2018. godina označena je padom vrijednosti kriptovaluti, odustajanjem od prihvaćanja plaćanja u istima pa sve do zabrane oglašavanja.

2019. su godine istraživanja blockchaina dokazala primjenjivost sustava te se tehnologija počela primjenjivati i na drugim područjima osim kriptovalti, a sve je više poznatih tvrtki počelo koristiti tu tehnologiju i plaćanja. 2020. godina samo potvrđuje sve veći ubrzaniji razvoj blockchain tehnologije i sve se veći broj sudionika uključuje u proizvodnju blockchaina.

Budućnost blockchain tehnologije je osigurana, ali poput svega ostalog, vrlo je teško predvidjeti kojim će se tempom i u kojem smjeru dalje razvijati.

1.4. Vrste blockchaina

Razvoj potreba sudionika i korisnika blockchaina uvjetovao je i ravoj nekoliko vrsta blockchaina: javni, privatni i korporacijski blockchain.

1.4.1. Javni blockchain

Javni blockchain dostupan je svima jer nema nikakvu kontrolu ili ograničenje pristupa što znači da bilo tko može sudjelovati slanjem transakcija ili provjeravati iste. Prednosti takvog sustava je potpuna decentralizacija i otvorenost. Podaci su javno dostupni svima premda se identitet sudionika skriva. Zbog otvorenosti, dosputan je velikom broju sudionika što onemogućuje monopol. Nedostatak je potreba za velikom količinom računalne snage koja potrebna za verificiranje transakcija. Bitcoin, Ethereum, i većina drugih kriptovaluti koriste otvorene (javne) blokove. Najveću tržišnu kapitalizaciju od travnja 2018. godine ima Bitcoin, koji je još uvijek na prvom mjestu.

1.4.2. Privatni blockchain

Osnivač/i mreže određuje/u tko ima pravo pristupiti mreži. Za razliku od javnih blockchaina, vlasnik privatnog blockchaina provjerava je li osoba koja želi pristupiti blockchainu vjerodostojna i prava. Nakon što se odobri pristup, novi član radi na održavanju blockchaina na decentralizirani način premda je sustav sam po sebi u potpunosti centraliziran. Centralizacija je vidljiva upravno na kontroli pristupa koja se mora odobriti. Pogodan je za velike organizacije unutar kojih su podaci pristupni svima, ali su prema »vanjskom svijetu« nedostupni. U svojem postojanju, ne oslanjaju se na anonimne vanjske čvorove koje mogu provjeravati valjanosti transakcije.

1.4.3. Korporacijski blockchain

Po svojem konceptu, korporacijski je blockchain kombinacija javnog i privatnog blockchaina. Nije u potpunosti otvorenog tipa niti je u potpunosti centraliziran na način da ga osnivač u potpunosti kontrolira. Korporacijskim blockchaina upravlja nekoliko organizacija koje imaju zajedničku potrebu brzo i kvalitetno izmjenjivati podatke i sustav je zatvoren prema vanjskim subjektima.

1.5. Obilježja blockchaina

Mnoge su osobine blockchaina koje ga čine sigurnim, provjerenim i valjanim načinom bilježenja transakcija. U nastavku su istaknute osobine koje ga čine jedinstvenim i primjenjivim (Anonymus, Bitcoin store 2022).

1.5.1 Decentraliziranost mreže

Decentraliziranost se očituje u činjenici da mrežom ne upravlja nikakvo centralno tijelo ili institucija poput banke, vlade ili neke tvrtke. Transakcije koje se bilježe u blokovima blockchaina nisu pohranjene na jednom mjestu već su raspršene između mnoštva računala i mjesta. Ukoliko se jedno računalo isključi iz sustava i prestane raditi, u sustavu će ostati još mnogo drugih računala koji će pokretati i održavati blockchain bez ikakvih poteškoća.

1.5.2. Transparentnost mreže

Zbog svoje decentraliziranosti i činjenice da blockchain postoji kao baza podataka koja se može dijeliti između korisnika, podaci su pohranjeni na više različitih mjesta istovremeno. Iz toga proizlazi i činjenica da svako računalo – čvor u blockchainu ima istovjetnu kopiju povijesti svih transakcija. Svaka nova transakcija istovremeno se bilježi na sva računala te stoga svi imaju pristup svim informacijama. Ništa nije skriveno ili nedostupno.

1.5.3. Sigurnost svih korisnika

Sigurnost se postiže temeljem prethodno navedenih osobina i načina funkcioniranja. Kako bi se transakcija potvrdila potrebno je da je potvrde sva računala-čvorovi koji sudjeluju u blockchainu temeljem zajedničkog konsenzusa. Osim toga, transakcije su šifrirane tako da je hakiranje istih gotovo nemoguće. S obzirom da sva računala provjeravaju povijest transakcija, svaki zlonamjerni pokušaj odmah će prepoznati sva računala u sustavi i isti će biti odmah odbijen.

1.5.4. Trenutno izvršavanje transakcija

Transakcije koje se izvršavaju putem blockchaina odrađuju se u svega nekoliko minuta u čitavom svijetu. Nije potrebno sastavljati i slati papirnate naloge niti čekati djelatnike na drugoj strani svijeta da odobre ili odbiju transakciju. Ona se gotovo trenutno izvršava i to na svim čvorovima koji pokreću blockchain. Naknade koje se pritom moraju platiti su minimalne.

1.5.5. Trenutni uvid u sve podatke

Blockchain bilježi svaki korak svake transakcije od samog početka i nastanka blockchaina pa do posljednje upravo učinjene transakcije. Poistovjetimo li to proizvodom, postavlja se pitanje postoji li proizvod kojeg korisnik u bilo kojem trenutku može preispitati i provjeriti svaku fazu nastajanja od samo početka proizvodnje sirovine i unazad pa sve do kupljenog proizvoda? Odgovor je definitivno ne, nije moguće. Blockhain to osigurava, odnosno to mu je temeljna odlika. Upravo ta osobina omogućuje primjenu blockchain tehnologije i na druga područja naših života za koja nikad ne bi doveli u vezu s tom tehnologijom i kriptovalutama koje su usko povezane uz blockchain.

1.6. Konsenzus

Konsenzus u kontekstu kriptovalute predstavlja mehanizam ili protokol kojim se sudionici u decentraliziranoj mreži slažu oko valjanosti transakcija ili promjena u blockchainu. Konsenzus je ključan za održavanje integriteta, sigurnosti i dosljednosti blockchaina. Osigurava da svi čvorovi u mreži postignu dogovor o stanju glavne knjige, unatoč nepostojanju središnjeg autoriteta.

U tradicionalnim centraliziranim sustavima, konsenzus se postiže kroz središnji autoritet od povjerenja koje provjerava i odobrava transakcije. Međutim, u decentraliziranim sustavima konsenzus se postiže putem distribuiranih mehanizama konsenzusa, gdje više čvorova ili sudionika, njih najmanje 51%, radi zajedno kako bi potvrdili i dogovorili stanje blockchaina. Ovaj decentralizirani konsenzus eliminira potrebu za središnjim autoritetom i povećava sigurnost i pouzdanost sustava.

1.6.1. Dokaz o radu (Proof of Work)

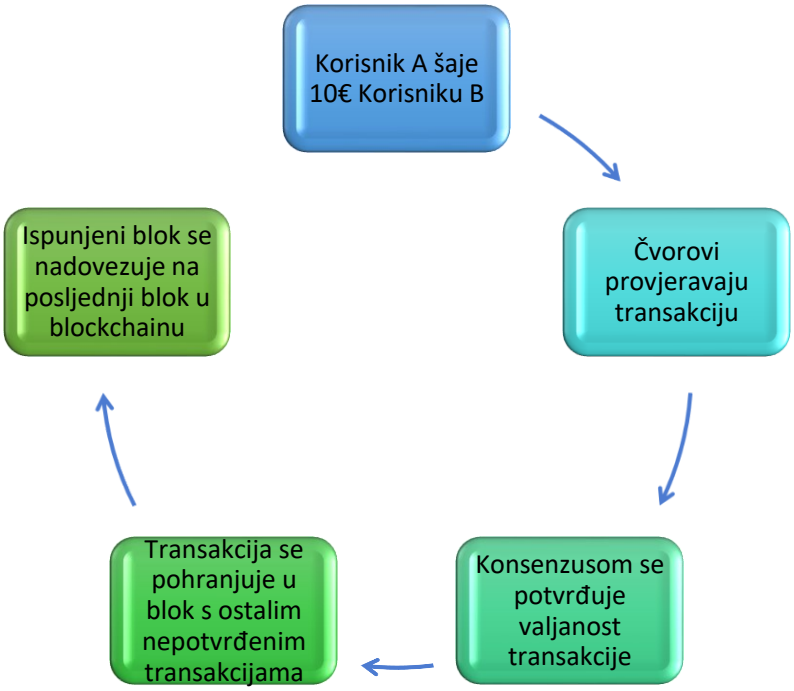
Najkorišteniji konsenzus za potvrdu transakcija i održavanje sigurnosti blockchaina je *dokaz o radu* (*Proof-of-Work* ili skraćeno POW). To je algoritam koji je razvijen 1993. godine kao mehanizam zaštite servera od spama i kibernetičkih napada koji su onesposobljavali računala povezana na napadnuti server. 2009. godine koncept je ponovno aktualiziran kako mehanizam konsenzusa za kriptovalutu Bitcoin. POW se koristi za potvrđivanje transakcije u Bitcoin mreži, za dodavanje novih blokova u lanac, za siguran rad i za sprječavanje problema duplanja tj. slanja npr. jednog Bitcoina više puta različitim korisnicima. Osim Bitcoina, POW koriste i druge kriptovalute poput Litecoina i Dogecoina.

