

PRIRUČNIK

2023



Tehnologija ulančanih blokova i kriptovaluta

Neven-Lucian Davidović

Patricija Ronta

Allesmont j.d.o.o.



Tehnologija ulančanih blokova i kriptovaluta
Neven-Lucian Davidović
Patricija Ronta

Ovaj priručnik izrađen je za potrebe projekta RCK ELPROS, referentni broj Poziva: UP.03.3.1.04 „Uspostava regionalnih centara kompetentnosti u strukovnom obrazovanju u (pod)sektorima: strojarstvo, elektrotehnika i računalstvo, poljoprivreda i zdravstvo“, Referentni broj Ugovora UP.03.3.1.04.0015. u okviru Europskog socijalnog fonda.

Copyright © 2023 Allesmont j.d.o.o.

Sva prava pridržana. Nijedan dio ovog priručnika ne smije se reproducirati ili koristiti na bilo koji način bez prethodnog pisanog dopuštenja vlasnika autorskih prava, osim upotrebe kratkih citata u prikazu priručnika.

Prvo papirnato izdanje: Studeni 2023.

Autori: Neven-Lucian Davidović (2. i 4. poglavlje), univ.bacc.ing.el. i Patricija Ronta (1., 3. i 5. poglavlje), univ.bacc.ing.el.

Tiskano u studenome 2023.

Sadržaj priručnika isključiva je odgovornost Korisnika.



Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.



Sadržaj

I

Prvi dio

I	Novac	11
1.1	Povijest i evolucija novca	11
1.1.1	Tumačenje i svrha novca	11
1.1.2	Temeljne uloge novca	12
1.1.3	Razvoj novca	14
1.1.4	Ostale rane valute	20
1.2	Zlatni standard - prethodnik fiat novcu	21
1.3	Fiat novac	22
1.3.1	Razlika između novca i valute	23
1.4	Razvoj monetarnih sustava	24
1.5	Elektronički novac	26
1.6	Digitalni novac - nastanak kriptovaluta	28
1.7	Razvoj Bitcoina i Kriptovaluta	28
1.7.1	Kriptovalute pored Bitcoina	29

Drugi dio

2	Tehnologije iza kriptovaluta	33
2.1	Razvoj interneta	34
2.2	Bitcoin	35
2.3	Model ravnopravnih partnera (<i>Peer to peer</i> mreža)	36
2.3.1	Značajke P2P mreže	37
2.3.2	Spajanje na <i>Peer to Peer</i> mrežu	37
2.4	Decentralizacija	38
2.5	Tehnologije koje su dovele do razvoja Bitcoin kriptovalute	39
2.6	Kriptografija	39
2.6.1	Osnovni koncepti kriptografije	39
2.6.2	Simetrična i asimetrična kriptografija	39
2.6.3	Kriptografska hash funkcija	41
2.6.4	Merkle stablo	43
2.6.5	Vremenska oznaka (<i>eng. Time-stamp</i>)	43
2.6.6	Vremenska oznaka Unix	44
2.6.7	Vremenske oznake u tehnologiji ulančanih blokova	45
2.6.8	Rudarenje ulančanih blokova	45
2.6.9	Pametni ugovori <i>eng. Smart Contracts</i>	45
2.6.10	Dokaz radom - PoW (<i>eng. Proof of Work</i>)	47
2.6.11	Prednosti i nedostaci PoW-a	48
2.6.12	Secure Hash Algorithm	48
2.6.13	Generiranje hash-a	49
2.7	Digitalni potpis	56
2.7.1	Algoritam digitalnog potpisa s eliptičnom krivuljom - ECDSA	58
2.7.2	Kriptografija eliptičnih krivulja – ECC – Elliptic Curve Cryptography	58
2.8	Tehnologija ulančanih blokova (<i>eng. Blockchain</i>)	59
2.8.1	Ključna svojstva – četiri stupa tehnologije ulančanih blokova	59
2.8.2	Konstrukcija lanca u tehnologiji ulančanih blokova	60

Treći dio

3	Blockchain tehnologija ≠ kriptovalute	65
3.1	Blockchain više je od kriptovalute	65
3.2	Pregled primjene Blockchain tehnologije	65
3.3	Upravljanje lancima opskrbe	66

3.4	Decentralizirane financije	68
3.5	Preoblikovanje financijskih eko-sustava	69
3.6	Postoji li najbolji blockchain sustav za DeFi?	69
3.7	Cardano	70
3.8	Byron: Temeljni razvoj	70
3.9	Shelly: Decentralizacija kontrole	71
3.10	Gougen: era pametnih ugovora	71
3.11	Basho: skaliranje	71
3.12	Voltaire - Upravljanje	71
3.13	ADA - token Cardano mreže	72
3.14	Polkadot	72
3.15	Paralelni lanci blokova	73
3.16	Substrate - razvojno okruženje za Polkadot blockchain	74
3.17	Kusama - platforma za istraživanje i razvoj	74
3.18	Hyperledger Blockchain	75
3.19	Hyperledger Fabric	75
3.20	Fabric pametni ugovori - ChainCode	76
3.21	Sastavni dijelovi Hyperledger Fabric sustava	77
3.22	Hyperledger Sawtooth	77
3.23	Blockchain podrazumijeva transparentno poslovanje	79

IV

Četvrti dio

4	Bitcoin eko sustav	85
4.1	Bitcoin eko sustav - najpoznatija primjena <i>blockchain</i> tehnologije	85
4.2	Prethodnici Bitcoin kriptovalute	86
4.2.1	Bit Gold Kriptovaluta	86
4.2.2	Usporedba Bit Golda i Bitcoina	87
4.2.3	Ključne karakteristike i spoznaje Bit Golda	87
4.2.4	Trostruko knjigovodstvo (<i>eng. Triple Entry Accounting</i>)	87
4.2.5	Javne transakcije	90
4.3	Arhitektura	92
4.4	Problem dvostrukog trošenja (<i>eng. Double-spending Problem</i>)	93
4.4.1	Rješenje problema dvostrukog trošenja	93

4.5	Vlasništvo	94
4.6	Novčanici za kriptovalute	94
4.6.1	Odabir novčanika	95
4.6.2	Sigurnost ovisno o vrsti novčanika – naglasak na desktop novčanike	95
4.6.3	Sigurne transakcije	97
4.6.4	Dvofaktorska autentifikacija	97
4.6.5	Multi-potpis	97
4.6.6	Razlika između Novčanika i Klijenta	97
4.6.7	Podjela novčanika prema odnosu ključeva	98
4.7	Podjela novčanika na vruće i hladne novčanike	100
4.7.1	Popunjavanje novčanika	104
4.7.2	Slanje plaćanja	104
4.8	Transakcije	104
4.8.1	Verifikacija transakcije	106
4.9	Kreiranje Bitcoina i značenje rudarenja	106
4.9.1	Rudarenje i postupak rudarenja	106
4.9.2	Rudarenje u rudarskim bazenima (<i>eng. Mining pools</i>)	107
4.9.3	Rudarska oprema	108
4.10	Napadi na Bitcoin, blockchain mreže i novčanike	109
4.10.1	Sybil napad (<i>eng. Sybil attack</i>)	109
4.10.2	Napad većine ili 51% napad (<i>eng. 51% attack, Majority attack</i>) .	109
4.10.3	Napad dvostrukog trošenja (<i>eng. Double spending attack</i>)	110
4.10.4	Nedostatak konsenzusa (fork)	110
4.10.5	Napad sebičnog rudarenja (<i>eng. Selfish mining attack</i>)	110
4.10.6	Napad vremenskog presretanja (<i>eng. Timejack attack</i>)	110
4.10.7	Finney napad (<i>eng. Finney attack</i>)	111
4.10.8	Napad utrke (<i>engl. Race attack</i>)	111
4.10.9	Napadi na Pametne ugovore (<i>engl Smart Contract-based Attacks</i>)	111

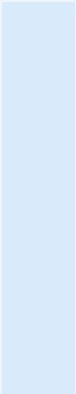
V

Peti dio

5	Bitcoin i energija	115
----------	---------------------------------	------------

VI

Bibliografija



Prvi dio

1	Novac	11
1.1	Povijest i evolucija novca	
1.2	Zlatni standard - prethodnik fiat novcu	
1.3	Fiat novac	
1.4	Razvoj monetarnih sustava	
1.5	Elektronički novac	
1.6	Digitalni novac - nastanak kriptovaluta	
1.7	Razvoj Bitcoina i Kriptovaluta	



1. Novac

1.1 Povijest i evolucija novca

Povijest novca obuhvaća tisućljeća evolucije, od direktnog sustava razmjene do suvremenog digitalnog novca. Tradicionalan novac, poput kovanica i papirnatih novčanica, imao je svoje korijene u fizičkom obliku, ali se s vremenom razvijao reflektirajući drukčije potrebe i društveni napredak. S pojavom interneta i digitalne revolucije, elektronički je novac postao sveprisutan, no njegova je osnova ostala vezana uz centralizirane financijske institucije kao što su banke [1].

U ovom će se poglavlju definirati pojam *novac*, njegova evolucija tijekom povijesti te će se objasniti što je to centralizirani sustav kao predstavnik tradicionalnog financijskog sustava i koji se uzroci kriju, osim prirodnog razvoja društva, za potrebu i stvaranje decentraliziranih sustava.

1.1.1 Tumačenje i svrha novca

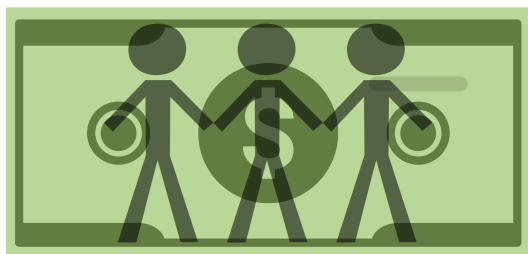
Kada se spomene riječ *novac*, može se reći da je prva asocijacija, vezana na pojam, *trgovina*. Drugim riječima, novac se asocira kao univerzalna jedinica koja ljudima omogućuje zamjenu gotovine za gotovo sve što žele, stoga je novac svojevrsna roba za koju se može kupiti svaka druga roba. Međutim, novac je više od sredstva razmjene ili mjere bogatstva. Poput nevidljive niti, on prodire u tkivo društva, oblikuje njegove vrijednosti i usmjerava kretanja. Ako se novac promatra kao pokretač društvenih vrijednosti, može se uočiti da on često nije samo ekonomski entitet, već i moralni pokazatelj, odražavajući sustav prioriteta i vrijednosti koje zajednica cijeni.

U društvu u kojem novac igra ključnu ulogu, on postaje katalizator društvenih normi i običaja. Način na koji se novac troši ili štedi, na što se troši i zašto, oslikava dublje uvjerenje zajednice te postaje alat kojim se izražava identitet, položaj i čak moralna vrijednost pojedinca.

Ako se u svijetu financijska moć često doživljava kao mjera uspjeha, tada novac postaje pokazatelj društvene moći. Određuje pristup obrazovanju, zdravstvenoj skrbi i mogućnosti napredovanja. Ovaj aspekt novca čini temelj društvene hijerarhije i raspodjele mogućnosti, često oblikujući društvene interakcije i odnose.

Osim toga, novac može biti katalizator promjena. Kroz filantropiju, ulaganja u obrazovanje ili podršku inovativnim projektima, novčana sredstva mogu pomaknuti društvenu mobilnost prema većoj jednakosti, pravdi ili napretku. Više nego samo sredstvo osobnog bogaćenja, njegova uloga pokretača društvenih vrijednosti leži u njegovoj upotrebi za oblikovanje zajednica i svijeta na bolje.

Prema navedenom, može se zaključiti da, u suvremenom društvu, novac igra ključnu ulogu ne samo u gospodarskom pogledu, već i u društvenim i psihološkim aspektima. Razumijevanje temeljne svrhe novca ide dalje od njegove praktične upotrebe; ona seže do dubljih slojeva identiteta i vrijednosti. Stoga, njegova uloga nije samo funkcionalna, već ima šire implikacije koje oblikuju našu percepciju svijeta i način na koji se društvo međusobno povezuje.



Slika 1.1: *Novac kao pokretač društvenih vrijednosti*

1.1.2 Temeljne uloge novca

Iako novac može biti fizički prisutan, njegova esencijalna vrijednost i moć proizlaze iz ideje koja ga podržava kao:

1. sredstvo razmjene
2. spremnik vrijednosti
3. obračunsku jedinicu

Navedeno predstavlja tri ključne funkcije novca koje ga čine vitalnim elementom u svakodnevnom funkcioniranju društva.

Novac kao sredstvo razmjene znači da je široko prihvaćen kao način plaćanja te time značajno olakšava trgovinu i obavljanje transakcija. Ako se zamisli zamjena dobara bez novca, takav proces bi bio nepraktičan te bi zahtijevao pronalazak određene osobe koja ima ono što vi želite i istovremeno želi ono što vi imate. U današnjoj, suvremenoj ekonomiji, ovakav bi proces tražio enormno puno vremena i truda te bi, sadašnjem naraštaju društva, ovakva razmjena bila gotovo nemoguća. Novac eliminira taj problem djelujući kao posrednik - ljudi mogu zamijeniti proizvode ili usluge za novac, a zatim taj isti novac druga strana može iskoristiti za kupnju dobara koji su njoj potrebni. Upravo zbog toga, novac je stup suvremenog gospodarstva i trgovine, omogućavajući da se transakcije svakodnevno obavljaju bez suvišnih poteškoća.

Spremnik vrijednosti obično se odnosi na različite oblike investicija ili sredstava koja se koriste za akumulaciju bogatstva ili kapitala s nadom ili predviđanjem da će njihova

buduća vrijednost porasti. Primjerice, uobičajeni načini štednje ili otvaranje investicijskih računa u bankama može služiti kao sredstvo za pohranu vrijednosti jer se očekuje da će se kroz određeno vrijeme dobiti kamate ili prinos na uloženi kapital. S druge strane, ulaganje u dionice ili plemenite metale poput zlata, također može predstavljati sredstvo za čuvanje vrijednosti.