Konsenzus POW može se objasniti u nekoliko koraka (Slika 13):

1. Korisnik A želi poslati 10€ Korisniku B – transakcija je pokrenuta.
2. Čvorovi u blockchain mreži provjeravaju transakciju i pomoću distribuirane knjige potvrđuju da je u pitanju nova transakcija. Provjera je moguća jer svaki čvor ima cjelovitu kopiju svih transakcija pa je provjera jednostavna. Ujedno se provjerava da Korisnik A ne želi zloupotrijebiti blockchain i isti iznos više puta poslati raznim korisnicima.
3. Mehanizam konsenzusa potvrđuje da je transakcija valjana i pohranjuje se u blockchain.
4. Provjerena transakcija se pohranjuje u blok s ostalim nepotvrđenim transakcijama.
5. Kada se kapacitet bloka ispuni, on se pohranjuje u blockchain odnosno nadovezuje se na posljednji blok u nizu.

Kako bi se mogao nadovezati, potrebno je otkriti složenu kriptografsku slagalicu ili šifru s kojom je novi blok zaštićen i koja se sastoji od niza slova i brojki. Korisnici mreže ulažu veliku snagu svojih računala kako bi riješili slagalicu odnosno otkrili šifru novog bloka i time ga nadovezali. Jednom otkrivena šifra novog bloka dijeli se s ostalim korisnicima koji je potvrđuju i time omogućuju računalu koji ju je otkrio pohranjivanje novog bloka u blockchnain. Otkrivanje tj. rješavanje zagonetke donosi nagradu i zbog toga se korisnici uključuju u pronalaženje šifri odnosno rudarenje.

Iz navedenog je vidljivo da svako računalo-čvor ulaže određeni rad kako bi se provjerila svaka nova transakcija pa je i mehanizam tako dobio naziv – dokaz o radu (Anonymus, Bitcoin store 2022).



Slika 13. *Prikaz rada mehanizma Proof-of-Work (POW) (prikaz autora rada)*

Transakciju koju započinje Korisnik A provjeravaju svi čvorovi u mreži i potvrđuju je ukoliko je valjana. Transakcija se pohranjuje u blok koji se nadovezuje na lanac kada se ispuni njegov kapacitet pohrane transakcija.

Prednosti ovog mehanizma su visoka razina sigurnosti zbog transparentnosti i pouzdanosti u način provođenja transakcija unutar mreže, decentraliziranost sustava i nagrade koje osvajaju korisnici – rudari ukoliko prvi odgonetnu šifru bloka i time priključe blok na lanac.

Nedostaci su visoki troškovi moderne računalne opreme koja je potrebna za rudarenje i visoki računi za struju. Mali korisnici se polako istiskuju jer ne mogu konkurirati velikim igračima koji imaju dovoljno sredstava za ulaganje u najsuvremeniju opremu, a time i veće mogućnosti za osvajanje nagrade.

Ukratko, POW je mehanizam konsenzusa koji zahtijeva od članova mreže da ulože puno vremena u rješavanju kriptografskih slagalica (matematičkih operacija) kako bi spriječili bilo koga da preuzme kontrolu nad sustavom. Koristi se za provjeravanje valjanosti transakcija, rudarenje kriptovaluta i rudarenje novih tokena. Zbog tog konsenzusa Bitcon i ostale kriptovalutne transakcije mogu se obraditi na siguran način bez uplitanja trećih strana. Dokaz o radu zahtijeva ogromnu količinu energije koja se povećava sa svakim dodatnim korisnikom.

1.6.2. Dokaz o ulogu (Proof-of-Stake)

Proof-of-Stake ili skraćeno POS predstavljen je 2011. godine u radu kojeg su bojavili Sunny King i Scott Nadal. "Za razliku od Proof of Work, Proof of Stake je mehanizam koji ne zahtijeva veliku količinu energije i ne uključuje rudarenje." (Frankenfield, n.d.)

Za razliku od POW mehanizma koji zahtjeva suvremenu računalnu opremu i visoke troškove što istiskuje iz utrke nekonkurentne korisnike koji si to ne mogu priuštiti, POS daje mogućnost i takvim igračima da sudjeluju ravnopravno u rudarenju zahvaljujući mehanizmu nasumičnog biranja korisnika koji će otkriti šifru bloka i time dobiti nagradu. Međutim, za razliku od POW mehanizma gdje korisnici ulažu snagu računala, u POS mehanizmu korisnici ulažu vlastiti određeni iznos kriptovaluti kao svojevrstan polog i garanciju da će, budu li odabrani, izrudariti novi blok. Svaki korisnik koji želi sudjelovati u POS mehanizmu i potvrđivati transakcije i za to dobivati nagradu, mora uložiti i zaključati na određeno vrijeme vlastiti broj kriptovaluti. Opisani proces poznat je pod nazivom stacking.

Ovakav pristup daje sigurnost da će odabrani korisnik potvrditi transakciju jer će u suprotnom izgubiti uloženi iznos i zauvijek gubi mogućnost potvrđivanja transakcija odnosno status validatora.

Nekoliko čimbenika utječe na odabir validatora za potvrdu transakcija. Dužina zaključanih kriptovaluti u obliku pologa i sam iznos istih jedan je od čimbenika koje algoritam koristi za odabir, ali kako bi svi dobili istu priliku, veliku ulogu ima i nasumični izbor.

Pozitivna strana ovog konsenzusa je definitivno nasumični odabir koji eliminira mogućnost da korisnici s većim mogućnostima imaju i veću vjerojatnost da će zaključati blok, dok je negativna strana potencijalna opasnost da će se zbog većih zamrznutih uloga i bez obzira na dozu sreće, vjerojatno uvijek birati uži krug korisnika (Anonymus, Bitcoin store, 2023).

Usporedimo li mehanizme čiji je zajednički cilj održavanje mreže, možemo utvrditi da svaki od njih ima prednosti i mane (Slika 14).

Proof-of-Work (POW)	Proof-of-Stake (POS)
Transakcije potvrđuju **rudari**	Transakcije potvrđuju **validatori**
Za sudjelovanje je potrebno kupiti (skupu) računalnu opremu kako bi postali rudari	Za sudjelovanje je potrebno uložiti kriptovalute u "staking pool" kako bi postali validatori
Troši mnogo električne energije	Energetski je efikasan
Velika razina sigurnosti	Siguran, ali ima mane
Rudari za potvrđene transakcije dobiju fiksno utvrđenu blok nagradu	Validatori za potvrđene transakcije dobiju dio transakcijske naknade u obliku nagrade

Slika 14. *Usporedba Proof-of-Work i Proof-of-Stake mehanizma*
(Izvor: https://www.bitcoin-store.hr/blog/sto-je-proof-of-stake/, pristupljeno 7.8.2023.)

U prikazu se uspoređuju Proof-of-Work i Proof-of-Stake kako bi se utvrdile međusobne razlike.

1.7. Mogućnosti primjene blockchain tehnologije

Osobina blockchaina da bilježi sve korake transakcija i informacija od samog začetka do sadašnjeg trenutka otvorila je vrata primjeni tehnologije i na druga područja znanosti i gospodarstva.

U zdravstvu se blockchain tehnologija može primjenjivati kako bi se bilježili rezultati raznih istraživanja i time bili dostupni svima, ali može se čuvati medicinska dokumentacija pacijenata koja bi bila dostupna svim liječnicima s kojima pacijenti dolaze u kontakt u bilo koje vrijeme.

Tržište nekretnina, veliki informatički sustavi koji bilježe vlasničke i posjedovne listove savršeni su primjeri uspješne primjene blockchain tehnologije.

Posebno je intrigantna ideja primjene tehnologije na demokratske izbore kako bi se izbjegle malverzacije prilikom glasovanja, a i sami glasovi bi se puno brže i jednostavnije prebrojali.

1.8. Kripto novčanik

Kriptovalute mogu se steći na više načina. Najjednostavnija i učestala metoda stjecanja kriptovaluta je kupovanje istih na specijaliziranim mrežnim stranicama ili na burzama kriptovaluti, neposredno od trgovaca ili na specijaliziranim bankomatima. U svim navedenim

slučajevima kupci mijenjaju „pravi“ fizički ili knjižni novac koje je ujedno i zakonito sredstvo plaćanja za kriptovalute.

Drugi način stjecanja kriptovaluti je njihovo rudarenje. Pojam označava primjenu računala u procesu potvrde transakcija određenog blockchaina. Isto tako, rudarenjem se mogu dodavati novi blokovi na blockchain čime rudari ostvaruju pravo na naknadu.

Korisnici blockchaina koji posjeduju određeni iznos kriptovaluti, čuvaju ih u takozvanim kripto novčanicima. Kripto novčanik je softver koji omogućava pohranu kriptovaluta. Naziva se novčanikom jer je osnovna svrha softvera jednaka i svrsi novčanika – čuvanje digitalnog, a u drugom slučaju običnog papirnatog novca.

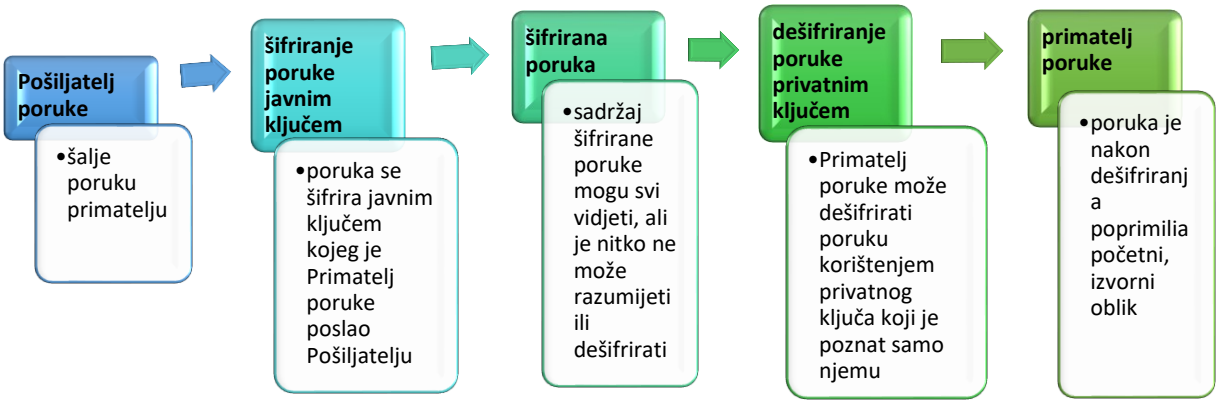
Kripto novčanici se temelje na blockchain tehnologiji odnosno, veza su između vlasnika kriptovaluti i samih kriptovaluta koje su pohranjene i postoje u lancu blokova blockchaina. Blockchain se definira kao javna knjiga u kojoj su zapisane sve transakcije, a samim time i sva salda kriptovaluti svih korisnika lanca. Novčanik je softver koji osigurava vlasniku pristup svojim kriptovalutama u lancu.

Kripto novčanik se sastoji od adrese, privatnog i javnog ključa koji se generiraju prilikom instalacije i inicijalnog otvaranja novčanika. Adresa novčanika omogućuje slanje, primanje i pohranu kriptovaluti.

Javni ključ je brojčana vrijednost koja služi za šifriranje podataka i provjeru autentičnosti adrese primatelja podataka. Koristi se za primanje kriptovaluti. Javni ključ se matematički izračunava iz privatnog ključa

Privatni ključ je šifrirani numerički broj koji „otključava“ kripto novčanik odnosno dokazuje vlasništvo nad kriptovalutama koje su pohranjene u kripto novčaniku. Poznat je samo vlasniku i služi za odobravanje transakcije odnosno autoriziranje prijenosa kriptovaluta drugom korisniku.

Postupak prijenosa kriptovaluti iz kripto novčanika pošiljatelja u kripto novčanik primatelja moguće je ostvariti korištenjem privatnog i javnog ključa (Slika 15).



Slika 15. *Prikaz komunikacije putem javnog ključa (prikaz autora rada)*

Poruka koja je poslana šifrira se javnim ključem na način da bude svima vidljiva, ali nerazumljiva. Primjenom privatnog ključa koji je povezan s javnim ključem, poruku je moguće pretvoriti u čitljiv oblik. To može napraviti samo vlasnik privatnog ključa.

Primatelj poruke šalje na adresu Pošiljatelja poruke javni ključ. Pošiljatelj šalje poruku Primatelju na način da je kriptira korištenjem javnog ključa kojeg mu je poslao primatelj. Tako kriptirana poruka može biti vidljiva svima, ali je jedino vlasnik privatnog ključa koji je povezan s dostavljenim javnim ključem može dešifrirati. Poruka stiže u kriptiranom obliku Primatelju poruke koji je dešifrira.

Prijenos poruke može se poistovjetiti s prijenosom kriptovaluti. Jednom kad je kriptovaluta prenesena od pošiljatelja prema primatelju, zapis transakcije se šalje u blockchain kako bi ga potvrdili drugi korisnici postupkom rudarenja. Postupak podrazumijeva provjeru svih postojećih prethodnih transakcija u blockchainu koji će rezultirati u konačnici potvrdom stanja u kripto novčaniku pošiljatelja i potvrditi će da ima dovoljan „saldo na računu“ koji mu omogućava prijenos odabranog iznosa na pošiljatelja. Osim toga, zahvaljujući kriptografiji, korisnici će potvrditi da nitko nije izmijenio početni sadržaj poruke.

Bitno je naglasiti da je u postupku transakcije najvažniji privatni ključ. Ukoliko vlasnik izgubi privatni ključ, izgubio je nepovratno i sadržaj svojeg kripto novčanika.

Kripto novčanici mogu biti raznovrsni, ali prema metodama pohrane razlikujemo:

1. **Vrući novčanik** (eng. Hot wallet) – novčanik koji je uvijek povezan na mrežu. Pogodan je za češće korištenje odnosno češće trgovanje kriptovalutama. Potrebno je preuzeti aplikaciju na računalo ili pametni telefon ili pristupiti mu putem Interneta. Premda se stupanj sigurnosti korištenja takve vrste novčanika povećava iz dana u dan, ipak postoji

određeni rizik hakiranja, a samim time i gubitka novčanika. Podsjetimo se da vlasnik privatnog ključa odnosno osoba koja ima privatni ključ, ima i vlasništvo nad novčanikom. S obzirom na veliku brzinu odrađivanja transakcija, hakiranje privatnog ključa i „provaljivanje“ u kripto novčanik je brže od samog otkrivanja od strane pravog vlasnika.

2. **Hladni novčanik** (eng. Cold wallet) – nije spojen na Internet i sigurniji je način čuvanja vrijednosti kriptovaluta. Izgledom je sličan USB prijenosnoj memoriji (Slika 16). Koristi se za dugotrajnu pohranu vrijednosti kriptovaluta i s obzirom da nije na mreži, hakerima je pristup onemogućen jer su privatni ključevi izolirani od samih računala ili pametnih telefona. Kako bi se novčanik otključao, potrebno je hladni novčanik priključiti na računalo ili pametni telefon i otključati ga lozinkom. Ostatak postupka je jednak prethodno opisanom.

Slika 16. *Ledger Nano S "hladni" kripto novčanik*

(Izvor: https://crobitcoin.com/ledger-nano-s-recenzija-video/, pristupljeno 7.8.2023.) Kripto novčanici koji imaju fizički oblik slični su usb prijenosnim memorijama. Oni su novčanik u kojima se pohranjuju kriptovalute.

2. Litecoin

Litecoin ili skraćeno LTC je kriptovaluta koja se temelji na Bitcoin protokolu i osmišljena je kao sredstvo za provođenje brzih i sigurnih transakcija s niskim troškovima naknade (Anonymus, Bitcoin store, n.d.).

Tvorac Litecoina je Charlie Lee, uspješan poduzetnik na području kriptovaluta. Litecoin je predstavljen 2011. godine dok je Charlie Lee bio zaposlen u Googleu kao softverski inženjer. 2013. godine napustio je Google i zaposlio se u *Coinbaseu*, tvrtki koja je pokrenula prvu digitalnu mjenjačnicu. 2017. napustio je Coinbase i pridružio se Litecoin Fondaciji. Usredotočio se na promicanje Litcoina i prihvaćanje kriptovaluti od sve većeg broja korisnika.

Slika 17. *Charlie Lee, tvorac Litecoina*
(Izvor: https://markets.businessinsider.com/news/currencies/litecoin-walmart-creator-charlie-lee-accidental-retweet-really-screwed-up-2021-9, pristupljeno 7.8.2023.)

Tvorac Litecoina je vlastitu kriptovalutu opisivao kao nadopunu Bitcoinu, a ne kao konkurenciju. Zajedno sa suradnicima, nastojali su ukloniti nedostatke koje su uočili prilikom rudarenja Bitcoina, među kojima se isticao mali broj transakcija po sekundi što će poskupiti cijenu transakcija i moguću centralizaciju rudarenja na način da su se stvarale takozvane farme visokospecijaliziranih performansi računala koje su istiskivale iz konkurencije računala skromnijih mogućnosti ostalih korisnika. Neki su se nedostaci Bitcoina preslikali i na Litecoin poput centralizacije proizvodnje. Često se za Bitcoin kaže da je to zlato (pohrana vrijednosti) dok je Litecoin (Slika 18) njegovo srebro (svakidašnje korištenje) (Anonymus, Kriptomat, n.d.).

Slika 18. *Logo Litecoina*

(Izvor: https://www.creativefabrica.com/pt/product/cryptocurrency-litecoin-logo/, pristupljeno 7.8.2023.)

Litecoin, poput Bitcoina, koristi konsenzus POW i blockchain je otvorenog tipa. To osigurava svim korisnicima stvaranje Litecoina ukoliko koriste svoju snagu računala za provjeru i ovjeravanje transakcija, a time i samih blokova. Ipak, temeljna razlika između te dvije kriptovalute je algoritam kojeg koriste za hashiranje blokova. Dok Bitcoin koristi Secure Hash Algoritam (SHA), Litecoin koristi algoritam Scrypt.

Scrypt je stvoren u Leeovom nastojanju da vlasnicima raznih trgovina omogući naplatu prodanih usluga i proizvoda u kriptovalutama. Tada je to bilo nemoguće zbog spore obrade transakcija i vrlo visokih naknada. Algoritam omogućava korisnicima istovremeno rudarenje Litecoina i drugih kriptovaluti koje koriste Scrypt. Osim toga, rudarenje je puno brže, a time i jeftinije od rudarenja Bitcoina. U međuvremenu, developeri Bitcoina su pronašli brži i jeftiniji način rudarenja primjenom Lightning Networka protokola plaćanja.