Važno je napomenuti da izbor sredstava za čuvanje vrijednosti ovisi o investicijskim ciljevima i razinama prihvatljivog rizika. Iako novac može biti pouzdan spremnik vrijednosti, investitori se suočavaju s mnogobrojnim izazovima, uključujući inflaciju i kamate. Stoga je diversifikacija portfelja¹ često ključna kako bi se postigla stabilnost i rast financijskih sredstava.

Nadalje, novac djeluje i kao obračunska jedinica, što znači da postavlja referentnu točku za usporedbu vrijednosti različitih dobara i usluga. Ako bi se vrijednosti robe izražavale u različitim stvarima umjesto u novcu, tada bi se, primjera radi, reklo da je neko računalo vrijedno 200 sati rada ili da je vrijedan ekvivalentu vrijednosti od pet bicikala. To bi svaku transakciju učinilo izuzetno složenom jer bi trebalo svakovremeno uspoređivati različite vrste dobara kako bi se razumjela vrijednost robe koja se kupuje. Zbog toga novac funkcionira kao zajednička mjera vrijednosti te pruža zajednički standard za procjenu vrijednosti svih dobara i usluga.



Slika 1.2: *Funkcije novca*

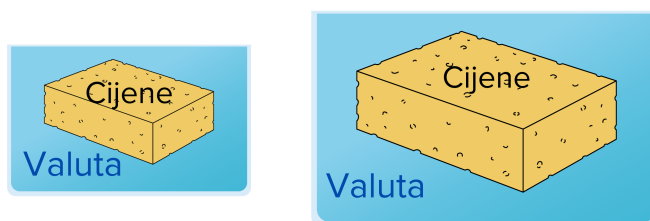
U svakoj su od navedenih funkcija novca prisutni kompromisi, odnosno niti jedna valuta nije savršena. Ako valuta preuzima ulogu spremnika vrijednosti, uglavnom se očekuje da će očuvati ili čak povećati svoju vrijednost tijekom vremena. Međutim, valute su često podložne promjenama volatilnosti i tržišnim fluktuacijama, što može rezultirati gubitkom vrijednosti, stoga pozitivan ishod ulaganja nije uvijek osiguran. Osim toga, kako bi valuta bila učinkovita kao obračunska jedinica, ona mora biti vrlo stabilna kako bi omogućila pouzdano izračunavanje cijena i vrijednosti dobara i usluga. Postizanje te stabilnosti može zahtijevati određene kontrole i intervencije u okviru monetarne politike², koja, pak, može utjecati na različite aspekte ekonomije.

Da bi valuta bila sredstvo razmjene, ona mora biti dovoljno prihvaćena i lako dostupna. Međutim, kako valuta postaje popularna i široko rasprostranjena, tako se javlja problem inflacije. Aktualan primjer ovakvog slučaja je kada je Republika Hrvatska iz valute *kuna* prešla na valutu *euro*. Neposredno prije uvođenja nove valute, cijene gotovo svih dobara

¹Financijska strategija koja se koristi kako bi se smanjio rizik investiranja putem ravnomjerne raspodjele sredstava u različite vrste investicija

²Predstavlja segment ekonomske politike kojim se regulira ponuda novca, kamatne stope i druge monetarne mjere s ciljem postizanja specifičnih ekonomskih ciljeva i stabilizacije gospodarstva

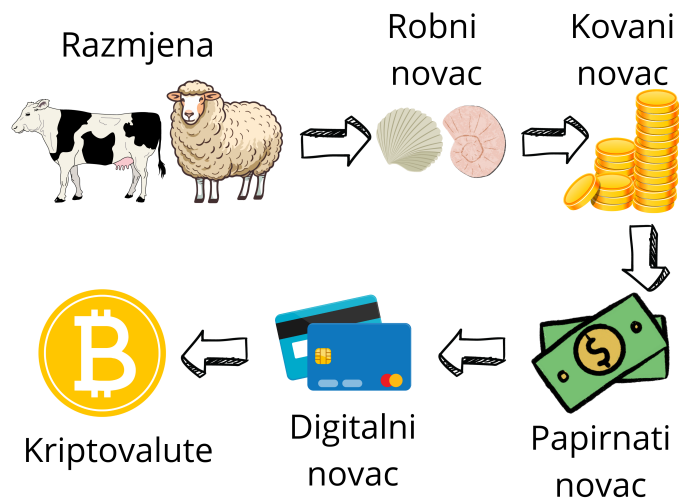
naglo su porasle, ali to nije imalo veze s proizvodnjom i vrednovanjem proizvoda, nego se ova inflacija temeljila na činjenici da zbog prekomjernog štampanja novih euro novčanica i pripremanja cijele države na novu valutu, euro je gubio na vrijednosti. Opisani problem slikovito prikazuje slika 1.3 gdje se *cijena* može smatrati kao spužva postavljena na bazen kojeg predstavlja *valuta*. Povećanjem dimenzije bazena i količine vode u njemu, odnosno povećanje opskrbom valuta, spužva, tj. cijene sada više upijaju ovakvu promjenu te za posljedicu dolazi do inflacije.



Slika 1.3: Utjecaj rasprostranjenosti valute na cijene

1.1.3 Razvoj novca

Razvoj je novca evoluirao kroz povijest kako bi zadovoljio potrebe ljudi za trgovinom i razmjenom. Razvojni put novca, počevši od trampe ili direktne razmjene, poput zamjene dobara, do kompleksnih financijskih sustava, pruža bolje shvaćanje uloge i utjecaja novca na sam život ljudi i gospodarski život. Na slici 1.4 prikazana je razvojna etapa novca.



Slika 1.4: Razvoj novca

Trampa ili direktna razmjena

Direktna razmjena, poznata i kao barter trgovina ili trampa, predstavlja oblik razmjene dobara ili usluga bez upotrebe novca kao posrednika. Ovaj koncept datira iz davnih vremena prije nego što je novac postao primarni način trgovine te predstavlja najjednostavniji oblik trgovanja. Prije nego što je novac postao glavno sredstvo razmjene, ljudi su u ranim zajednicama imali jednake potrebe za trgovinom kao i ljudi današnjega vremena. Međutim,

svaki pojedinac ili zajednica imali su različite potrebe u kontekstu određenih dobara i usluga. Neki su imali viška hrane, drugi su bili vješti u izradi alata ili odjeće, dok su treći imali veći broj resursa i imovine. Upravo je trgovanje omogućilo ljudima da zadovolje svoje raznolike potrebe razmjenom viška onoga što su imali za ono što im je nedostajalo.

Barter se trgovina prakticirala diljem svijeta tijekom raznih vremenskih razdoblja i kulturnih konteksta. U drevnim civilizacijama poput Mezopotamije, Kine i Egipta, ljudi su razmjenjivali proizvode kao što su stoka, tkanine, cigarete, sol, žito, pšenica i slično, koja su imala intrinzičnu vrijednost ili su se smatrala vrijednima u toj zajednici. Upravo je takav način trgovanja potaknuo lokalnu proizvodnju i zajednice na razvijanje resursa koji su im dani prirodom i uvjetima. Lokalni je farmer mogao razmijeniti vlastito uzgojene žitarice za odjeću s krojačem ili alat s kovačem, stoga su u ovakvom sustavu trgovanja ljudi bili slobodni od bankarskih računa i transakcija.

Međutim, jedan je od najvećih izazova direktne razmjene bila procjena vrijednosti dobara i usluga koje se razmjenjuju. Odnos vrijednosti između različitih proizvoda ili usluga može varirati, što može rezultirati neuravnoteženom razmjenom ili neusklađenošću u potrebama pojedinca. Pored toga, veliki je problem predstavljala lokalna ograničenost i sam transport jer nije bilo jednostavno, niti praktično, veliku količinu stoke donijeti s jednog mjesta na drugo. Osim lokalne ograničenosti, količinska ograničenost koja je postavljala granice raspoloživosti pojedinih dobara, nije pomogla u osiguravanju dovoljne količine dobara da se zadovolje potrebe svih kupaca. Upravo su ove navedene karakteristike bile temelj za traženjem i osmišljavanjem jednostavnijeg i praktičnijeg načina trgovanja, a kao rješenje razvija se robni novac.

Robni novac

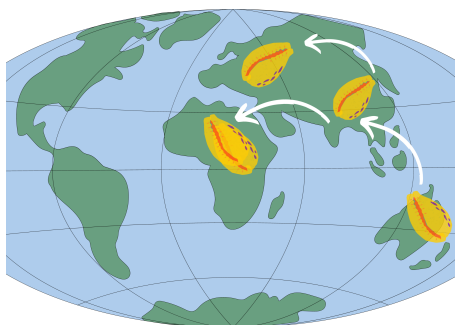
Razvoj ljudske civilizacije i otežano trgovanje direktnom razmjenom, potaklo je mnoge različite kulture na koncept da se određena roba koja ima intrinzičnu vrijednost i široku prihvaćenost koristi kao referenca za procjenu vrijednosti ostalih dobara i usluga tijekom trgovanja. Ovakva se ideja može smatrati prvotnom standardizacijom, ili barem iskazom želje za standardizacijom, određenih dobara sa svrhom lakšeg uspoređivanja vrijednosti i jednostavnijom trgovinom.

Neka od najznačajnijih dobara koja su se koristila kao referenca su sol, školjke i stoka. Sol je bila posebno važan oblik robnog novca jer je bio osnovni element u svakoj prehrani te je služila i kao konzervans hrane i omogućila njihovo sporije kvarenje. Stoka poput goveda, ovaca ili koza imale su stvarnu i opipljivu vrijednost u prehrani, proizvodnji tkanina ili poljoprivredi, a kao takvu su je ljudi cijenili zbog njene praktične uporabe.

Posebno su zanimljiva vrsta robnog novca bile školjke. Čovjek osim što treba zadovoljiti primarne potrebe, također želi zadovoljiti i estetskim potrebama, a ljuske školjki koje su krasile nakit, distribuiran čak i ljudima udaljenim od mora, ispunjavale su tu potrebu [2]. Jedna od najpoznatijih vrsta primitivnog novca bile su kauri školjke (*eng. cowrie shells*), školjke morskih puževa. Kauri školjke, zajedno s vrstama kao što su *cypraea moneta* i *cypraea annulus*, posjedovale su sve karakteristike očekivane od novca - bile su trajne, praktične i lako prepoznatljive. Gotovo su sve bile istih veličina i oblika, što je omogućavalo njihovo jednostavno prebrojavanje ili vaganje za utvrđivanje vrijednosti plaćanja.

Kauri školjke, pronađene uglavnom u toplim vodama Indijskog i Tihog oceana, putovale su preko mora i planina, postajući jedno od najčešće korištenih sredstava plaćanja

među trgovinskim nacijama Staroga svijeta. Kružile su širom Azije, Afrike, Oceanija, a čak i dijelovima Europe. Najstariji tragovi njihove upotrebe, pronađeni na brončanim predmetima pronađenim u Kini, datiraju iz 13. stoljeća pr. Kr. Neke su riječi u kineskom jeziku koje označavaju ekonomske pojmove poput *novca*, *srebra*, *kupnje* ili *vrijednosti*, koristile simbole školjki.



Slika 1.5: *Trgovina kauri školjkama*

Skupljanje i trgovina kauri školjkama razvijala se na Maldivima gotovo kao industrija. Žene su tkale mreže od lišća kokosa na koje su se male školjke pričvršćivale. Nakon sušenja na plaži, ostajale su samo školjke, spremne za daljnju upotrebu kao sredstvo plaćanja. Veći dio proizvodnje transportiran je lokalnim pomorcima do velikih distribucijskih centara, posebno u Bengal.

Načelo ponude i potražnje, ključno u ekonomiji, određivalo je vrijednost kauri školjki. U udaljenim regijama, daleko od proizvodnih centara ili trgovinskih središta, određena se vrsta stoke mogla kupiti za šaku školjki. Karavane arapskih trgovaca uvodile su ograničenu upotrebu kauri školjki u Africi. Nasuprot tome, europske su sile poput Portugala, Francuske, Engleske i Nizozemske iskoristile afričku privlačnost prema kauri školjkama kao idealno sredstvo plaćanja za trgovinu robljem, zlatom i drugim dobrima. Međutim, masovni unos kauri školjki na zapadnu obalu Afrike izazvao je poremećaje - 17. je stoljeće doživjelo nestašicu kauri školjki u Indiji, dok su lokalne valute u Africi pale u zaborav ili su jednostavno nestale.

Iako su se koristile sve do 20. stoljeća, sjećanje na ovo vrlo korišteno i rasprostranjeno sredstvo plaćanja živi kroz zbirke muzeja posvećenih novcu kao spomen njihovog značajnog utjecaja na sam razvoj numizmatike.³



Slika 1.6: *Kauri školjka*

³Znanost koja proučava novac u njegovim različitim oblicima i funkcijama.

Kovani novac

Kovani novac predstavlja bitan dio ljudske civilizacije i bitan korak u evoluciji novčanoga sustava. Na početku je bio uspostavljen sustav razmjene dobara, ali oko 5. ili 6. stoljeća pr. Kr., kao sredstvo plaćanja pojavljuje se novi oblik - kovanica, revolucionirajući ekonomske razmjene. Nastanak kovanica imao je za cilj riješiti izazove barter sustava u kojem bi osoba trebala zamijeniti bilo koju stavku ili uslugu kako bi dobila ono što želi. Glavni je problem ležao u činjenici da ako osoba nije imala ništa što druga osoba u krugu razmjene želi ili treba, razmjena se nije mogla obaviti. Ljudi su se s vremenom počeli specijalizirati u određenim zanimanjima te raditi i proizvoditi ono u čemu su bili vješti. Takva je specijalizacija bila udar na barter sustav jer su ljudi postali ovisni o drugima da proizvode i pružaju ono što sami ne mogu, prožimajući pitanje koliko uistinu vrijedi tuđi ili vlastiti rad. Upravo problem u nedostatku standardizacije, ali i problem u očuvanju bogatstva kada se trgovalo predmetima koji bi se mogli potrošiti u roku od nekoliko dana, društvo i kolektivna potreba društva stvorila je kovani novac.