Pojavom spomenutog protokola, Litecoin je naišao na nove probleme. Transakcije su na Bitcoin mnogo brže i jeftinije. Dodatna panika među ulagačima i korisnicima Litecoina nastala je kada je izumitelj Litecoina, Charles Lee, prodao većinu svojeg udjela u kriptovaluti. Druge se kriptovalute razvijaju ubrzanim korakom i nude druge mogućnosti tako da tvorcima Litecoina ne preostaje ništa drugo nego obogaćivati ponudu i mogućnosti Litecoina. Tehnologija se stalno razvija i svaki zastoj na starome daje prednost ostalim sudionicima na tržištu kriptovaluti da preuzmu vodeće uloge.

Litecoin ima definiranu ukupnu količinu novčića i iznosi 84.000.000. dok je Bitcoinova granica postavljena na 21.000.000. U prosjeku se svaki novi blok Litecoina dodaje za 2.5 minuta dok se Bitcoin nadograđuje svakih cca 10 minuta. Omjer 1:4 u vremenu dodavanja blokova preslikava se i na omjer maksimalne količine novčića.

Nagrada za prvi blok bila je 50 Litecoina. Nakon svakih 840 000 izrudarenih blokova za što je potrebno cca 4 godine, nagrada se prepolovljuje. Predviđeno je da će se posljednji Litecoin izrudariti 20142. godine kada će nagrada za rudarenje doći na nulu. Trenutna nagrada iznosi 6,25 Litecoina po bloku (Anonymus, Litecoin foundation, n.d.).

Osobine Litecoina preslikavaju osobine blockchaina koje su opisane na samom početku ovog rada:

1. Decentraliziranost – ne postoji središnji entitet koji upravlja sustavom već sustav funkcionira na mreži međusobno povezanih računala putem Etherneta.
2. Transparentnost – svaki čvor u mreži ima kopiju svih prethodnih transakcija.
3. Sigurnost – svaki čvor može u bilo kojem trenutku provjeriti povijest transakcija tako da je nemoguće izmijeniti bilo koju prošlu već potvrđenu transakciju jer bi se to moralo odraditi na svim računalima u mreži.
4. Otvorenost protokola – kod je dostupan i besplatan na Iternetu. Moguće ga je preuzeti i modificirati te je svako novo programsko rješenje koje će ukloniti eventualne nedostatke Litecoina dobrodošlo.

3. Ethereum

„Ethereum je otvorena blockchain platforma (decentralizirani lanac zapisa) koja omogućava bilo kome da na njoj izgradi i koristi decentralizirane aplikacije (tzv. pametne ugovore) koje izvršava blockchain tehnologija. Ethereum se često naziva i svjetskim računalom, jer se računalne operacije izvršavaju simultano na velikom broju čvorova koji su decentralizirani, što znači da su aplikacije koje su ugrađene u blockchain praktički nezaustavljive. Na tom svjetskom računalu ne postoji neki "admin" koji ima ovlasti kojima bi mogao zaustavljati, editirati ili cenzurirati aplikacije, kao što je to moguće na običnim računalima i serverima." (Kolić, 2017)

3.1. Nastanak Ethereuma

Tvorac Ethereuma je Vitalik Buterin (Slika 19), mladi perspektivni matematičar i informatičar koji je od malih nogu pokazivao strast za programiranje i općenito za svijet informatike. Rođen je 1994. godine u Kolomni, u Ruskoj Federaciji, ali je u dobi od sedam godina preselio u Kanadu s roditeljima koji su tamo potražili bolje uvjete života. Od prvog dana školovanja pokazao je nadprosječne mogućnosti na području matematike i informatike. Sa sedamnaest godina zainteresirao se za Bitcoin i blockchain i s vremenom to je postala njegova opsesija. Počeo je s pisanjem blogova o blockchainu i kriptovalutama. 2011. godine postaje suosnivač i glavni urednik časopisa *Bitcoin Magazine*. Na toj funkciji ostaje do 2014. godine.

Slika 19. *Vitalik Butern (izvor: https://ecd.rs/blog/vitalik-buterin-mladi-genije-savremenog-doba/, pristupljeno 7.8.2023.)*

Kao predstavnik časopisa, sudjelovao je na kripto konferenciji u San Hoseu. Susret s velikim brojem istomišljenika potaklo ga je da širom svijeta istražuje sve mogućnosti koje blockchain

može pružati. Posjet Izraelskim tvrtkama *CovertCoins* i *MasterCoin* dao mu je uvid u novo značenje transakcija zabilježenih u blockchnainu gdje se svaka od njih tretirala „…jedan potpuni i valjani financijski ugovor, zauvijek zabilježen, uvijek dostupan i nesporan, a takva ideja potaknula je Vitalikovu maštu da ode korak dalje u načinu i svrsi korištenja blockchain tehnologije u odnosu na postojeći Bitcoin“ (Mirković, 2020).

2013. godine Vitalik je predstavio *Ethereum Whitepaper* kao revolucionarno djelo u kojem je opisao novi koncept i pozvao sve zainteresirane da se pridruže u kreiranju nove kriptovalute Ethereum (Slika 20).

2014. godine Ethereum projekt je službeno predstavljen javnosti na konferenciju u Miamiu. Nekoliko mjeseci nakon toga Vitalik i njegovi suradnici (Gavin Wood, Mihai Alisie, Anthony Di Lorio, Charles Hoskinson, Joseph Lubin i Jeffrey Wilcke) objavili su pre-prodaju ETH – Ethereum tokena i time priskrbili gotovo 18 milijuna dolara s kojima su osnovali *Ethereum Foundation* i financirali daljnji razvoj kriptovalute. 30. srpnja 2015. godine generiran je prvi blok transakcija čime je službeno započeo blockchain.

Ether – ETH je „gorivo“ koje okreće mrežu. Kako bi se izvršila transakcija ili prijenos informacija potreban je rad rudara koji će provjeriti i potvrditi transakciju i koji su plaćeni Etherom. Isto tako, programeri plaćaju korištenje mreže u Etherima jer im ona omogućava stvaranje decentraliziranih aplikacija i pametnih ugovor. Kako bi se provela transakcija ili pametni ugovor, potrebno je platiti naknadu koja se naziva ETH gas. Naknada se plaća za utrošenu energiju koja je potrebna za izvršenje, označava se sa Gwei i iznosi 10^{-9} ETH (Anonymus, Kriptoportal, 2021). Programski jezik Solidity kojeg je konceptualizirao i razvio Gavin Wood osnovni je razvojni jezik Ethereuma koji omogućava daljnji razvoj pametnih ugovora i decentraliziranih aplikacija.

Slika 20. *Ethereum logo (Izvor: https://ethereum.org/en/assets/, pristupljeno 7.8.2023.)*

3.2. Pametni ugovori

Zahvaljujući istraživačkom i vizionarskom radu Vitalika Buterina, Ethereum je dodao novu vrijednost blockcnain tehnologiji. Mreža ne osigurava samo prijenos transakcija i informacija već pomoću pametnih ugovora i decentraliziranih aplikacija omogućuje mnogostruke koristi i primjene. „*Smart contract* ili pametni ugovor je kompjuterski program ili transakcijski protokol koji je programiran da automatski izvršava zadaću ukoliko dođe do zadovoljavanja određenih uvjeta koje autor programa postavlja“ (Anonymus, Kriptoportal, 2021).

Koncept pametnih ugovora može se objasniti na primjeru starih automata za prodaju slatkiša ili za slušanje glazbe. Ukoliko se želi kupiti slatkiš ili poslušati pjesma bilo je potrebno ubaciti određeni iznos u automat i odabrati slatkiš ili pjesmu. Automat je „provjerio“ je li ubačen točan iznos i odabran proizvod. Ukoliko su oba uvjeta bila zadovoljena, proizvod je isporučen.

Nick Sabo je 90-tih godina prvi put upotrijebio termin pametni ugovor djelu *Smart Contracts: Building Blocks for Digital Markets* i definirao ga kao niz zapisanih pravila i protokola kojih se obje strane moraju pridržavati.

Pametni ugovor je program koji se nalazi na blockchainu, nepromjenjiv je, svima dostupan i jasan i ispunjava se kada su svi njegovi uvjeti ispunjeni. Prednost pametnih ugovora što nema nikakvih nejasnoća u njihovom ispunjavanju i naknadnih reklamacija. Uvjeti su svima jasni kao i rezultat koje će proizaći iz njihovog ispunjavanja. Takav koncept osigurava povjerenje u sustav i normalno trgovanje i između stranaka koje se ne poznaju. Koriste se za prijenos novca, kriptovaluti, nekretnina i drugih vrsta imovine (Nešić, 2021).

3.3. Decentralizirane aplikacije (DAaps)

Decentralizirane aplikacije su digitalni programi koji rade na Peer-to-peer mreži odnosno na blockchainu. Za razliku od ostalih aplikacija koje svakodnevno koristimo i iza kojih stoje tvorci koji njima upravljaju i nadograđuju, DAaps su decentralizirane aplikacije iza kojih stoje korisnici mreže koji mogu pružati ili koristiti njihove usluge. Takve aplikacije ne ovise o jednoj organizaciji ili pojedincu već su podržane od korisnika blockchaina.