Prvo područje u kojem je korišten kovani novac još je uvijek predmet rasprave [3]. Prema zapadnoj povijesti, prvi pronađeni novčići potječu s područja današnje Turske, nekadašnjeg Lidijskog Kraljevstva. Takvi novčići, otkriveni oko 700. pr. Kr., nisu zahtijevali kompleksne strojeve za njihovu izradu. Bili su prirodna kombinacija zlata i srebra, poznata kao elektum. Stanovnici su Lidijskog Kraljevstva urezivali dizajne na jednoj strani novčića, a drugu su stranu obilježili utorima kako bi dali na njihovoj jedinstvenosti. Ti su novčići bili vagani kako bi se odredila njihova vrijednost iz razloga što je bilo teško stvoriti konzistentan dizajn za sve kovanice. Osim toga, novčići su dolazili u različitim oblicima i veličinama jer su se koristili u svojem prirodnom stanju.



Slika 1.7: *Lidijski novčići [4]*

Oko istog vremena kao i stanovnici Lidijskog Kraljevstva, u drevnoj su Kini stvarani prvi poznati novčići. Nakon prestanka korištenja kauri školjki kao valuta, koristili su se komadi zlata s oznakama kineskih gradova, a nešto malo kasnije za valutu su uzeti i noževi različitih metala. Tek oko 220. godine pr. Kr. novčići su postali popularni u cijeloj zemlji. Većina tih kineskih novčića ima neku vrstu kvadratne ili kružne rupe, a razlog je bio olakšani transport vezanjem novčića za špagu ili konac.



Slika 1.8: *Kineska kovanica [5]*

Početkom 27. godine pr. Kr., Rimljani su razvili sustav gdje je vrijednost kovanica bila ono što je bilo navedeno na novčiću. Drugim riječima, vrijednost samog novčića više nije bila navedena u njegovoj masi. Važno je napomenuti da je upravo ovo bio važan korak za razvoj onoga što se koristi danas, a to je fiat novac (detaljnije u nastavku). Ovakav koncept omogućio je Rimljanima da kasnije devalviraju svoju valutu smanjenjem količine plemenitih metala u svakom novčiću. Naime, ako je, hipotetski, na novčiću navedena vrijednost od 2€, tada ljudi vjeruju da je njegova stvarna vrijednost upravo tih navedenih 2 €. Međutim, kada su Rimljani smanjili količinu plemenitih metala, odnosno ako je novčić prvotno bio napravljen od 90% zlata, a sada je od samo 25% zlata, na njemu i dalje piše da vrijedi isto - 2€. Razlika je što se takvom novčiću njegova stvarna vrijednost smanjuje jer je u samom njegovom sastavu manje plemenitih metala. Dakle, možda izvana jednaka nominalna vrijednost ne obećaje jednaku stvarnu vrijednost.



Slika 1.9: Rimska kovanica [6]

U antičko doba pa sve do 1550. godine, proces stvaranja novčića uključivao je udaranje komada metala između dva kalupa. Taj proces, poznat kao *kovani novac*, bio je spor proces koji je ponekad zahtijevao dvije osobe - jednu za udaranje, a drugu za držanje kalupa na mjestu. Kasnije su se koristile ploče metala od odgovarajućeg promjera kako bi se istovremeno stvorili višestruki novčići, a razlog je bio zadovoljenje rastuće potražnje za novčićima u poslovnim transakcijama. Međutim, takav proces u kojem se stvaraju više novčića odjednom, rezultirao je generičkim novčićima, što je kasnije olakšalo krivotvorenje. Naime, niti jedan od novčića nije bio točno onog promjera kojeg je trebao biti. Nadalje, novčići nisu bili savršeno okrugli, što je omogućilo odrezivanje rubova novčića od plemenitih metala. Prema tome bilo je potrebno pronaći sigurniji i bolji način stvaranja novčića, a taj se novi način nije pojavio sve do renesanse i industrijskog doba.

Jedan od boljih, alternativnih načina izrade novčića bilo je lijevanje novčića. Taj se proces temeljio na ulijevanju rastopljenog metala u unaprijed napravljeni kalup, a uglavnom se koristio u Aziji. Tijekom ovog procesa, iz jednog se kalupa moglo izraditi i do dvanaest novčića, za razliku od samo jednog novčića udarcem, tj. kovanjem. Osim toga, proizvedeni novčići bili su čišći, ravnomjernije i pravilnije oblikovani te su time otežali krivotvorenje, prijevaru i uklanjanje komadića plemenitih metala s novčića.

Tijekom industrijske revolucije, novčići s brušenim rubom postali su gotovo revolucionarni. Osnova ovog proces bio je stroj, odnosno novčići su se stvarali i izrađivali pomoću rada stroja. Poznato je da je za vrijeme industrijske revolucije izumljen Wattov parni stroj, a budući da je porast broja ljudi koji su odlazili raditi u tvornice povećao potrebu za novčićima, investitor po imenu Matthew Boulton iskoristio je izum parnog stroja kako bi napajao stroj za izradu novčića. Na kraju je to dovelo do ugovora o kovanju novčića za East India Company te do ugovora o opskrbi strojeva britanskoj kraljevskoj kovnici.

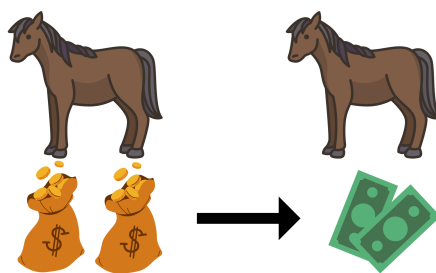
Kroz povijest, ljude je privlačio sjaj i ljepota novčića, a u modernome dobu nekolicina se ljudi bavi kolekcionarstvom kovanica. Osim što ljudi gledaju kovanice kao nešto što se može prikupljati i kao nešto što je sredstvo poslovanja i trgovanja, gledaju ih i kao sredstvo za ulaganje. Naime, u posljednjih su 150 godina dionice postale sve popularnije, a paralelno s njima je rasla koncepcija ulaganja u kovanice na temelju promatranja sadržaja plemenitih metala.

Mnoge kovanice koje se koriste u današnjem vremenu sadrže vrlo malo ili gotovo nimalo srebra ili zlata. Dobar primjer toga predstavlja Kennedy poludolar, prvi put izrađen 1964. godine kao počast nakon atentata na predsjednika Johna F. Keneddyja. Novčić je bio sastavljen od 90% srebra i 10% bakra. Već sljedeće je godine udio srebra smanjen na oko 40%. Konačno, sav je srebrni sadržaj uklonjen iz poludolara 1971. godine. To je samo jedan od primjera smanjenja sadržaja plemenitih metala u novčićima. Naime, vlasti su shvatile kako je sadržaj plemenitih metala postao vrijedniji od nominalne vrijednosti novčića, što je rezultiralo postupnim smanjivanjem udjela srebra ili zlata u mnogim drugim kovanicama koje su se koristile u svakodnevnoj upotrebi. Taj je proces odražavao spoznaju vlasti o nužnosti prilagodbe novčanih kovanica radi očuvanja njihove stabilnosti i funkcionalnosti u dinamičnom ekonomskom kontekstu.

Papirni novac

Papirni novac ima dugu povijest koja započinje s prvim korijenima u drevnoj Kini. Iako je papir prvi put izrađen u 7. stoljeću tijekom vladavine dinastije Tang (618. - 907.), prvi papirni novac nije zaživio sve do 11. stoljeća, a on je bio izumljen kao oblik depozita od trgovca tijekom dinastije Tang.

Jedan od ključnih razloga za nastanak papirnatog novca leži u potrebi za lakšom razmjenom bogatstva i jednostavnijom trgovinom. Metalni novčići napravljeni od zlata, srebra ili bakra, bili su iznimno teški za prijenos, posebno pri velikim transakcijama. Zbog toga su trgovci tražili alternativan način kako bi se olakšale transakcija i unaprijedila razmjena.



Slika 1.10: Prikaz jednostavnije razmjene papirnatim novcem

Zanimljivo je da su u to vrijeme mnogi trgovci počeli ostavljati svoje teške metalne novčiće na sigurnim mjestima u zamjenu za papirnatu potvrdu, *jiaozhi*, koje su predstavljale iznos depozita koji su ostavili. Takav način, nastao zbog potrebe za lakšom razmjenom bogatstva, polako je evoluirao. Kineska središnja vlada počela je proizvoditi vlastiti papirni novac, koristeći drvene matrice i više boja tinte, što je označilo značajan korak u razvoju papirnog novca.

Nakon revolucionarnih inovacija u Kini, Mongolsko Carstvo odigralo je ključnu ulogu u širenju i promicanju papirnog novca. Kublai Khan, unuk Džingis-kana, aktivno je poticao uporabu papirnog novca, uspostavljajući ga kao jedinu valutu u 13. stoljeću, što rezultira prekretnicom u širokoj uporabi papirnatog novca na području Kine.



Slika 1.11: *Jiaozi, prvi papirnat novac [7]*

Da bi papirni novac postao prihvaćen i praktičan, odvijale su se različite faze traženja optimalnog materijala ili standarda koji bi se mogao koristiti kao osnova za stvaranje papirnog novca. Tako su se isprobavale različite smjese papira, uključujući i one s dodatkom svile kako bi se poboljšala trajnost novčanica te određeni standardi (kao što je srebrni standard) kako bi se odredio način na koji bi se vrijednost novčanica mogla vezati za određenu količinu plemenitih metala.

Unatoč širokoj uporabi papirnatog novca u Aziji, njegov ulazak u Europu bio je izazovan zbog vjerskih i kulturnih predrasuda. U to se vrijeme u Europi promicala upotreba plemenitih metala kao oblik valute ili mjerila vrijednosti. Unatoč opisanim preprekama, putnici poput Marca Pola imali su ključnu ulogu u prenošenju koncepta papirnatog novca u Europu [8].

Za vrijeme 17. stoljeća, u Švedskoj su se pojavile prve papirnat novčanice, a već od idućeg su stoljeća postale prihvaćene i rasprostranjene diljem Europe, dok je u SAD-u papirni novac počeo kružiti tijekom Revolucionarnog rata. Za razliku od prvotnog kineskog papirnatog novca koji se temeljio na povjerenju, sada je svaka tiskana novčanica morala imati odgovarajuću količinu zlata u trezorima središnje banke kako bi bila podržana.



Slika 1.12: *Primjer prvog izdanog papirnog novca u Švedskoj, 1661. godine [9]*

1.1.4 Ostale rane valute

U prethodnom se potpoglavlju dao pregled najznačajnijih predstavnika prvih valuta i razvoj novca. Među njima, postoje još neke valute [10] koje su se koristile u ranim etapama povijesti te su također pridonijele značajnom utjecaju i razvoju financijskog sustava.

Zub kita

Zub kita, poznat kao *tambua*, predstavlja specifičan oblik valute s fidžijskih otoka. On nije samo služio kao sredstvo plaćanja, već je imao i simboličku vrijednost. Njegova je važnost bila evidentna u različitim sferama fidžijskog života, od ekonomije do rituala i ceremonija poput vjenčanja i dočeka posjetitelja, a to potvrđuje doček posjeta kraljice Elizabete i vojvode od Edinburgha 1982. godine. Također, bio je pokazatelj prestiža, moći i statusa unutar zajednica, stoga osobe koje su posjedovale zub kita obično su bile visoke poštovane i cijenjene u društvu. Njegova visoka tržišna vrijednost ležala je upravo u navedenim estetskim i kulturnim vrijednostima.

Kamena valuta Rai

Rai kamenje ili kamena valuta s Yap otoka, predstavlja oblik tradicionalnog novca koji se koristio u skupini od deset manjih otoka u središnjem Pacifiku. Spomenuta se valuta sastojala od golemih kamenih diskova izrađenih od vapnenca, poznatih kao *fei*. Ti su diskovi imali različite veličine s promjerom koji se kretao od nekoliko centimetara do nekoliko metara.

Jedinstvenost Rai kamenja nije bila samo u fizičkom izgledu i veličini, već i u načinu na koji su se koristili i njihovom značenju unutar zajednice. Iako su korišteni kao sredstvo plaćanja, njihova je važnost bila više simbolična i imala je duboke kulturne i društvene implikacije za stanovnike Yap otoka.

Proizvodnja Rai kamenja bila je izuzetno zahtjevna. Kamenje je ekstrahirano iz udaljenih kamenoloma, ponekad i stotinama kilometara daleko od otoka Yap. Diskovi su izvađeni ručno, a zbog svoje mase i veličine, transportirani su preko mora na posebnim plovilima. Važno je napomenuti da je jedna od karakteristika ove valute bila ta da diskovi nisu morali fizički mijenjati vlasnika; bilo je dovoljno znati samo u čijem je vlasništvu određeni disk.

Kao što je već napisano, vrijednost Rai kamenja nije bila samo materijalna, već je imala i simboličko značenje u ritualima, ceremonijama i društvenim događajima. Veći su diskovi uglavnom imali veću vrijednost, ali se zbog veličine nisu premještali s izvornog mjesta. Danas se opisani kameni diskovi koriste više kao značajan element povijesti i tradicije, ali oni i dalje nose svoju vrijednost u zajednici Yap otoka.

1.2 Zlatni standard - prethodnik fiat novcu

Zlatni standard finansijski je sustav u kojemu se vrijednost valute temelji na zlatu. Ovaj koncept datira još iz antičkih civilizacija i bio je važan element svjetskih ekonomija tijekom većeg dijela povijesti. Sustav se temelji na ideji da je novac *fiksiran* za određenu količinu zlata, što osigurava stabilnost valute.

Glavna prednost zlatnog standarda leži u tome što ograničava sposobnost vlade da tiskanjem novca nekontrolirano povećava opskrbu novcem, jer je količina valute ograničena količinom zlata koja se posjeduje. Upravo je to pružalo vjerodostojnost valuti i poticalo stabilnost cijena, sprječavajući hiperinflaciju⁴. Osim toga, zlatni standard poticao je

⁴Hiperinflacija je ekstremni oblik inflacije, tj. rapidnog i ekstremnog rasta općih cijena do te mjere da novac brzo gubi svoju vrijednost. U ovom scenariju, inflacija postaje izuzetno visoka, često prelazeći 50% mjesečno. To znači da cijene rastu toliko brzo da novac postaje gotovo bezvrijedan za kratko vrijeme.

međunarodnu trgovinu i stabilnost valuta diljem svijeta. Zemlje su mogle lakše međusobno trgovati jer je valuta imala fiksnu vrijednost prema zlatu, olakšavajući trgovinu bez straha od velikih valutnih fluktuacija.