3.4. NFT

Blockchain Ethereum omogućio je razvoj NFT-ova. NFT je engleska kratica za izraz *non-fungible token* ili na hrvatskom jeziku nezamjenjiv token ili žeton. Engleski izraz fungible označava materijalno ili nematerijalnu imovinu ili predmet koja ima određenu novčanu vrijednost, ali se ne može zamijeniti za drugu imovinu iste vrijednosti. Možemo zamijeniti novčanicu od 100 € za dvije od 50 €, ali ne možemo zamijeniti jedinstvenu rukotvorinu za drugu jer su različite premda mogu imati istu financijsku vrijednost (Anonymus, Bitcoin store, 2021).

NFT je kriptografski zaštićen djelić blockchaina koji ima jedinstvenu vrijednost. Za razliku od ostalih tokena ili žetona koji imaju određenu vrijednost poput fizičkih novčanica od 100 € u kojem je slučaju sasvim svejedno koju novčanicu imamo u novčaniku, NFT je digitalna vrijednost koja je jedinstvena i neponovljiva poput poznate umjetničke slike.

Kriptografska zaštita daje sigurnost vlasniku da se njegova vrijednost ne može manipulirati, falsificirati ili ukrasti zbog jednostavne činjenice da je upisana u bloku koji je dio blockchaina i po samoj njegovoj prirodi, u potpunosti nepromijenjena i nedodirljiva.

Primjena NFT moguća je na različitim područjima ljudskog djelovanja, ali široku primjenu ima u dokazivanju vlasništva nad umjetničkim djelima. Na dražbama se pojavljuju potpuno digitalna umjetnička djela koja se mogu pohraniti u obliku NFT-a. Primjer: umjetnik može napraviti digitalnu fotografiju i prodati je u obliku NFT-a.

Novi vlasnik može dijeliti sliku umjetnika putem mrežnih platformi ili tiskati je putem pisača, ali sve su to samo kopije originalnog dijela koji je pohranjen u blockchainu putem NFT-a na ime novog vlasnika i on je jedini i isključiti vlasnik umjetničkog djela. Svi ostali, koji posjeduju fotografiju, u biti posjeduju kopiju i ne mogu dokazati vlasništvo nad originalom.

Postavlja se pitanje čemu služe takvi pametni ugovori. Kupnja NFT-a daje pravo vlasništva nad digitalnom ili materijalnom imovinom i za to postoji zainteresirana zajednica koja je voljna izdvojiti određeni iznos. Osim toga, stvaranje jedinstvenog proizvoda putem NFT-a je vrlo jednostavno jer postoje platforme na Internetu koje to omogućavaju. Naknada za izradu NFT-a se plaća u Etherima. Najpraktičnija primjena ovakvog načina trgovanja umjetničkim i autorskim djelima je i činjenica da će sustav zaštitit autorsko pravo i prilikom svake daljnje preprodaje „zarobljene“ umjetnine u NFT-u autoru dodijeliti proviziju (Vrbanus, 2021).

4. Usporedba Litecoina i Ethereuma

Obje kriptovalute nastale su na temeljima Bitcoina ili točnije, nastale su kako bi uklonile nedostatke koji su se pojavili prilikom rudarenja Bitcoina. Premda su nastale iz iste težnje za poboljšanjem starije kriptovalute, bitno se razlikuju.

4.1. Nastanak i koncept

Litecoin je nastao 2011. godine na osnovama Bitcoina kao nastojanje da se transakcije izvršavaju brže i za manje naknade. Ethereum je nastao 2014. godine kako bi uklonio već spomenute nedostatke Bitcoina, ali je koncept obogaćen pametnim ugovorima kao automatskim izvršiteljima transakcija ukoliko se ispune uvjeti koji su postavljeni pametnim ugovorima.

Isto tako, Ethereum podržava i druge kriptovalute koje koriste njegovu mrežu, ali trguju odvojeno dok Litecoin nema tu mogućnost. Osim transakcija kriptovaluta i pametnih ugovora, Ethereum podržava i NFT-ove kao „dokaze“ jedinstvenih vrijednosti što definitivno Litecoin nema.

Usporedimo li koncepte tih dviju kriptovaluta, možemo utvrditi da je Litecoin valuta koja se koristi za izvršenje transakcija dok je Ethereum platforma koja, osim mogućnosti koje pruža Litecoin, može korisnicima osigurati dodatne mogućnosti. Programeri mogu na platformi razvijati pametne ugovore i decentralizirane aplikacije. Samim time, Ethereum platforma je primjenjivija i bogatija uslugama koje korisnici mogu koristiti.

4.2. Algoritam Scrypt i programski jezik Solidity

Litecoin se temelji na Peer-to-peer mehanizmu koji omogućava prijenos valuti bez središnjeg autoriteta ili institucije. U potpunosti je decentraliziran i transparentan. Nastao je na temeljima Bitcoina i koristi algoritam Scrypt dok je Ethereum nastao na vlastitoj Ethereum platformi i razvio je vlastiti programski jezik Solidity. Poput Litecoina, decentraliziran je i transparentan.

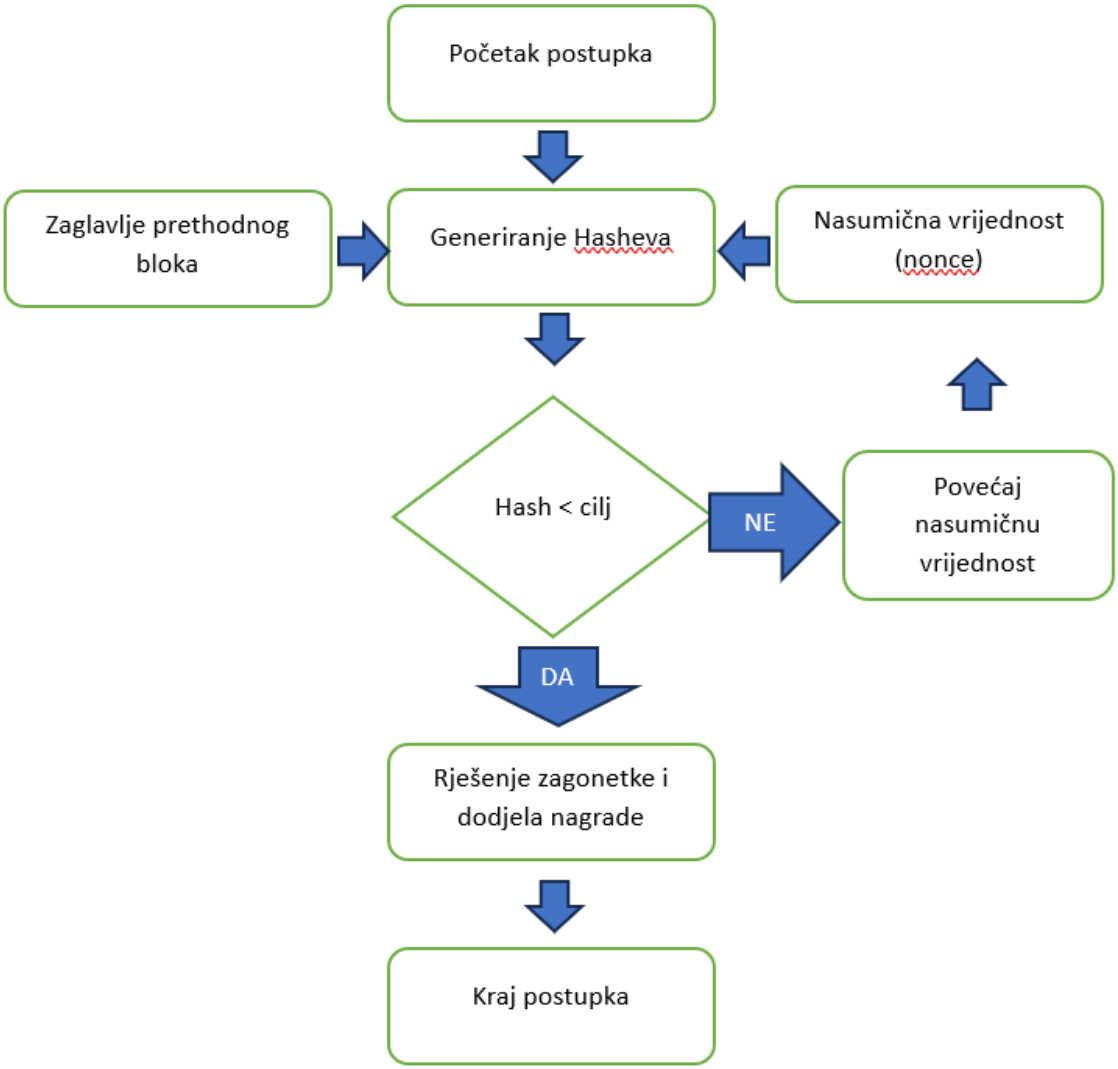
Algoritam raspršivanja je funkcija koja sve ulazne podatke bez obzira na njihovu količinu (slovo, riječ, rečenica, stranica, knjiga…) pretvara u izlaz fiksne duljine poznat pod nazivom *raspršivanje* (Rhodes, 2023). Koristi se u aplikacijama koje zahtijevaju brzu, sigurnu i dosljednu obradu podataka. Svojstva učinkovitih algoritama raspršivanja su:

1. Lakoća obrade – standardna računala moraju s lakoćom i gotovo trenutno pretvoriti bilo koji ulaz u izlaz.
2. Isti ulaz podataka mora rezultirati uvijek istim izlazom podataka
3. Izlazni podaci ne daju naznake o ulaznim podacima – svi izlazni podaci jednake su duljine bez obzira je li ulaz slovo, riječ, knjiga
4. Teško je pronaći različite ulaze koji daju iste izlazne podatke – broj ulaznih podataka u algoritam je beskonačan, ali broj izlaznih podataka je ograničen s obzirom na uvijek jednaku duljinu izlaznih podataka. Što je izlazni podatak duži, manja je vjerojatnost da će dva različita ulazna podatka dati isti izlazni podatak. Vjerojatnost da se to dogodi mora biti približno nula.
5. Pretvaranje podataka u obrnutom smjeru je gotovo nemoguć – algoritmi raspršivanja dizajnirani su na način da je inverzna funkcija nemoguća