Međutim, zlatni standard nije bio bez nedostataka. Ograničavanje opskrbe novcem ograničavalo je mogućnost vlade da reagira na gospodarke krize. Također, ako bi došlo do naglog rasta proizvodnje zlata ili otkrića novih nalazišta, to bi moglo dovesti do deflacije.⁵

Zlatni je standard bio široko rasprostranjen i prihvaćen tijekom 19. i početkom 20. stoljeća. No, nakon Prvog svjetskog rata i posebno nakon Velike depresije 1930-ih, mnoge su zemlje odustale od zlatnog standarda zbog potrebe za fleksibilnijim financijskim sustavom koji bi omogućio veću kontrolu nad monetarnom politikom. Nakon Drugog svjetskog rata, Bretton Woods sporazum uspostavio je vezu valuta s dolarom koji je bio fiksiran za zlato, ali se sustav raspao 1971. godine kada je SAD napustio vezu dolara i zlata.

Iako zlatni standard danas nije široko prihvaćen u globalnim ekonomijama, njegovo naslijeđe ostavlja dubok trag u formiranju monetarne politike i procjeni vrijednosti valuta u odnosu na druge. Ovaj koncept je ostavio temelje za moderne financijske sustave, potičući istraživanje i razvoj alternativnih načina upravljanja novcem, uključujući koncepte kao što su fiat novac i monetarna politika centralnih banaka. Bez obzira na to što više nije prakticiran izravno, zlatni standard i dalje služi kao ključna točka referentne vrijednosti i duboko je ukorijenjen u povijesti financija i ekonomije.

1.3 Fiat novac

Fiat novac oblik je valute koju podržava samo vlastita deklaracija vladajućeg tijela ili vlade, a ne materijalna imovina poput zlata ili srebra. Njegova vrijednost dolazi iz povjerenja javnosti u vladu i ekonomski sustav, a ne iz intrinzične vrijednosti kao što je bio slučaj kod novca koji se temeljio na plemenitim metalima. Većina današnjih papirnatih novčanica poput eura, dolara, funte i sličnih, spadaju u fiat valute.

Riječ *fiat* latinska je riječ koja nosi prevedeno značenje *neka bude*, naglašavajući time funkcionalnost ovakvog sustava - neka određena valuta bude određene vrijednosti jer ju je država tako deklarirala. Sam koncept fiat novca ima dugu povijest. U prošlosti, novac je bio materijalno podržan vrijednim metalima, no s vremenom su se javile potrebe za fleksibilnijim oblikom valute koji bi se mogao proizvoditi lakše, ekonomičnije i koji bi olakšavao trgovinu i izvršavanje većih transakcija.

Ključan trenutak u razvoju fiat novca bio je napuštanje zlatnog standarda tijekom 20. stoljeća. Kao što je već objašnjeno, zlatni je standard bio sustav u kojem je svaka valuta bila fiksirana za određenu količinu zlata, što je ograničavalo količinu novca koju je vlada mogla izdati.

Ratne posljedice i gospodarske krize rezultirale su zahtijevanjem mnogih zemalja na veću slobodu tiskanja novca i podupiranje ekonomije, a s vremenom su gotovo sve zemlje prešle na sustav fiat novca. Taj prelazak omogućio im je fleksibilniju monetarnu politiku i olakšao prilagodbe na promjene u ekonomiji kao i na prilagodbe posljedicama svjetskih katastrofa.

⁵Deflacija je opći pad razine cijena dobara i usluga unutar ekonomije. Suprotno inflaciji, koja označava rast cijena kao rezultat smanjenja potražnje za proizvodima i uslugama, pada novčane opskrbe ili smanjenja agregatne potrošnje unutar gospodarstva.

Fiat novac funkcionira na osnovi povjerenja u emitenta - u većini je slučajeva to centralna banka ili država, a takvo održavanje povjerenja ključno je za stabilnost i vrijednost fiat novca. Naime, vlade imaju kontrolu nad količinom novca u opticaju te mogu upravljati kamatnim stopama i drugim instrumentima monetarne politike kako bi regulirale gospodarstvo.

Iako fiat novac pruža fleksibilnost i prilagođenost, postavlja određene izazove. Prekomjerno tiskanje novca dovodi do inflacije, što može negativno utjecati na kupovnu moć građana. Također, povjerenje javnosti u valutu može varirati, ovisno o stabilnosti vlade i ekonomskoj politici.

Važno je napomenuti da prosječni vijek trajanja fiat valuta može varirati ovisno o mnogim čimbenicima. Njihov vijek trajanja nije univerzalno određen jer ovisi o političkim, ekonomskim i društvenim uvjetima zemlje koja emitira tu valutu, kao i o globalnim financijskim promjenama.

Neke fiat valute imaju relativno dugi vijek trajanja, poput američkog dolara, eura ili britanske funte. Međutim, postoje primjeri valuta koje su imale, za razliku od prethodno spomenutih, znatno kraći vijek trajanja zbog političkih nestabilnosti, hiperinflacije ili drugih ekonomskih problema. Takvi su primjeri valuta:

1. Njemačka marka (1923.) - nakon Prvog svjetskog rata, Njemačka je doživjela enormnu hiperinflaciju te kao posljedica tome, njemačka je marka postala bezvrijedna, što je dovelo do velikog gubitka povjerenja u tu valutu
2. Zimbabveanski dolar (2008.) - Zimbabve je doživio nezapamćenu hiperinflaciju, zbog čega je zimbabveanski dolar izgubio svoju vrijednost. Bilježene su velike denominacije novčanica, ali su one postale beskorisne i bezvrijedne za svakodnevnu upotrebu
3. Mađarski pengő (1946.) - Mađarska je nakon Drugog svjetskog rata doživjela veliku inflaciju, stoga je tada trenutna valuta pengő izgubila u potpunosti na svojoj vrijednosti
4. Talijanski liru (2002.) - iako nije bilo gospodarske krize ili hiperinflacije, Italija je odlučila uvesti euro kao službenu valutu zamjenjujući tadašnju valutu lira

U prosjeku, vijek trajanja fiat valuta može iti nekoliko desetljeća, ali to je samo općenita procjena. Mnogi drugi faktori mogu znatno utjecati na trajanje valute, a u nekim slučajevima, države su izdale druge valute ili prešle na drugi monetarni sustav kako bi riješile ekonomske probleme ili promijenile političke prilike.

Unatoč navedenim izazovima, fiat je novac postao dominantan oblik valute u modernim gospodarstvima širom svijeta, a njegova važnost leži u fleksibilnosti koju pruža vladama, omogućujući im reagiranje na dinamične ekonomske uvjete i potrebe gospodarstva.

1.3.1 Razlika između novca i valute

Novac je općeniti pojam koji obuhvaća sve oblike imovine ili sredstava koja se koriste kao sredstvo razmjene, mjeru vrijednosti i pohranu bogatstva. S druge je strane valuta specifičan oblik novca koji je zakonsko sredstvo plaćanja unutar određene države ili ekonomske regije. Osim toga, valuta je primarno sredstvo razmjene u modernome svijetu, zamijenivši davnu barter trgovinu kao način trgovanja pojedinim dobrima i uslugama.

Termini *novac* i *valuta* često se smatraju istim. Međutim, iako su povezani, imaju bitno različita značenja. Novac, u svojoj suštini, predstavlja apstraktnu vrijednost koja se može izraziti samo numerički. To je sustav vrijednosti koji omogućuje razmjenu dobara i usluga,

ali sam po sebi nije opipljiv. Čekovi, elektronička transakcija - sve su to oblici novca koji postoje kao zapis brojeva. S druge strane, valuta je fizički prisutna i opipljiva. Ona je ono što se osjeti prilikom izvršenja plaćanja, a to su novčanice i kovanice koje se drže u rukama prilikom svakodnevnih transakcija. Iako valuta također predstavlja numeričku vrijednost, razlika je u njenom opipljivosti i materijalnoj prisutnosti.

Za stvaranje dovoljne količine valute, potrebno ju je tiskati, a to je u nadležnosti vlade. S druge strane, novac kao apstraktna vrijednost, ne zahtijeva takav proces. Primjerice, prilikom online kupovine, transakcija se odvija preko banke pri čemu se brojevi samo prebacuju s vašeg računa na račun trgovca. Prema tome, novac je lako zamjenjiv za robu ili usluge jer se temelji na sustavu vrijednosti, dok valuta, iako također lako razmjnjiva, zahtijeva fizičku razmjenu. Kada se potroši, potrebno je posjetiti banku i podići određenu vrijednost novčanica.

U konačnici, valuta je svakodnevna pratnja u transakcijama, ali novac ostaje univerzalni jezik vrijednosti. Dok valuta zauzima svoje mjesto u fizičkom obliku razmjene, novac prožima svaki kutak svijeta, izražavajući se kroz različite oblike i kontekste. Dok su vlade nekad podržavale valutu zlatom i srebrom, novac danas često ima svoju vrijednost utemeljenu na povjerenju i povijesti financijskih tržišta. U konačnici, njihova suptilna, ali bitna razlika, prožima svakodnevne interakcije s financijama i tržištima, oblikujući način na koji se percipira i koristi sredstvo plaćanja u svijetu oko nas.

Tablica 1.1: Razlika između novca i valute

Novac	Valuta
Može biti spremište vrijednosti i u svojoj je prirodi nematerijalan	Ne može biti spremište vrijednosti, iako je opipljiva, vidljiva i materijalna
Odnosi se na stvarnu vrijednost roba ili usluga koje se trguju	Sredstvo koje se prenosi kako bi se povećala kupovna moć i obavlja se svakodnevne transakcije
Ima intrinzičnu vrijednost	Nema intrinzičnu vrijednost
Vrijednost bilo koje robe ili usluge može se izraziti u obliku novca i može se navesti u određenoj valuti.	Vrijednost bilo koje robe ili usluge ne može se izvesti pomoću određene valute jer je ona samo sredstvo razmjene, a ne mjerilo vrijednosti.
Može obavljati različite funkcije i ima svoj značaj u bilo kojoj ekonomiji.	Bilo koji oblik novca koji se koristi u javnosti.

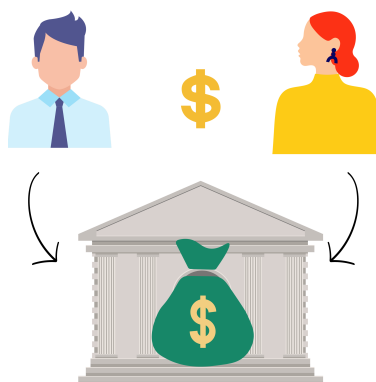
1.4 Razvoj monetarnih sustava

Razvoj monetarnih sustava prati ljudsku civilizaciju od njezinih najranijih faza. U početku, ljudi su se oslanjali na razmjenu dobara kako bi zadovoljili svoje potrebe - roba poput školjki, soli, stoke ili žitarica bile su običan oblik razmjene. S razvojem trgovine, počela su se koristiti različita sredstva kako bi se određena razmjena mogla izvršiti.

Prvi korak prema razvoju monetarnih sustava dogodio se kroz kovanje kovanica od plemenitih metala. Takve su kovanice imale intrinzičnu vrijednost, postajući prvi oblik

novca. Kasnije, pojava papirnato novca predstavila je drukčiji oblik novčanog prometa - papirnatu su novčanice zamijenile metalne kovanice, predstavljajući obećanje da su podržani određenom količinom plemenitih metala u trezoru centralne banke.

Razvoj monetarnih sustava nije samo bio pitanje uvođenja novih oblika novca, već i razvoja institucija koje upravljaju tim novčanim sustavima. Stvaranje centralnih banaka bio je ključan korak u organiziranju financijskih sustava iz razloga što te institucije kontroliraju emisiju novca, nadziru kamatne stope i djeluju kao regulatori financijskih tržišta.



Slika 1.13: *Monetarni sustav*

Dugoročna stabilnost cijena već je dugi niz godina glavni cilj monetarne politike. Naime, niska i stabilna inflacija olakšava svakodnevna osobna financijska pitanja te omogućava učinkovito funkcioniranje gospodarstva. Važno je napomenuti da ovakav koncept nije dovoljan, a to su i pokazale gospodarske krize. Opasne financijske neravnoteže mogu nastati i ispod prividno mirne površine niske i stabilne inflacije. Tradicionalna prudenijalna politika, koja se uglavnom fokusirala na stabilnost pojedinačnih banaka, pokazala se nedostatnom u suočavanju s vrstom sistematskih rizika koji su doveli do određenih gospodarskih i svjetskih kriza.

Nije novost da monetarna politika sa sobom nosi niz nedostataka koji mogu ograničiti njezinu učinkovitost i mogućnost prilagodbe brzim promjenama u ekonomskom okruženju. Jedan je od takvih glavnih nedostataka zakašnjela reakcija sustava. Odluke o promjeni kamatnih stopa ili prilagodbi novčane opskrbe mogu zahtijevati vrijeme, a ekonomija se može mijenjati brže od brzine prilagodbe monetarne politike, što može rezultirati suboptimalnim odgovorom na ekonomske promjene.

Također, efikasnost monetarne politike nije uvijek zajamčena. Promjene u kamatnim stopama ili novčanoj opskrbi ne moraju uvijek rezultirati očekivanim rezultatima. Gospodarstvo može reagirati na način koji nisu predviđeni ili se suočiti s ograničenjima u postizanju željenih ciljeva, a osim toga donošenje takvih promjena utječe na socioekonomsku nejednakost.