Bitcoin koristi hash funkciju SHA-256 koja se smatra kompleksnim algoritmom. Prva rudarenja temeljila su se na korištenju procesorske moći (Central processing unit – CPU) te se naknadno prešlo na grafičke komponente računala (Graphics processing unit – GPU). Takva su se rudarenja izvršavala na vlastitoj opremi i trošila su velike količine električne energije. Vremenom su se rudari počeli udruživati u takozvane bazene rudara u vidu servera koji kombinira pojedinačnu računalnu snagu rudara i umrežuje ih čime se stvarala nova brza i efikasna mreža. 2013. godine osmišljava se super računalo čija je jedina svrha postojanja bilo rudarenje kriptovaluti. Računalo koristi integrirane sklopove za specifičnu primjenu (Application specific integrated circuit – ASIC). Rudari koji su koristili takav princip rudarenja i dalje su se udruživali čime se stvarala koncentracija rudara te je pojedinačno rudarenje postajalo sve teže. Rudarenje podrazumijeva izvođenje vrlo složenih matematičkih operacija kako bi se odgonetnule „zagonetke“ koje je rudarima postavio mehanizam Proof-of-work. Zadatak rudara je hashirati zaglavlje bloka tako da taj hash bude manji ili jednak „cilju“. Postupak rudarenja prikazan je na Slici br. 21. Postupak hashiranja zahtijeva veliki broj opetovanih pokušaja putem unošenja vrijednosti nasumične vrijednosti *nonce* sve dok se zagonetka ne odgonetne, odnosno pronađe odgovarajuća vrijednost (Ghimire, Selvaraj, 2018).

Jednom kad se zagonetka riješi, blok se prenosi čvorovima na mreži kako bi se potvrdio.

Ograničavajući faktor rudarenja je jačina procesora odnosno računala.



Slika 21. *Postupak rudarenja*

(izvor: https://www.researchgate.net/figure/Proof-of-Work-Flowchart_fig6_331040157, pristupano dana 8.9.2023.)

Litecoin je prva kriptovaluta koja je počela koristiti Scrypt unutar Proof-of-work konsenzusa. Scrypt je algoritam koji je vrlo sličan algoritmu SHA-256, ali koji ne zahtjeva jake procesore i ASIC već veliku količinu memorije. Naime, Scrypt je nastao kako bi se izbjegle koncentracije računala i omogućilo i drugim sudionicima mreže da rudare zahvaljujući velikim količinama memorije koju imaju na raspolaganju. Dok algoritam SHA-256 omogućuje paralelne izračune, Scrypt izračuni se moraju serijski izvršavati.

Za razliku od Litecoina, Ethereumom se željelo postići nešto više od jednostavnog prijenosa vlasništva i praćenja transakcija. Ethereum je svojevrsna jedinstvena programabilna platforma koja, uz prijenos vlasništva i praćenje istog, služi i za stvaranje i izvršavanje već prethodno

spomenutih i opisanih pametnih ugovora. Kako bi se pratile promjene stanja imovine, koristi se Ether – internu digitalnu valutu koju je moguće slati u transakcijama. Ether se može dijeliti na manje jedinice zvane *wei* te je 1 Ether jednak 10^{-18} wei.

U nastavku je prikazana denominacija Ethera (Slika 22.)

Value (in wei)	Exponent	Common name	SI name
1	1	wei	Wei
1,000	10^3	Babbage	Kilowei or femtoether
1,000,000	10^6	Lovelace	Megawei or picoether
1,000,000,000	10^9	Shannon	Gigawei or nanoether
1,000,000,000,000	10^{12}	Szabo	Microether or micro
1,000,000,000,000,000	10^{15}	Finney	Milliether or milli
1,000,000,000,000,000,000	*10^{18}*	*Ether*	*Ether*
1,000,000,000,000,000,000,000	10^{21}	Grand	Kiloether
1,000,000,000,000,000,000,000,000	10^{24}		Megaether

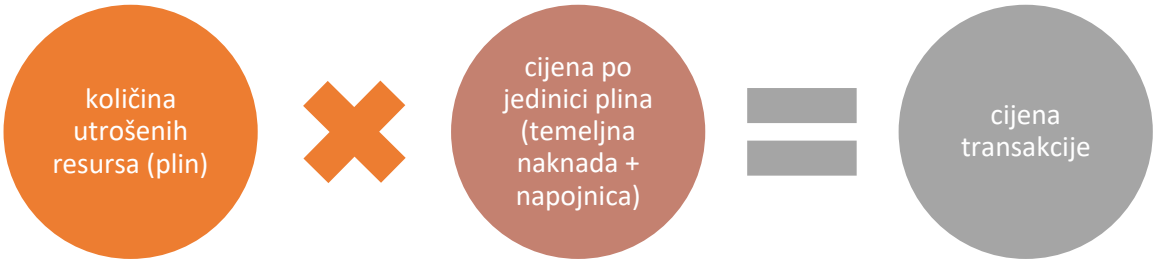
Slika 22. *Denominacija valute Ether (Izvor: https://dl.ebooksworld.ir/motoman/Mastering_Ethereum_Andreas.M.Antonopoulos.www.EBooksWorld.ir.pdf, pristupano dana 8.9.2023.)*

Osim weia, u Ethereumu postoji i parametar *plin (engl. gas)* koji služi kao sredstvo plaćanja troškova za izvršenje usluga na platformi. Plin je mjerna jedinica koja mjeri količinu računalnog napora koji je potreban kako bi se izvršila određena operacija na mreži. Takve naknade onemogućuju neželjenu „besplatnu“ poštu ili beskonačne petlje koje narušavaju sustav. Naknada za plin je umnožak utrošene količine plina (računalnih napora) potrebne za izvršenje neke operacije pomnožene s jediničnom cijenom plina. Prilikom isplate naknade rudarima i obračunu, plin se konvertira u Ehere odnosno weie.

Korisnik sustava sam određuje količinu gasa kojeg je spreman platiti kako bi se transakcija ili pametan ugovor izvršio. Nisko određena naknada može izgurati izvršenje transakcije dok će visoko postavljena naknada korisniku nepotrebno utrošiti Ether. Kako bi korisnik mogao realno odrediti cijenu naknade vodi se dvjema vrijednostima (@corwintines, 2023):

1. Base fee (temeljna naknada) – minimum koji se mora platiti
2. Priority fee (napojnica) – „savjet“ koliko dodati temeljnoj naknadi kako bi se ukupna naknada dojmila privlačnom za rudare i time osigurala prava tj. realna cijena za izvršenje transakcije.

Umnožak utrošene količine plina s cijenom po jedini utrošenog plina koja je nastala kao zbroj temeljne naknade i napojnice rezultira ukupnom cijenom (troškom) transakcije što je prikazano na slici broj 23:



Slika 23. *Primjer obračuna cijene transakcije na Ethereum platformi*

Naknadu za izvršenje transakcije objašnjena je u sljedećem primjeru:

Primjer: Osoba A šalje 1 ETH osobi B. Za to je potrebno utrošiti 10.000 jedinica plina. Iznos osnovne naknade je 5 gwei (10^{-9} ETH), sugerirana napojnica je 1 gwei. Kalkulacija:

Sa računa osobe A skida se 1,00006 ETH, osoba B će na svoj račun dobiti 1 ETH, validator dobiva napojnicu od 0,00001 gwei (10000 x 0,000000001 ETH).

Ethereum koristi razne programske jezike kako bi se pisali pametni ugovori, ali najviše se koristi programski jezik Solidity. Pametni ugorovi su nepromjenjivi kompjuterski kodovi koji se autonomno izvršavaju na Ethereum platformi pomoću EVM (*Ethereum virtual mashine*) i jednom ugrađenu u blockchain više se ne mogu mijenjati. Korisnici mogu pokrenuti izvršenje pametnog ugovora šaljući transakciju na adresu pametnog ugovora i određeni iznos Ethera, ako je to potrebno. Isto tako, jedan pametan ugovor može pokrenuti izvršenje drugog pametnog ugovora šaljući mu Ether.

Iz svega navedenog vidljivo je da je Litecoin koncipiran kako bi brzo, sigurno i jeftino izvršavao transakcije i pratio stanje imovine, dok je Ethereum osigurao osim navedenog i izvršavanje

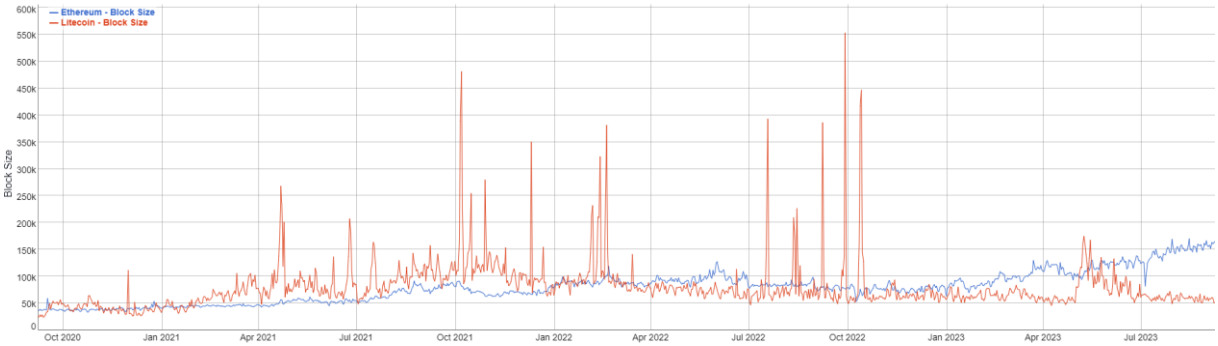
pametnih ugovora koje korisnici mogu sami programirati koristeći programski jezik Solidity i ugraditi ih u blockchain.