Upravo zbog toga, makroekonomska politika treba posvetiti veću pažnju financijskoj stabilnosti. Međutim, kamatna stopa često će biti grub i skup podsjetnik za suočavanje s financijskim neravnotežama. Bi li se trebalo dovesti u pitanje poslova dva milijuna ljudi jer su banke preopterećene ili cijene nekretnina prebrzo rastu? Umjesto toga, prva linija obrane trebale bi biti strategije koje mogu ciljati financijsku stabilnost na izravniji i učinkovitiji način, uključujući makroprudencijalne alate poput ograničenja omjera kreditiranja i zaduženosti te mjere upravljanja kapitalnim tokovima. Prema svemu navedenome,

moderni monetarni sustavi uključuju kompleksne strukture. Monetarna politika obuhvaća kontrolu kamatnih stopa, regulaciju količine novca u opticaju, intervencije na tržištima i druge mjere kako bi se postigli ciljevi stabilnosti i rasta u gospodarstvu. Ako se promatra u suvremenome kontekstu, tada monetarni sustavi i politika variraju od zemlje do zemlje, prilagođavajući se specifičnostima njihovih ekonomija i ciljevima koje žele postići. Razvoj monetarnih sustava odražava se na svakodnevni život, oblikuje gospodarske uvjete i ima dubok utjecaj na društvo u cjelini.

1.5 Elektronički novac

Elektronički je novac proizašao iz potrebe za efikasnijim, fleksibilnijim i sigurnijim načinima obavljanja financijskih transakcija. Njegova se povijest proteže kroz inovacije, tehnološki napredak i evoluciju financijskih sustava tijekom različitih vremenskih razdoblja. Početkom 20. stoljeća, ljudi su svjedočili prvim koracima prema razvoju elektroničkog novca, a ključnu su ulogu u tom procesu odigrali kreditne i debitne kartice.

Diners Club, pionir kreditnih kartica, osnovan je 1950-ih godina te je prva tvrtka koja je omogućila korištenje kreditnih kartica za kupnju. Ideja je bila revolucionarna jer umjesto nošenja gotovine, ljudi su sada mogli plaćati pomoću male, plastične kartice koja je bila lakša, praktičnija i jednostavnija za obavljanje transakcija. Korisnici su mogli tako obavljati kupnje u određenim trgovinama i restoranima, stvarajući i sudjelujući u prvim koracima razvoja elektroničkog novca.



Slika 1.14: *Diners Club kreditna kartica [11]*

Kao reakcija na uspjeh kreditnih kartica, debitne su kartice započele svoj razvojni put. Kreditne su kartice omogućile potrošačima jednostavan pristup sredstvima koja nisu uvijek bila trenutno dostupna na njihovim bankovnim računima. Međutim, debitne su kartice napravile presudnu razliku, a to je da umjesto posuđivanja sredstava od banke, korisnici su mogli direktno koristiti novac koji su već posjedovali.

Debitne kartice funkcioniraju kao elektronička alternativa čekovima ili gotovini. Kada korisnik koristi debitnu karticu za plaćanje, iznos transakcije odmah se odbija iz povezanog bankovnog računa. Ova izravna povezanost eliminira potrebu za zaduživanjem ili korištenjem kredita za transakcije.

Prema opisanome, debitne su se kartice rapidno proširile zbog svoje praktičnosti i jednostavnosti korištenja. Banke su počele izdavati ove kartice svojim klijentima kao standardnu opciju zajedno s bankovnim računima. Navedeno je stvorilo široku bazu korisnika koji su uvidjeli prednosti debitnih kartica u odnosu na tradicionalne načine plaćanja.

Pojava i razvoj debitnih kartica značajno je utjecala na način na koji ljudi upravljaju svojim financijama. Postale su uobičajen način plaćanja u svakodnevnim transakcijama,

uključujući kupnju namirnica, plaćanje računa ili obavljanje transakcija na bankovnom računu. Takva prilagođenost i jednostavnost korištenja značajno su promijenile navike potrošača.

Nakon debitnih kartica, razvojni put nastavljaju e-trgovine i internet bankarstvo, a njihov je uspon iz temelja promijenio način na koji ljudi obavljaju financijske transakcije. Pojava interneta tijekom 1990-ih donijela je revolucionarne promjene u financijskom svijetu, stvarajući novu eru u kojoj su e-trgovina i internet bankarstvo postali vodeći oblici digitalnih transakcija.

E-trgovina, kao središnji dio online poslovanja, omogućila je kupcima da obavljaju kupnju i prodaju proizvode ili usluge putem interneta. Ovaj koncept omogućuje pristup trgovini iz udobnosti vlastita doma ili putem mobilnih uređaja, omogućujući korisnicima još jednostavnije i lakše obavljanje transakcija. Uz e-trgovinu, internet je bankarstvo postalo ključno. Banke su osmislile online platforme koje korisnicima omogućuju upravljanje svojim financijama putem interneta, a osim toga omogućen im je i pristup njihovim bankovnim računima, prijenos novca, plaćanje računa i druge financijske transakcije putem interneta, eliminirajući potrebu za posjedovanjem gotovine, svakodnevnim odlaskom u trgovine i slično.

Opisana digitalna revolucija promijenila je način na koji ljudi percipiraju i koriste novac. Postala je uobičajena praksa koristiti internetsko bankarstvo za upravljanje financijama, što je rezultiralo smanjenjem fizičkih posjeta bankama. Također, proširila je mogućnost plaćanja i omogućila pristup globalnom tržištu putem mobilnog uređaja i vlastitog doma, eliminirajući potrebu za fizičkim posjedovanjem nekakve druge valute u nekom od tržišta s drukčijom monetarnom politikom.

Razvoj e-trgovine i internetskog bankarstva također je potaknuo inovacije u sigurnosnim tehnologijama. Sve veća briga za sigurnost podataka i privatnost potaknula je razvoj sofisticiranih sustava enkripcije, autentifikacije korisnika i drugih protokola kako bi se osigurala sigurnost financijskih transakcija putem interneta.

Pored toga, početak 21. stoljeća obilježila je mobilna revolucija. Razvoj pametnih telefona i mobilnih aplikacija sa sobom su donijeli još jednu revoluciju u načinu na koji se obavljaju financijske transakcije.

Tehnologija NFC (Near Field Communication) bila je ključna u promjeni načina plaćanja. Omogućila je beskontaktna plaćanja što je transformiralo iskustvo kupovine. NFC čipovi u pametnim telefonima omogućavaju korisnicima da jednostavnim prislonjavanjem uređaja na terminal obave transakciju, što je proces plaćanja učinilo bržim i praktičnijim.

S porastom mobilnih plaćanja i aplikacija, povećala se važnost sigurnosti i zaštite privatnosti podataka korisnika. Razvoj sigurnosnih protokola poput biometrijskog skeniranja, dvofaktornog autentificiranja i enkripcije postao je neophodan kako bi se osigurala sigurnost financijskih transakcija ne samo putem mobilnih uređaja, nego u bilo kojem digitalnom obliku.

Nastavak razvoja mobilnih tehnologija i integracije novih tehnoloških inovacija, poput blockchain tehnologije i proširenja NFC funkcionalnosti, predstavljat će ključne smjerove budućnosti mobilnih financijskih transakcija, ali i samih digitalnih transakcija. Sve veći broj ljudi oslanjat će se na mobilne uređaje za upravljanje svojim financijama, a mobilni sektor će i dalje biti pod snažnim pritiskom da osigura sigurnost i pouzdanost u tom rastućem digitalnom ekosustavu.

1.6 Digitalni novac - nastanak kriptovaluta

Prije pojave kriptovaluta, svjetska financijska infrastruktura oslanjala se na centralizirane institucije poput banaka i vlada. Međutim, ovi sustavi su pokazali nekoliko nedostataka koji su potaknuli potrebu za alternativnim rješenjem:

1. Centralizacija i kontrola - tradicionalni financijski sustavi podložni su centralizaciji i kontroli od strane institucija kao što su banke ili vlade. Ovo je rezultiralo situacijama gdje su te institucije imale apsolutnu kontrolu nad novcem, što je stvorilo neravnotežu moći i povjerenja.
2. Visoki troškovi transakcija - bankovni sustavi često su povezani s visokim troškovima transakcija, posebno kod međunarodnih prijenosa novca. Ovi troškovi mogu biti značajni, posebno za manje transakcije ili za ljude koji žive u zemljama s visokim naknadama.
3. Spori transferi i ograničenja - klasični sustavi za prijenos novca često su spori, posebno kada je riječ o međunarodnim transakcijama koje zahtijevaju niz posrednika i provjera. Osim toga, ovisnost o radnoj satnici banaka znači da su neke transakcije ograničene na radno vrijeme.
4. Sigurnosni rizici i privatnost - centralizirani sustavi, zbog toga što veliki broj korisnika ovisi o njima kao jednom, centralnom tijelu, podložni su cyber napadima, što može dovesti do gubitka podataka i krađe identiteta. Također, mnogi korisnici osjećaju da su njihovi financijski podaci nedovoljno zaštićeni i da gube kontrolu nad vlastitom privatnošću.

S obzirom na ove izazove, potreba za alternativnim sustavom koji bi omogućio decentraliziranu, sigurnu, jeftinu i brzu razmjenu vrijednosti postala je sve izraženija. Kriptovalute su nastale kao odgovor na ove nedostatke, koristeći tehnologiju blockchaina kako bi pružile rješenje koje se oslanja na decentralizaciju, transparentnost, sigurnost i brzinu.

Kriptovalute su digitalni oblik valute koji se koristi kao sredstvo razmjene putem kriptografskih protokola za osiguranje transakcija i kontrolu stvaranja dodatnih jedinica. Njihov nastanak datira iz kasnog 20. stoljeća, ali je pravi procvat doživio s pojavom Bitcoina.

Sama ideja kriptovaluta temelji se na konceptu decentraliziranog sustava. U najjednostavnijem smislu, to znači da kriptovalute ne ovise o jednoj centralnoj instituciji poput banke ili vlade. Umjesto toga, koriste tehnologiju zvanu blockchain za evidentiranje transakcija.

Bitcoin je prva kriptovaluta i stvorio ju je (ili grupa ljudi pod pseudonimom) Satoshi Nakamoto 2009. godine. Nakamoto je predstavio Bitcoin kao odgovor na nedostatke tradicionalnih valuta koje su podložne centraliziranom nadzoru i manipulaciji.

Nakon pojave Bitcoina, mnoge druge kriptovalute su se razvile, svaka s vlastitim jedinstvenim karakteristikama i svrhom. Ethereum je jedan od najpoznatijih primjera, a on, osim što omogućuje transfer vrijednosti poput Bitcoina, Ethereum podržava i *pametne ugovore*, što je omogućilo razvoj decentraliziranih aplikacija (dApps).

1.7 Razvoj Bitcoina i Kriptovaluta

Bitcoin je započeo kao konceptualni bijeli papir nepoznatog pravog autorstva. Glavni razlog stvaranja ove ideje je kreiranje decentralizirane valute koja ne ovisi o centralnim autoritetima, a sama ideja kao takva temeljila se na implementaciji tehnologije blockchaina koja bi omogućila transparentnost i sigurnost transakcija.

Prije pojave Bitcoina, nekoliko je digitalnih valuta pokušalo zaplirati financijskim tržištima, poput B-Money i Bit Gold. No, 31. listopada 2008., sve se mijenja s objavljivanjem znanstvenog rada pod naslovom *Bitcoin: A Peer-to-Peer Electronic Cash System* od strane osobe ili grupe pod pseudonimom Satoshi Nakamoto. Ovaj rad, poznat kao Bijela knjiga, opisuje Bitcoin kao teoretski digitalni resurs otvorenog koda, stvarajući koncept valute koju nitko ne posjeduje, ali svatko može koristiti i razvijati.

U početku 2009., Bitcoin softver postaje javno dostupan, a Satoshi Nakamoto rudari prve bitcoine, pokrećući praksu krypto rudarenja. Mali tim programera i entuzijasta aktivno sudjeluje u razvoju, nesvjesni da sudjeluju u revolucionarnoj tehnologiji.

Godina 2010. obilježena je prvim široko prihvaćenim transakcijama kriptovalutama. Laszlo Hanyecz kupuje dvije pizze za 10 000 bitcoina, transakcija koja bi danas bila vrijedna stotine milijuna dolara. Krajem iste godine, Satoshi Nakamoto se povlači iz javnosti, ostavljajući iza sebe posljednju poruku na forumu bitcointalk. U to vrijeme, prva online trgovina prihvaća Bitcoin, dok Silk Road postaje kontroverzno kriminalno tržište.

Godina 2011. označava trenutak kada je Bitcoin dostigao jednakost s dolarom. No, iste godine, Mt. Gox, jedna od najvećih bitcoin mjenjačnica, biva hakirana, rezultirajući krađom 2 000 bitcoina. Krajem 2012., ukupna vrijednost bitcoina prelazi milijardu dolara.

Siječanj 2014. označava masivni hakirani Mt. Gox, gdje je ukradeno 850 000 bitcoina. Iako ostaje najveća krađa u povijesti kriptovaluta, krivci nisu pronađeni. Kasnije iste godine, osnivač Silk Road-a osuđen je na doživotni zatvor zbog ilegalne prodaje droge na web stranici koja je koristila Bitcoin za anonimne transakcije.

Godine 2016., Bitcoin kreće u rast koji je doveo do tzv. Bull tržišta. Uspon cijene kulminira početkom 2018., kada Bitcoin doseže rekordnu vrijednost od 20 000 USD. No, cijene su brzo pale, dosegovši najnižu točku na 3 250 USD.

Ovi ključni događaji označili su put Bitcoina od skromnih početaka do svjetske pozornosti i prihvaćanja unutar financijskog pejzaža. Njegova priča je bila putovanje puno uzbuđenja, od prvih transakcija i prvih prihvaćanja do suočavanja s izazovima poput hakiranja mjenjačnica i korištenja u ilegalnim aktivnostima.

Iako je prošao kroz brojne visove i padove u cijenama te je bio dio kontroverzi, Bitcoin je postao simbol novih tehnoloških mogućnosti, decentraliziranosti i promjene u percepciji novca. Njegova evolucija nastavlja se kako se prilagođava regulacijama, tehnološkim inovacijama i sve većem interesu investitora.

Također, Bitcoin često se promatra kao temelj za razvoj krypto industrije koja je postala mnogo više od alternative tradicionalnim valutama. Njegova vrijednost i značaj kao sredstva plaćanja nastavlja inspirirati istraživanje, razvoj i prihvaćanje kriptovaluta širom svijeta. S vremenom, Bitcoin se uspinje i pada, ali ostaje ključni akter u razgovorima o budućnosti financijskog sustava.

1.7.1 Kriptovalute pored Bitcoina

Bitcoin je zauzeo centralno mjesto u svijetu kriptovaluta, ali paralelno s njim, pojavilo se nekoliko drugih značajnih digitalnih valuta, svaka sa svojim jedinstvenim karakteristikama i ciljevima.

Ethereum (ETH)

Osnovan 2015. godine od strane Vitalika Buterina, Ethereum se izdvaja po konceptu platforme za izradu pametnih ugovora i decentraliziranih aplikacija. Osim osnovne funkcije prijenosa vrijednosti, Ethereumov blockchain omogućuje programerima stvaranje složenih aplikacija unutar svoje mreže, koristeći Ether kao gorivo za transakcije.

Ripple (XRP)

Ripple, stvoren 2012. godine od strane Ripple Labs-a, usmjeren je na unaprjeđenje međunarodnih bankarskih transakcija. Kroz svoju kriptovalutu XRP, Ripple se koristi kao sredstvo za brze i jeftine novčane transakcije između financijskih institucija, čime se nastoji smanjiti vrijeme i troškovi transakcija.

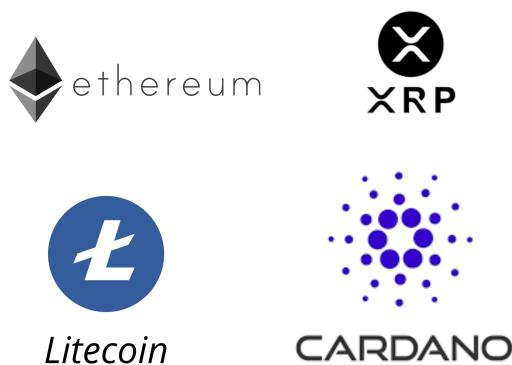
Litecoin (LTC)

Charlie Lee je 2011. godine kreirao Litecoin, kriptovalutu koja dijeli sličnosti s Bitcoinom, ali se fokusira na brža vremena potvrde transakcija i poboljšanu skalabilnost. Litecoin se često smatra *srebrnim* Bitcoinom zbog svojih sličnosti, ali i dodatnih značajki.

Cardano (ADA)

Cardano, stvoren 2017. godine, ističe se svojim fokusom na sigurnost, skalabilnost i održivost. Koristi matematičke dokaze o posjedu (Proof of Stake) za izvršavanje transakcija unutar mreže, što se smatra efikasnijim od Proof of Work sustava (PoW), čime se želi osigurati stabilnost i održivost kripto platforme.

Svaka od ovih kriptovaluta donosi svoje jedinstvene karakteristike i pristupe težnjama kriptoindustrije, pružajući alternativne opcije i rješenja izvan Bitcoinovog dominantnog položaja u svijetu digitalnih valuta.



Slika 1.15: *Primjeri kriptovaluta*



Drugi dio

2 Tehnologije iza kriptovaluta . . 33

- 2.1 Razvoj interneta
- 2.2 Bitcoin
- 2.3 Model ravnopravnih partnera (*Peer to peer mreža*)
- 2.4 Decentralizacija
- 2.5 Tehnologije koje su dovele do razvoja Bitcoin kriptovalute
- 2.6 Kriptografija
- 2.7 Digitalni potpis
- 2.8 Tehnologija ulančanih blokova (*eng. Blockchain*)



2. Tehnologije iza kriptovaluta

Trenutno se svijet nalazi u trećem razvojnem razdoblju interneta koje je započelo 1991. godine, nakon što je internet korišten isključivo u vojnim i akademskim krugovima te se danas primjenjuje u svakodnevnom životu. Osim što se internet koristi u komunikaciji, obrazovanju, medicini, industriji i dr., s vremenom se počeo koristiti i u transakcijske svrhe. Najprije naravno s fiat valutama, a onda i s kriptovalutama, odnosno Bitcoinom. Bitcoin kao prva decentralizirana i digitalna valuta zapravo koristi tehnologiju ulančanih blokova (*eng. blockchain*), a sama tehnologija ima četiri ključna stupa – decentralizacija, nepromjenjivost, transparentnost i sigurnost. Decentralizacija blockchaina predstavlja strukturu u kojoj ne postoji središnje tijelo koje bi upravljalo transakcijama; nepromjenjivost se sastoji u tome da nakon dodavanja bloka u lanac ne može doći do izmjene istog; transparentnost predstavlja javnu dostupnost transakcija i podataka, kao i evidenciju i povijest svih blokova, u svakom trenutku i naposljetku, sigurnost koja se krije u samome dizajnu – otvoren i decentraliziran sustav ne zahtijeva dodatnu zaštitu podataka. Ovdje je važno spomenuti i kako se blockchain temelji na P2P (*engl. Peer to Peer*) mreži, gdje je svako sudjelujuće računalo ravnopravni partner te čini čvor (*eng. Node*) u mreži ulančanih blokova. Upravo ovakva struktura osigurava da svaki čvor istovremeno bude davatelj i korisnik, sa zajedničkim pristupom dostupnim podacima bez potrebe za ranije spomenutim centralnim serverom.

U priručniku će, uz sve navedeno, biti objašnjene i ideje koje su prethodile, i na temelju kojih je nastala kriptovaluta Bitcoin, a razvijene su u poljima kriptografije, konsenzusnih protokola i P2P mreže. Ideje koje će biti obrađene su: Kriptografija s javnim ključem ili asimetrična kriptografija, Merkle stablo, Vremenska oznaka, Pametni ugovori, Dokaz radom i naposljetku, Secure Hash Algorithm 2 (SHA-2).

2.1 Razvoj interneta

Povijesni razvoj Interneta u izravnoj je vezi s povijesnim razvojem računala koji je započeo tijekom 17. stoljeća, kada je prvi puta korištena i riječ „računar“, tada označavajući osobu koja je iznimno nadarena za aritmetiku i računanje. Sredinom 20. stoljeća su električna energija, vojni zahtjevi i ciljevi Drugog svjetskog rata doprinijeli razvoju elektromehaničkih računala, nakon čega je uslijedila računalna revolucija u 6 razdoblja, sve do razvoja računala kakvima se danas koristimo. Tako je primjerice četvrto razdoblje obilježila tehnologija mikroprocesora, stvarajući mogućnost proizvodnje osobnih računala, dok se posljednja dva razdoblja odnose na platformu koja je osmišljena kao osnova za razvoj umjetne inteligencije.

Internet istovremeno predstavlja globalnu sposobnost komunikacije, mehanizam za širenje informacija te sredstvo suradnje i interakcije između pojedinaca i njihovih računala, neovisno o njihovoj geografskoj lokaciji. Internet je moguće definirati kao „digitalizirano i suvremeno informacijsko-komunikacijsko sredstvo i digitaliziran medij koji djeluje na principu mrežnog povezivanja i nelinearnog kretanja prema sadržajima na mreži.“

Povijest Interneta moguće je podijeliti u tri razvojna razdoblja:

1. 1961.-1985., razvoj kao tajna, vojna tehnologija
2. 1985.-1991., razvoj u akademskim krugovima
3. 1991.-prema danas, razvoj kao popularna i komercijalna tehnologija, sveprisutna u svakodnevnom životu

Prije nastanka interneta kakvog danas poznajemo, znanstvenici i inženjeri razmišljali su o, i nastojali stvoriti globalne komunikacijske mreže. Koncept takve prve mreže formuliran je prvi puta 1962. godine od strane američkog znanstvenika J. C. R. Licklidera, koji je predložio ideju „Galaktičkog interkonekcijskog računalnog mrežnog sustava“, odnosno Galaktičke mreže. Vizionarski je zamislio globalno povezan skup računala putem kojeg bi svatko mogao brzo pristupiti podacima i programima s bilo kojeg mjesta. Njegov koncept bio je vrlo sličan konceptu današnjeg interneta. Licklider je bio prvi voditelj programa istraživanja računala u DARPA-i (*Defense Advanced Research Projects Agency*), počevši u listopadu 1962. godine. Temelj za stvaranje interneta odvio se kada su 1969. godine Američko ministarstvo obrane i Sveučilište Kalifornija u Los Angelesu uspostavili ARPANET – Advanced Research Projects Agency Network. ARPANET je prva računalna mreža koja je koristila paketni prijenos podataka te je pružila temelje za daljnji razvoj interneta. Cilj ARPANET-a bio je povezati računala, četiri različita čvora na Sveučilištu Kalifornija u LA, Institutu za informacijske znanosti na Sveučilištu Stanford, Sveučilištu Utah te Sveučilištu Kalifornija u Santa Barbari, u svrhu olakšavanja i ubrzavanja razmjene podataka i istraživanja. Prva tri čvora spojena su 1969. godine, a četvrti čvor povezan je iduće godine, sve pomoću usmjerivača (rutera), koji su omogućili slanje podataka kroz mrežu koristeći tehniku pametne komunikacije. Godine 1983. ARPANET prelazi na, tijekom 70-ih godina razvijen, TCP/IP protokol (Transport Control Protocol/Internet Protocol) – osnovni protokol koji se koristi na internetu. Ovaj je protokol postao standard za komunikaciju koja se provodi između računala i mreža, te omogućuje pouzdano i sigurno slanje podataka putem mreže. Karakteristike protokola su: pouzdanost, održavanje redoslijeda podataka, segmentacija te kontrola zagušenja mreže. Standardizacija internet protokola i arhitekture omogućena je djelovanjem Međunarodne unije za telekomunikaciju (International Telecommunication Union – ITU), koja je razvijala standardne protokole kao što je upravo TCP/IP, te radom Radnog tijela za razvoj interneta (Internet Engineering Task

Force – IETF), koji je radio na razvoju i poboljšanju tehničkih specifikacija za različite protokole interneta. U trenutku puštanja ARPANET-a u rad, dolazi do razvoja aplikacija. Tako su s vremenom razvijeni generički servisi interneta u koje spadaju prijenos podataka, elektronička pošta, World Wide Web i društveni mediji.

Tijekom 1980-ih i 1990-ih internet prestaju koristiti isključivo akademske i vojne institucije – dolazi do širenja interneta na komercijalne mreže postajući tako dostupan široj javnosti. Navedeno je rezultiralo razvojem prvog preglednika mreže – World Wide Web (WWW), često zvanog samo Web, od strane Sir Tim Berners-Leea 1989. godine tijekom rada u CERN-u (Europskom laboratoriju za fiziku čestica). World Wide Web je informatički sustav koji korisnicima omogućuje pristup raznim podacima putem interneta i predstavlja jednu od najvažnijih usluga koje internet pruža. Nastavno na WWW, prva web stranica stvorena je 1990. godine („info.cern.ch“), dostupna i danas, na kojoj je moguće pronaći informacije o WWW i kako se njime koristiti. World Wide Web 1991. godine postaje dostupan svima. Od stvaranja prvog preglednika, na tržištu se javljaju brojni web preglednici, a s pojavom Googlea 1997. godine otvara se veći broj mogućnosti za pretraživanje mreže. Uz Google Chrome, javljaju se i Mozilla Firefox, Microsoft Edge, Apple Safari i drugi.

Mobilni internet javio se već 1990-ih godina, ali su prve mobilne mreže bile skupe, spore i ograničene za korištenje, što vezano za dostupnost što za mogućnosti koje nude. Vrlo brzo je došlo do razvoja novih standarda za mobilni internet – 3G (treća) i 4G (četvrta generacija), što je omogućilo brži prijenos podataka i veće mogućnosti vezane uz samu funkcionalnost. Danas je omogućen pristup najnovijim generacijama mobilne mreže – 5G i Wi-Fi 6, koje naravno pružaju veće brzine prijenosa podataka i veću pouzdanost u odnosu na prethodne.

Internet je zbog široke primjene postao neizostavan u svakodnevnom životu – koristi se u svim sferama, od vojske pa do obrazovanja, gospodarstva, industrije, medicine, a posebno u području medija i telekomunikacije. Sve veći broj ljudi zbog rasprostranjenosti i dostupnosti pametnih telefona, prijenosnih računala i tableta ima pristup internetu. Prema najnovijim statistikama, u 2023. godini, internet koristi 5.3 milijardi ljudi, što čini više od 65% svjetske populacije.

Iako je danas brzina interneta prilično brza, smatra se kako će u budućnosti biti i brža. Razvojem umjetne inteligencije, strojnog učenja, virtualne i proširene stvarnosti i dr., internet će imati sve više mogućnosti, bit će pametniji i sposobniji prilagoditi se potrebama korisnika.

2.2 Bitcoin

Bitcoin je digitalni zapis u javnom registru koji prati vlasništvo u Bitcoin sustavu. Registar bilježi vlasništvo bez otkrivanja identiteta osobe, korištenjem digitalnih adresa koje su poput pseudonima. Vlasništvo bitcoina ovisi o posjedovanju tajnog digitalnog ključa koji vlasniku daje mogućnost prijenosa bitcoina na druge adrese – bitcoinom se može kupiti roba ili usluga bilo koje tvrtke koja prihvaća bitocin.

Bitcoinom ne upravlja tvrtka ili organizacija – vodi ga mreža računala kojoj se može priključiti bilo tko instaliranjem besplatnog Bitcoin softvera otvorenog koda. Sustav je dizajniran tako da zlonamjerni napadači mogu sudjelovati, ali će biti učinkovito ignorirani dokle god većina mreže ostane iskrena. Čak i ako bi napadači stekli većinu računalne

snage u mreži, mogli bi poništiti vlastite transakcije i blokirati nove transakcije dok drže većinu, ali ne bi mogli izravno ukrasti bitcoine.

Bitcoin je započeo kao besplatni računalni program otvorenog koda napisan od strane autora ili grupe autora koji su koristili pseudonim Satoshi Nakamoto. Pseudonim se koristio i u izvornom kodu i u bijeloj knjizi koja opisuje ideju. Nakamotovo uključanje u Bitcoin projekt oslabilo je sredinom 2010., nakon čega je zajednica predvođena Gavinom Andresenom, preuzela odgovornost za izvorni kod.