4.3. Veličina bloka

Charlie Lee je prilikom osmišljavanja Litecoina želio izbjeći nedostatke Bitcoin blockchaina te je smanjio veličinu bloka sa 1,024 KB na 256 KB kako bi skratio vrijeme stvaranja novog bloka i time onemogućio hakere u njihovoj nakani da manipuliraju blockchain transakcijama. Za stvaranje Bitcoin u prosjeku je potrebno oko deset minuta dok se blok Litecoina stvori u prosjeku za 2,5 minuta.

Svaki Ethereum blok ima ograničenu veličinu koja može varirati ovisno o zahtjevima mreže. Ciljna veličina bloka je 15 milijuna plina dok je maksimalna veličina bloka dvostruko veća odnosno 30 milijuna plina. To znači da ukupna količina utrošenog plina za izvršenje transakcija i pametnih ugovora mora biti manja od ograničenja kako bi se osiguralo da veličina blokova uvijek bude unutar određenih granica. S obzirom da svaki čvor u mreži mora provjeriti svaku transakciju, na taj se način omogućuje i manjim čvorovima (manje snage i memorije) sudjelovanje u radu mreže. Prosječno vrijeme za stvaranje Ethereum bloka je 12 sekundi.

U nastavku (Slika 24) je usporedba veličine blokova za Litecoin (crvena crta) i Ethereum (plava crta) prikazana grafičkim prikazom. Vidljivo je da su blokovi Litecoina ponekad iznadprosječno veliki dok su Ethereum blokovi podjednake veličine bez odstupanja.



Slika 24. *Veličina blokova Litecoin i Ethereum*

(Izvor: https://bitinfocharts.com/comparison/size-eth-ltc.html#3y, dostupno dana 8.9.2023.)

4.4. Protokol

Premda su obje kriptovalute nastale na protokolu Proof-of-work (opisano u poglavlju 1.6.1.), Litecoin je ostao i dalje na tom protokolu dok je Ethereum prešao na Proof-of-Stake protokol (opisano u poglavlju 1.6.2.). 2020. godine pokrenut je Ethereum POS blockchain koji je postojao usporedno s Ethereum glavnom mrežom i služio je za testiranje protokola i uklanjanje svih nedostataka koji su se pojavili kako bi prijelaz na novi protokol bio siguran. 2022. godine dogodio se prijelaz. Prelaskom rudari su zamijenjeni validatorima i potrošnja mreže smanjena je za više od 99% (Anonymus, Crypto, 2023) što je vrlo bitno u nastojanjima da se poslovanje i život učini održivim za buduće generacije.

4.5. Numerička usporedba

Premda kriptovaluta Bitcoin nije tema ovoga rada, neizostavna je u usporedbi kriptovaluti jer je ona bila prva kriptovaluta iz koje se razvio Litecoin.

Kako bi se kriptovalute mogle numerički, odnosno statistički usporediti, u nastavku, u Tablici broj 1, prikazani su podaci i vrijednosti koje su objavljene na dan 7.8.2023. godine na mrežnim stranicama *https://bitinfocharts.com/:*

Tablica 1.: Financijski i drugi podaci za Bitcoin, Ethereum i Litecoin na dan 7.8.2023. godine

Kategorija usporedbe	BITCOIN	LITECOIN	ETHEREUM
Broj postojećih tokena	19,450,302 BTC	74,834,968 LTC	127,029,547 ETH
Tržišna kapitalizacija	$565,448,752,912	$6,110,002,010	$231,268,756,946
Vrijednost za jedinicu na današnji dan	29,071.46 USD	81.65 USD	1,820.59 USD
Broj transakcija u posljednja 24 sata	448,541	148,477	1,036,575
Prosječni broj transakcija po satu	18,689	6,187	43,191
Promet u posljednja 24 sata	146,268 BTC ($4,264,498,482) 0.7520 % market cap	16,264,470 LTC ($1,330,694,043) 21. 73% market cap	846,462 ETH ($1,543,480,225) 0.6 664% market cap

Prosječan promet po satu u posljednja 24 sata	6,094 BTC ($177,687,437)	677,686 LTC ($55,445,585)	35,269 ETH ($64,311,676)
Prosječna vrijednost transakcije	0.3261 BTC ($9,507)	109.54 LTC ($8,962)	0.8166 ETH ($1,489)
Medijan vrijednosti transakcije	0.0000033 BTC ($0.096)	1.13 LTC ($92.34)	0 ETH ($0)
Prosječna naknada za transakciju	0.000028 BTC ($0.81) 0.00000014 BTC/byte	0.000093 LTC ($0.0076) 0.0000003 5 LTC/byte	0.0028 ETH ($5.11)
Medijan vrijednosti za naknadu za transakciju	0.0000089 BTC ($0.258)	0.0000073 LTC ($0.0006)	0.0011 ETH ($1.93)
Prosječno vrijeme stvaranja bloka	9m 48s	2m 46s	12.1s
Trenutni broj blokova	802,131 (2023-08-07 20:48:18)	2,522,883 (2023-08-07 20:57:33)	17,865,017 (2023-08-07 21:03:47)
Veličina bloka	761.247 KBytes	54.241 KBytes	145.643 KBytes
Stvoreno blokova u zadnja 24 sata	145	519	7,127
Prosječan broj stvorenih blokova u satu u zadnja 24 sata	6	22	297
Nagrada po stvorenom bloku	6.25+0.1353 BTC ($186,164. 8) next halving @ block 840000 (in 37869 blocks ~ 257 days)	6.25+0.02122 LTC ($513. 09)	2+0.4074+0+0- 0.324 ETH ($3,798.96)
Nagrade u posljednja 24 sata	906.25+19.61 BTC ($26,993, 895.46)	3,244+11.01 LTC ($266,2 91.62)	14,254+2903+0+0- 2309 ETH ($27,075,207)
Naknada za nagradu	1.62%	0.3%	2.8%
Profitabilnost rudarenja	0.0628 USD/Day for 1 THash/s	0.3545 USD/Day for 1 GHash/s	0 USD/Day for 1 Hash/s
100 najbogatijih	2,863,392 BTC ($83,483,395,513) 14.72 % Total	32,149,609 LTC ($2,630,352,841) 42. 96% Total	-
Piramida bogatstva (najboljih 10/100/1.000/10 .000 adresa)	5.79% / 14.72% / 32.90% / 55.58% Total	14.66% / 42.96% / 70.66% / 98.37% Total	-
Adrese prema bogatstvu (najboljih	40,624,078 / 17,007,709 / 7,293,083 / 2,089,129	2,400,027 / 745,378 / 204,003 / 30,508	-

10/100/1.000/10.000 adresa)			
Aktivne adrese u posljednja 24 sata	749,288	206,669	585,229
100 najvećih transakcija	last 24h: 300,367 BTC ($8,757,330,797) 205.35% Total	last 24h: 4,817,651 LTC ($394,160,960) 29.62% Total	last 24h: 290,070 ETH ($528,928,220) 34.27% Total
Nastanak prvog bloka	09.01.2009	08.10.2011	30.07.2015
Veličina blockchaina	491.50 GB	91.10 GB	345.17 GB

Izvor: *https://bitinfocharts.com, pristupljeno 7.8.2023.*

Iz navedenih podataka vidljivo je da se sve tri kriptovalute razlikuju po tržišnoj vrijednosti, veličini blokova, veličini blockchaina, brzini stvaranja blokova, broju transakcija i nizu drugih pokazatelja. Možemo ih usporediti s motornim vozilima. Ukoliko usporedimo motocikl, osobni automobil i dostavno vozilo, osnovna svrha sva tri vozila je prevesti osobu i predmete od točke A do točke B.

Svako od tih vozila može izvršiti taj zadatak, ali na drugačiji način i s različitim mogućnostima. Korisnici znaju kakav im je prijevoz potreban. Žele li uživati u vožnji i izbjegavati gužve, odabrati će motocikl znajući da može prevesti maksimalno dvije osobe i malo predmeta. Za ugodniju vožnju do pet osoba i nešto više predmeta, korisnici će odabrati osobni automobil. Trebaju li prevesti veću količinu predmeta ili predmete većih dimenzija, odabrati će dostavno vozilo. Zaključujemo da korisnici imaju odlučujuću ulogu u odabiru prijevoznog sredstva, a odluka se temelji na njihovim potrebama.

S obzirom da su sve tri kriptovalute i dalje vrlo aktivne te da ih korisnici svakodnevno koriste za svoje transakcije i u druge svrhe, činjenica je da su bez obzira na razlike, pronašle svoje korisnike.

5. Zaključak

Kriptovalute su valute koje su još nedovoljno poznate ljudima, zainteresiranim individualcima, pa čak i korisnicima koji se njima već koriste. Zbog složenog načina funkcioniranja i potrebnog određenog stupnja obrazovanja na području računalstva, još uvijek su ograničene na manju skupinu ljudi koji su voljni razumijeti i primjenjivati principe na kojima se temelje kriptovalute.