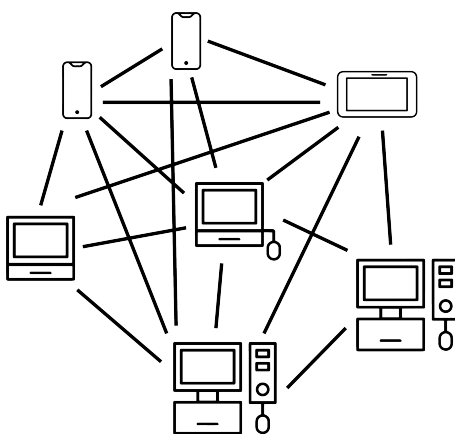
Vrijednost Bitcoina leži u:

1. Upotrebljivosti – bitcoine je moguće koristiti za kupnju dobara i usluga
2. Mjenjačka vrijednost – mogućnost trgovanja Bitcoina za druge valute na burzama
3. Spekulacija – popularnost Bitcoina raste, a s njom i njegova vrijednost
4. Rijetkost – količina dostupnog Bitcoina je algoritamski ograničena na 21 milijun Bitcoina.

2.3 Model ravnopravnih partnera (*Peer to peer mreža*)

Ideja P2P mreže (*eng. Peer to Peer*) postojala je i prije pojave interneta, a implementacija P2P mreže prvi put provedena je 1999. godine, kada je glazbena platforma *Napster* objavila svoju platformu za dijeljenje datoteka.

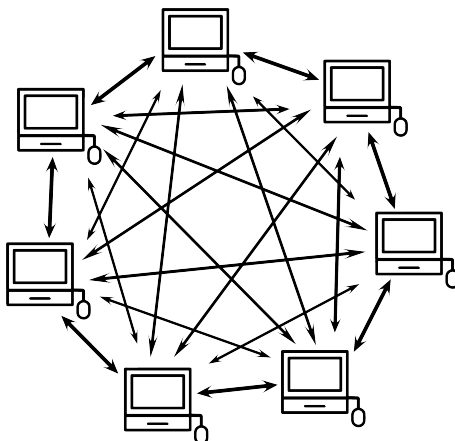
P2P mreža predstavlja distribuirani sustav u kojem svako računalo čini ravnopravnog partnera (*eng. Peer*) spojeno na mrežu ulančanih blokova (*eng. Blockchain*) stvarajući čvor (*eng. Node*) u mreži. U ovakvom sustavu su svi čvorovi ravnopravni sudionici, što je vidljivo na 2.1. U idealnoj P2P mreži, svaki čvor stavlja dio svojih resursa (npr. određeni kapacitet, prostor na disku, propusnost mreže) na raspolaganje svim sudionicima mreže, bez potrebe za središnjim računalom ili serverom, odnosno bez posrednika. Ovakva organizacija čini svaki čvor istovremeno davateljem i korisnikom, pružajući zajednički pristup svim podacima bez potrebe za centralnim serverom. Svako računalo koje je povezano s mrežom ulančanih blokova sudjeluje u potvrdi transakcija i blokova, odnosno u procesu validacije.



Slika 2.1: Prikaz P2P mreže u kojoj je svako računalo ili čvor ravnopravno

2.3.1 Značajke P2P mreže

Blockchain koji funkcionira putem P2P mreža distribuiran je i decentraliziran (Slika 2.2). Pojam distribuiran označava dijeljenje resursa između svih sudjelujućih čvorova, dok decentraliziran predstavlja da niti jedan čvor nije centralan, odnosno da ne postoji središnje računalo koje bi diktiralo operacije.



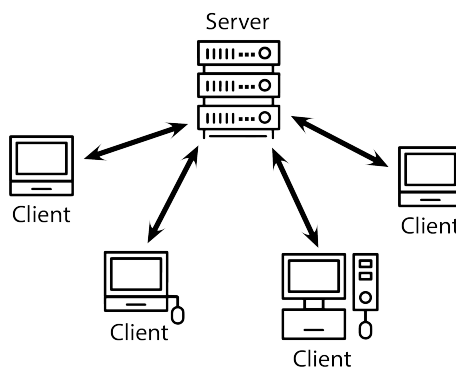
Slika 2.2: *Blockchain preko P2P mreže primjer je decentralizirane arhitekture gdje svaki sudjelujući čvor istovremeno djeluje kao davatelj i korisnik (poslužitelj i primatelj) zadržavajući kopiju blockchaina*

Kao distribuiran sustav, blockchain se nalazi na stotinama tisuća čvorova i dijeli njihove resurse tijekom rada. Blockchain pohranjuje podatke diljem svoje P2P mreže, eliminirajući niz rizika povezanih s centraliziranim čuvanjem podataka. Nema ovisnosti o jednom poslužitelju, stoga blockchain nema centralnu točku neuspjeha. Njegova decentralizirana arhitektura čini da svaki sudjelujući čvor čuva kopiju blockchaina, održavajući kvalitetu podataka putem masovne replikacije baze podataka i računalnog povjerenja. Nema centralizirane službene kopije podataka, i nijedan korisnik nije "pouzdaniji" od bilo kojeg drugog u ovoj arhitekturi. S blockchainom, transakcije se emitiraju u mrežu, a poruke se dostavljaju prema najboljim naporima. Po dolasku novih transakcija, čvorovi validatori, poznati kao rudari (eng. *Miners*), provjeravaju ih i dodaju u blok koji grade, a zatim emitiraju završeni blok drugim čvorovima. Ova operacija nastavlja se do kraja životnog ciklusa blockchaina, uz nagrade ili poticaje za čvorove koji sudjeluju u procesu validacije, uobičajeno poznatom kao rudarenje blokova (eng. *Mining*). Sumirane značajke P2P mreže:

1. svaki čvor (računalo) koji je dio mreže, u mreži je ravnopravan partner;
2. ne postoji središnje računalo u mreži;
3. svaki je partner istovremeno davatelj i korisnik (poslužitelj i primatelj);
4. svako računalo sudjeluje u procesu validacije;
5. svako računalo dijeli i razmjenjuje radno opterećenje.

2.3.2 Spajanje na *Peer to Peer* mrežu

Za spajanje na P2P mrežu, kao ravnopravni partner, potrebno je računalo, internet i P2P Softver. P2P Softver s pridruženim računalom postaje čvor (Slika 2.3) u mreži te diktira i provjerava pravila kojih se drže svi prisutni čvorovi u mreži.



Slika 2.3: Spajanje na Peer to Peer mrežu

2.4 Decentralizacija

U svojim ranim danima, internet je bio decentraliziran. To znači da nije postojao središnji server koji upravlja svime, već beskonačan broj čvorova povezanih u mrežu koji su mogli međusobno razmjenjivati informacije putem zajedničkog, besplatnog protokola (TCP/IP). U slučaju zakazivanja jednog čvora, stabilnost mreže u cjelini nije bila narušena. Do danas se na ovoj decentraliziranoj osnovi nije ništa promijenilo, osim što su dodane snažno centralizirane aplikacije na ovu početnu razinu. Činjenica da se većina ljudi i dalje oslanja na velike pružatelje usluga, čime žrtvuje privatnost, ima veze s praktičnošću. Decentralizacija je uvijek kompliciranija, a dok centralizirani sustav olakšava korištenje, istovremeno korisnika izlaže centralnoj vlasti, koja primjerice u slučaju e-pošte, može čitati komunikaciju korisnika.

Tijekom svakodnevnog korištenja interneta, u većini slučajeva korisnik ne koristi decentraliziranu mrežu, već se služi centraliziranim platformama kakve imaju najčešće korištene aplikacije (npr. Facebook, X – ranije poznat kao Twitter, Airbnb i dr.). Takve aplikacije imaju korisnička sučelja pomoću kojih se korisnik brzo i jednostavno orijentira i njima služi, te osiguravaju prisutnost najvećeg mogućeg broja ljudi s kojima postoje zajednički interesi.

Centralizirani sustavi mogu biti pojašnjeni kao piramide u kojima se sve niti slijevaju prema vrhu, a ono što je na vrhu ima kontrolna prava. Nedostatak takvog sustava je mogućnost kvara – ako se centralna kontrola isključi, cijeli sustav postaje onemogućen za korištenje. S druge strane, decentralizirana arhitektura, koja se krije iza Bitcoin-a, sigurna je po dizajnu – podaci su otvorena tipa, ne postoji centralno računalo koje bi diktiralo operacije, te u slučaju napada ne dolazi do pada cijelog sustava.

Centralizirana arhitektura, odnosno centralni server, je privlačniji i zlonamjernim napadačima, jer napad takvog servera omogućuje pristup svim traženim informacijama odjednom. Upravo to je dovelo do hakiranja nekoliko centralno organiziranih kripto burzi, dok sama Bitcoin mreža nikada nije bila kompromitirana.

Decentralizirani sustav smatra se etički vrijednijim, efikasnijim, otpornijim te s mogućnošću napretka – Bitcoin se sam razvija kao softver otvorenog koda jer svatko može pridonijeti njegovom poboljšanju, a ako je prijedlog dobar, mreža će ga prihvatiti i prilagoditi.

Potpuna decentralizacija je prema tome jedinstvena prodajna točka Bitcoina, koja ga ujedno čini i izuzetno otpornim.

2.5 Tehnologije koje su dovele do razvoja Bitcoin kriptovalute

Bitcoin kriptovaluta prva je uspješna decentralizirana kriptovaluta, odnosno digitalni novac, nastala na temelju nekoliko ključnih ideja iz prošlosti razvijenih u poljima kriptografije, konsenzusnih protokola i P2P mreža. U nastavku će biti obrađene sljedeće ideje:

- 2.5.1. Kriptografija s javnim ključem ili asimetrična kriptografija (*eng. Public-key cryptography*) - Whitfield Diffie i Martin Hellman, 1976. godina
- 2.5.2. Merkle stablo (*eng. Merkle Tree*) – Ralph C. Merkle, 1979. godina
- 2.5.3. Vremenska oznaka (*eng. Time-stamp*) - Stuart Haber i W. Scott Stornetta, 1991. godina
- 2.5.4. Pametni ugovori (*eng. Smart contracts*) – Nick Szabo, 1994. godina
- 2.5.5. Dokaz radom (*eng. Proof of Work, POW*) – koncept osmislile Cynthia Dwork i Moni Naor 1993., a Adam Back ga je 1997. godine neovisno poboljšao i implementirao u sustavu protiv spama - HashCash
- 2.5.6. Secure Hash Algorithm 2 (SHA-2) – NSA (United States National Security Agency), 2001. godine

2.6 Kriptografija

Digitalni sustav plaćanja kao što je Bitcoin zahtijeva snažnu sigurnost protiv prevara. Nekoliko ključnih komponenti tehnologije ulančanih blokova, uključujući svojstvo nepromjenjivosti, izgrađene su korištenjem kriptografskih principa.

Kriptografija je praksa i proučavanje metoda osiguravanja komunikacije u prisutnosti potencijalnih neprijatelja trećih strana. Formalnije se može definirati kao protokol koji sprječava treće strane i javnost u čitanju privatnih poruka. Brojne značajke informacijske sigurnosti, poput autentifikacije, povjerljivosti podataka, integriteta podataka i neporecivosti, ključne su za modernu kriptografiju. Njezino postojanje može se prepoznati u disciplinama matematike, računalnih znanosti, elektroinženjeringa, znanosti o komunikacijama i fizike, gdje se primjene protežu od elektroničke trgovine, kartica s čipom za plaćanje, računalnih lozinki, vojnih komunikacija do, naravno, kriptovaluta.

2.6.1 Osnovni koncepti kriptografije

Cilj kriptografije jest transformirati bilo koje podatke iz njihovog izvornog oblika, poznatog kao otvoreni tekst, u oblik koji se naziva kriptotekst. Ovaj proces se naziva enkripcijom. Suprotni proces, koji obuhvaća vraćanje otvorenog teksta iz kriptoteksta, naziva se dekripcijom. Bitno je shvatiti da otvoreni tekst ne mora biti samo tekstualna poruka; može biti računalna datoteka koja predstavlja binarne ili druge vrste podataka, slika, baza podataka i dr.. Određeni kriptosustav radi na temelju specifičnih algoritama za enkripciju i dekripciju. Algoritam predstavlja računalni postupak koji slijedi određeni skup pravila. Postupak enkripcije otvorenog teksta pomoću određenog algoritma ovisi o kodu, poznatom kao tajni ključ, koji je zapravo veliki broj.

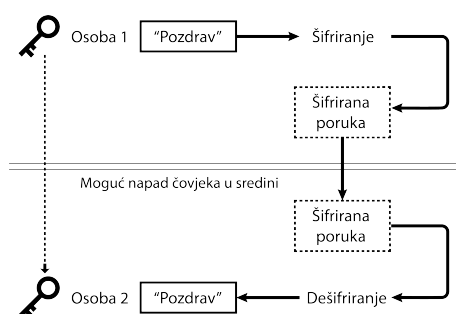
2.6.2 Simetrična i asimetrična kriptografija

Simetrična kriptografija

Simetrična kriptografija predstavlja sustav u kojem pošiljalatelj i primatelj dijele isti ključ za šifriranje i dešifriranje poruka. Iako su simetrični sustavi jednostavniji i brži, imaju

veliku slabost - osobe uključene u proces moraju međusobno razmijeniti ključ kako bi uspješno dešifrirale kriptotekst. Taj proces razmjene može biti ranjiv jer postoji potencijalna opasnost da treća strana otkrije ključ.

Na primjer, ako Osoba 1 želi izmijeniti poruku s Osobom 2 (Slika 2.4), koristi svoj tajni ključ s ciljem šifriranja poruke "Pozdrav" i šalje je Osobi 2. Osoba 1 također dijeli tajni ključ s Osobom 2, a ta razmjena ključeva može se dogoditi online ili offline (npr. putem USB uređaja). Kada Osoba 2 primi poruku, pretpostavlja se da posjeduje tajni ključ i koristi ga za dešifriranje poruke. Iako kriptografski algoritam osigurava siguran prijenos poruke u ovom primjeru, ključ nije zaštićen. Strana osoba koji dođe do ključa lako može otkriti tajnu poruku. Ovaj proces zahtijeva sigurnu razmjenu ključeva kako bi simetrična kriptografija funkcionirala.