Suvremeni razvoj tehnologije, nova dostignuća u računalstvu i sve zahtjevniji složeni sustavi upravljanja i poslovanja, neminovno utječu na ljude i njihov svjetonazor.

Otpor u promjeni novih postignuća je normala ljudska pojava jer zahtjeva dodatno ulaganje vremena, novca i truda u učenje i razumijevanje, ali ujedno je i jedini način da se društvo dalje razvija.

Blockchaini i kriptovalute nailaze na skeptike isto kao što su na skeptike nailizile prve kovanice, papirne novčanice i kreditne kartice, a danas su sastavni dio svakodnevice koje postupno, ali sigurno, zamjenjuju novi pojavni oblici novca odnosno vrijednosti.

Nematerijalna pojava kriptovaluta koja postoji samo u virtualnom svijetu sa sobom donosi i određeni stupanj straha i nepovjerenja, ali nezaobilazna je buduća etapa u razvoju financijskih i drugih transakcija.

Ethereum i Litecoin su kriptovalute koje su se razvile na principu blockchaina, prihvaćene su kao siguran oblik izvšavanja transakcija te imaju svoje sličnosti i različitosti, prednosti i mane.

Neminovno je da će se dalje razvijati prema potrebama sudionika i novim postignućima te će se zasigurno, osim transakcija, u budućnosti u njih ugraditi i mnoge druge vrijednosti.

S obzirom na njihove osobine, obje kriptovalute su pronašle veliki broj pobornika koji ih koriste svakog trenutka i zahaljujući kojima opstaju i razvijaju se u suvremenom svijetu.

Literatura

Knjige

Dannen, C., (2017.): *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. [online]. New York, SAD: Apress, str. 10., 89-138., Dostupno na: http://ndl.ethernet.edu.et/bitstream/123456789/26027/1/Chris%20Dannen.pdf

Mohanty, D., (2018.): *Ethereum for Architects and Developers: With Case Studies and Code Samples in Solidity.* [online]. Noida, Uttar Pradesh, Indija: Apress, pp. 1-54., Dostupno na: https://content.e-bookshelf.de/media/reading/L-11856868-3b8b3ec656.pdf

Antonopoulos, A. M. & Wood, G. (2019), Mastering Ethereum, [e-book], Sebastopol, USA, O'Reilly Media, Inc, dostupno na https://dl.ebooksworld.ir/motoman/Mastering_Ethereum_Andreas.M.Antonopoulos.www.EBooksWorld.ir.pdf, [pritupljeno 8.9.2023.]

Druga literatura

Arunović, D., (2018), *Što je u stvari blockchain i kako radi?* [online], dostupno na https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011, [pristupljeno 4.8.2023.]

Čavrak, H., (n.d.), Enigma, *Hrvatski matematički elektronski časopis* [online], dostupno na http://e.math.hr/old/enigma/index.html, [pristupljeno 4.8.2023.]

Frankenfield, J., (n.d.), *What Is Ethereum and How Does It Work?*, [online] Investopedia, dostupno na: https://www.investopedia.com/terms/e/ethereum.asp, [pristupljeno: 22.9.2021]

Ghimmire, S., Selvaraj, H. (2018), *A Survey on Bitcoin Cryptocurrency and its Mining*, ResearchGate, dostupno na:

https://www.researchgate.net/publication/331040157_A_Survey_on_Bitcoin_Cryptocurrency_and_its_Mining, [pristupljeno 8.9.2023.]

Kolić, J., (2017), *Što je Ethereum, gdje ćemo ga koristiti, kakva ga budućnost čeka – doznali smo u Splitu!* [online], dostupno na https://www.netokracija.com/ethereum-valuta-tomislav-mamic-139768, [pristupljeno 7.8.2023.]

Mirković, I., (2020), *Vitalik Buterin - Mladi genij modernog doba* [online], dostupno na https://ecd.rs/blog/vitalik-buterin-mladi-genije-savremenog-doba/, [pristupljeno 7.8.2023.]

Nešić, S., (2021), *Šta je Pametni Ugovor – Smart Contract?* [online], dostupno na https://ecd.rs/blog/sta-je-pametni-ugovor-smart-contract/, [pristupljeno 7.8.2023.]

Rhodes, D., (2023.): *Što je algoritam raspršivanja? Uvod*, Komodo, dostupno na: https://komodoplatform.com/en/academy/hashing-algorithm/, [pristupljeno 8.9.2023.]

Sarwar M.I., Nisar K., Khan A., (2019.): *Blockchain – From Cryptocurrency to Vertical Industries - A Deep Shift*, dostupno na: www.researchgate.net/figure/Formation-of-Blockchain-6_fig1_338651863, [pristupljeno 4.8.2023.]

Sheldon, R., (2021), *A timeline and history of blockchain technology* [online], dostupno na https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology, [pristupljeno 4.8.2023.]

Swarowski.eth, (2022.), *Blockchain tehnologija – provijest, Medium.com*, dostupno na: https://medium.com/@swarowski.eth/blockchain-tehnologija-povijest-933c77e1ecbf [pristupljeno 4.8.2023.]

Vrbanus, S. (2021), *Što su nft-i i zašto ljudi za njih daju milijune?* [online], dostupno na https://www.bug.hr/blockchain/sto-su-nft-i-i-zasto-ljudi-za-njih-daju-milijune-19244, [pristupljeno 4.8.2023.]

@corwintines (2023): *Plin i naknade*, Ethereum.org, dostupno na: https://ethereum.org/en/developers/docs/gas/, [pristupljeno 8.9.2023.]

Bitcoin store, (2022), *Što je blockchain i kako funkcionira?* [online], dostupno na: https://www.bitcoin-store.hr/blog/sto-je-blockchain-i-kako-funkcionira/, [pristupljeno 4.8.2023.]

Bitcoin store (2022), *Što je Proof of Work? Značenje, obilježja i prednosti* [online], dostupno na: https://www.bitcoin-store.hr/blog/sto-je-proof-of-work/, [pristupljeno 4.8.2023.]

Bitcoin store (2023), *Što je Proof of Stake? Značenje, obilježja i prednosti* [online], dostupno na: https://www.bitcoin-store.hr/blog/sto-je-proof-of-stake/, [pristupljeno 4.8.2023.]

Bitcoin store (2021), *Što je NFT i kako funkcionira? Vodič za početnike* [online], dostupno na: https://www.bitcoin-store.hr/blog/sto-je-nft-i-kako-funkcionira-vodic-za-pocetnike/, [pristupljeno 7.8.2023.]

Bitcoin store (n.d.), *Litecoin LTC* [online], dostupno na: https://www.bitcoin-store.hr/kriptovalute/litecoin-ltc/, [pristupljeno 7.8.2023.]

Crypto (2023), *Posebno rođendansko izdanje Ethereuma: 8 godina decentralizacije* [online], dostupno na: https://kriptovijesti.net/posebno-rodendansko-izdanje-ethereuma-8-godina-decentralizacije/, [pristupljeno 7.8.2023.]

Kriptomat atm (n.d.), *Što je Litcoin (LTC)?* [online], dostupno na https://kriptomat.cash/sto-je-i-kako-funkcionira-litecoin/, [pristupljeno 7.8.2023.]

Kriptoportal (2021), *Šta je Ethereum i zbog čega je jedan od najvažnijih kripto projekata?* [online], dostupno na https://kriptoportal.net/sta-je-ethereum/, [pristupljeno 7.8.2023.]

Litecoin foundation Ltd (n.d.), *What is Litecoin?* [online], dostupno na https://www.litecoin.net/what-is-litecoin#get-started, [pristupljeno 7.8.2023.]

Rhodes D. (2020), *What's A Hashing Algorithm? An Introduction* [online], dostupno na: https://komodoplatform.com/en/academy/hashing-algorithm/, [pristupljeno 8.10.2023.]

Popis slika

Sažetak

Temeljni cilj ovog rada je bio prikaz razvoja dviju kriptovaluta tokom povijesti te njihove sličnosti, razlike i primjena. Ethereum i Litecoin se, za razliku od Bitcoin-a, obrađuju puno brže. Znatiželja je došla u tome, kako i po čemu razlikujemo kriptovalute, naspram fizičkih valuta država. Svaka valuta ima različite aspekte, poput Ethereum-a. Osim generalnih transakcija Ethera (Ξ), valute Ethereum-a, također nudi i razmjenu raznih medija, poput slika, zvuka, i ostale vrste. Današnjim razmišljanjima, kriptovalute su još daleko od prihvaćanja većinu ljudi, uglavnom zbog nesigurnosti.

Ključne riječi:

kriptovaluta, Bitcoin, Ethereum, Litecoin, blockchain, valuta, medij, Ether

Abstract

The basic goal of this paper was to show the development of two cryptocurrencies throughout history and their similarities, differences and applications. Ethereum and Litecoin, unlike Bitcoin, are processed much faster. Interest began on how and by what we distinguish cryptocurrencies from the physical currencies of coutries. Each currency has different aspects, like Ethereum. In addition to the general transactions of Ethereum (Ξ), Ethereum's currency, it also offers the exchange of various media, such as images, sound, and other types. In today's thinking, cryptocurrencies are still far from being accepted by most people, mostly due to uncertainty.

Key words:

cryptocurrency, Bitcoin, Ethereum, Litecoin, blockchain, currency, medium, Ether