Slika 2.4: Koraci u simetričnoj kriptografiji

Kriptografija s javnim ključem - asimetrična kriptografija

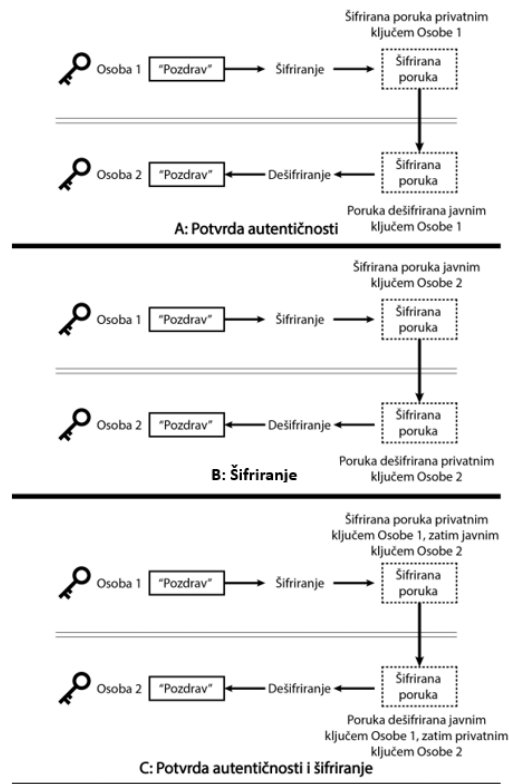
Kriptografija s javnim ključem, poznata i kao asimetrična kriptografija, predstavlja sustav koji koristi parove ključeva: javni ključ, koji se može javno distribuirati, i privatni ključ, koji je poznat isključivo vlasniku. Ovaj postupak ima dva glavna cilja: autentifikaciju, gdje javni ključ potvrđuje da je pošiljatelj poruke vlasnik pripadajućeg privatnog ključa, te šifriranje, gdje samo vlasnik pripadajućeg privatnog ključa može dešifrirati poruku šifriranu javnim ključem. Zbog računalne kompleksnosti asimetrične enkripcije, obično se primjenjuje samo na male blokove podataka, uglavnom za prijenos simetričnog ključa koji šifrira preostali potencijalno dugi slijed poruka. Slika 5 prikazuje sljedeće:

A) Osoba 1 šifrira poruku "Pozdrav" koristeći svoj privatni ključ koji je poznat samo njoj. Nakon što Osoba 1 pošalje ovu poruku Osobi 2, ona je dešifrira pomoću javnog ključa Osobe 1. Dekripcija koja daje pozitivan rezultat potvrđuje da je poruku poslala Osoba 1. Iako ova komunikacija osigurava autentičnost, ne pruža šifriranje i podložna je potencijalnom napadu od treće strane, gdje bilo tko tko posjeduje javni ključ Osobe 1, koji je poznat po konvenciji, može pročitati poruku.

B) Osoba 1 šifrira poruku "Pozdrav" koristeći javni ključ Osobe 2. Nakon što Osoba 1 pošalje ovu poruku Osobi 2, ona je dešifrira pomoću svog privatnog ključa. Ova komunikacija je sigurna od napada čovjeka u sredini, jer pruža šifriranje koje potvrđuje da je nitko ne može dešifrirati bez privatnog ključa Osobe 2, koji je poznat samo njoj. Međutim, ovo ne potvrđuje autentičnost poruke, jer bilo tko može poslati tu poruku koristeći javni ključ Osobe 2.

C) Osoba 1 šifrira poruku "Pozdrav" koristeći svoj privatni ključ, zatim javni ključ Osobe 2. Nakon što primi poruku, Osoba 2 je dešifrira koristeći svoj privatni ključ, zatim javni ključ

Osobe 1. Za razliku od dijela A), ova komunikacija je sigurna od napada treće strane. Nitko ne može pročitati poruku bez privatnog ključa Osobe 2, kojoj je poruka poslana, stoga pruža šifriranje. Ako dekripcija daje pozitivan rezultat, to također potvrđuje autentičnost poruke.



Slika 2.5: Kriptografija s javnim ključem - Asimetrična kriptografija. Slučaj A prikazuje potvrdu autentičnosti poruke, slučaj B prikazuje šifriranje, dok slučaj C prikazuje i potvrdu autentičnosti i šifriranje.

2.6.3 Kriptografska hash funkcija

Kriptografska hash funkcija je matematički algoritam koji preslikava podatke proizvoljne veličine u bitni niz fiksne veličine, nazvan hash. Dizajnirana je kao jednosmjerna funkcija koja je neizvediva za inverziju. Jedini način za rekreiranje ulaznih podataka iz izlaza idealne kriptografske hash funkcije je pokušati iscrpnu pretragu mogućih unosa kako bi se vidjelo jesu li podudarni.

Idealna kriptografska hash funkcija ima pet glavnih svojstava:

1. deterministička je, tako da ista poruka uvijek rezultira istim hash-om;
2. izračunavanje hash vrijednosti za bilo koju današnju poruku je brzo;
3. neizvedivo je generirati poruku iz njene hash vrijednosti osim pokušavanjem svih mogućih kombinacija,
4. mala promjena u poruci trebala bi promijeniti hash vrijednost tako značajno da nova hash vrijednost izgleda nekorelirano sa starom hash vrijednošću, i
5. pronalaženje dvije različite poruke s istom hash vrijednosti je neizvedivo.

Tri su glavne funkcije hasha da:

- deterministički izmiješa podatke
- prihvati unos bilo koje duljine i generira rezultat fiksne duljine
- ulaz ne može biti izveden iz izlaza

Hash funkcija koju Bitcoin koristi, a bit će detaljnije objašnjena kasnije u ovom poglavlju, je SHA-256. SHA-256 jednosmjerna je funkcija što znači da nitko matematički ne može obrnuti izlaz, kako bi odredio ulaz. Ono što je bitno naglasiti je da bez obzira na duljinu ulaza, SHA-256 taj ulaz uvijek generira u točno 64 znaka dug (heksadekadski) niz izlaza.

Primjer rečenice koja će biti korištena kako bi se pojasnilo napisano – neovisno o duljini ulaza, izlaz je uvijek jednako dug – je rečenica: „Tehnologija ulančanih blokova i kriptovaluta – Priručnik“, u kojoj se gleda samo ono napisano unutar navodnika.

Ulaz:

Tehnologija ulančanih blokova i kriptovaluta – Priručnik

Izlaz:

52FD5BE891B665CB68AE35014F497375C9E7CEC4C0C2F0CC87B9AB5CA730E6CA

Ako bi se rečenica promatrala zajedno s navodnicima, tada je ulaz:

„Tehnologija ulančanih blokova i kriptovaluta – Priručnik“

a izlaz:

6D554CF9767A20862D6426CB4DF00D690898A0D0E56A5012058676A47601505F

Može se uočiti kako navodnici u potpunosti mijenjaju generirani hash, što se tiče nasumične kombinacije brojeva i slova, ali duljina hash-a ostaje jednaka – 64 znaka. Naime, prvi string izlaza

52FD5BE891B665CB68AE35014F497375C9E7CEC4C0C2F0CC87B9AB5CA730E6CA

i drugi string izlaz

6D554CF9767A20862D6426CB4DF00D690898A0D0E56A5012058676A47601505F

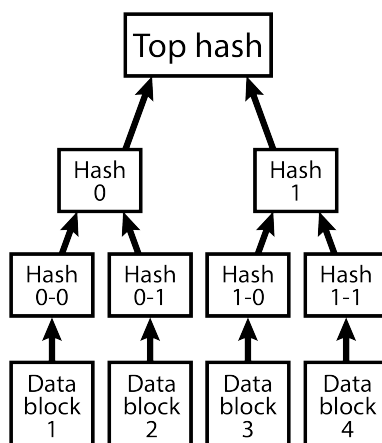
imaju 64 znaka, a razlika je samo u navodnicima rečenice koja je korištena kao ulaz.

U nastavku slijedi još nekoliko primjera izlaznih stringova SHA-256 hash funkcije:

7AE3F3DC6D00E54035F745C98A2C1390BA00D2AF1A9162A2B56C4800EA70C768
7E4B5DFBBDBD126457F9B7D6104A1B93358A74EC98DA2C7F9068F9329447C76
B24B720E24087E2604F0D2CBEA3BEBB4694116CE89D947518C29BDDBF8B09327
CE1930782B4D89960A29C815F4B0F08760AB81742E6AF1B05FD992E82E6CA138

2.6.4 Merkle stablo

Merkle stablo (Slika 2.6) binarna je struktura podataka osmišljena od strane Ralpha Merkla, 1979. godine, i koristi se za sažimanje i provjeru integriteta velikog skupa podataka. Za razliku od običnog stabla, konstruira se rekurzivnim hashiranjem parova čvorova. Kriptografske hash funkcije često se koriste za provjeru integriteta popisa stavki kao što su razbijeni dijelovi velikog preuzimanja. U takvim slučajevima, jedna od opcija je spojiti sve dijelove i uzeti hash cijelog preuzimanja. Problem s tim je da ako je jedan dio oštećen, korisnik neće saznati sve dok cijelo preuzimanje ne završi, a čak i tada neće znati koji je dio oštećen. Bolje rješenje je uzeti hash svakog dijela pojedinačno kako bi se svaki dio mogao provjeriti kako dolazi. Međutim, ako postoji veliki broj dijelova, veća je šansa da će se neka od hash vrijednosti pokvariti. Osim toga, to je puno podataka koje pouzdani izvor mora pohraniti. Idealno bi bilo da pouzdani izvor mora pružiti samo jedan hash, a ostali hashevi mogu se preuzeti s nepouzdatih izvora, poput sudionika u P2P mreži. To se može postići pomoću vršnog hash-a generiranog hashiranjem svih hash dijelova. Dobivena struktura naziva se hash lista.



Slika 2.6: Struktura Merkleova stabla

Ako je broj dijelova vrlo velik, lista hasheva svih dijelova također može biti prilično velika. Da bi se samo jedan dio provjerio protiv pouzdanog vršnog hash-a, trebalo bi dobiti sve hasheve u listi hasheva. Upravo u ovom hash ili Merkle stablu, uzimaju se hashevi svih dijelova kao i u listi hasheva, ali se zatim ovi hashevi pariraju i uzima se hash svakog para, i ti hashevi se ponovno sparuju, i tako dalje dok na vrhu ovog stabla hasheva ne ostane samo jedan hash.

2.6.5 Vremenska oznaka (eng. *Time-stamp*)

Haber i Stornetta su 1991. u radu *How To Time-Stamp a Digital Document* predložili računalno izvedive postupke digitalnog vremenskog označavanja tekstualnih, zvučnih, slikovnih i video dokumenata zbog njihove sve veće upotrebe, a s ciljem saznanja kada je dokument stvoren ili posljednji put izmijenjen. Predstavljene metode vremenskog označavanja prema njima moraju zadovoljiti dva kriterija – prvo, moraju se vremenski označiti stvarni bitovi dokumenta (actual bits), bez pretpostavke o fizičkom mediju na kojem je dokument zabilježen, i drugo, datum i vrijeme vremenske oznake ne smiju biti podložni krivotvorenju. U istom radu su predložili dva moguća rješenja, s tim da

oba uključuju korištenje jednosmjernih funkcija za hash, čiji se izlazi obrađuju umjesto dokumenata i digitalnih potpisa, a rješenja se razlikuju jedino u načinu na koji se datum i vrijeme čine nemogućim za krivotvorenje. Prvo rješenje sastoji se od toga da su hashevi dokumenata predani TSS (engl. Time Stamping Service) povezani zajedno, a certifikati koji zabilježavaju povezivanje određenog dokumenta se distribuiraju drugim klijentima nizvodno i uzvodno od tog dokumenta. U drugom predloženom rješenju, nekoliko klijenata unutar skupine mora vremenski označiti hash, a članovi se biraju putem pseudoslučajnog generatora koji koristi sam hash dokumenta. Ovo generiranje čini nemogućim namjerno odabiranje klijenata koji bi trebali, ili ne bi trebali, vremenski označiti hash, što je moguće implementirati bez potrebe za centraliziranim TSS-om.

2.6.6 Vremenska oznaka Unix

Vremenska oznaka (eng. *Time-stamp*) predstavlja točno određeno vrijeme i datum, a vremenska oznaka Unix broji broj sekundi koji su prošle od 00:00:00 (UTC – Coordinated Universal Time), 1. siječnja (četvrtak) 1970. godine (Unix epoha), umanjeno za skokove sekundi. S obzirom na to da se koristi UTC, ovo točno određeno vrijeme se tehnički ne mijenja, bez obzira na to gdje se osoba nalazi u svijetu. Koristeći ovu oznaku vremena, svaki dan ima točno 86,400 sekundi kako bi se oduzeli skokovi sekundi od epohe. Osim što Unix vremenska oznaka djeluje kao izvor varijacije za hash blok, istovremeno čini manipulaciju tehnologijom ulaćanih lanaca izazovnijom. Bitcoin protokol vremensku oznaku smatra vjerodostojnom ako je vremenska oznaka veća od medijane vremenske oznake prethodnih 11 blokova i manja od vremena prilagođenog mreži, plus dva sata. „Vrijeme prilagođeno mreži“ označava medijan vremenskih oznaka vraćenih od strane svih čvorova povezanih sa sudjelujućim čvorom. Unix vremenska oznaka pohranjena je kao 32-bitni cjelobrojni broj u mnogim sustavima, a djeluje na način da konvertira vremenske oznake koristeći metode za sekunde, milisekunde i mikrosekunde, kako bi očitala datume. Razdoblje korištenja Unix vremenske oznake prestat će 19. siječnja 2038. (traje otprilike 68 godina), jer će doći do „prelijevanja“ 32-bitnog broja. To bi značilo da će prije spomenutog datuma, 19. siječnja 2038. godine, veliki broj aplikacija morati usvojiti novu konvenciju za vremenske oznake ili biti prebačeni na 64-bitne sustave.

Vremenske oznake koriste se u svrhu vođenja evidencije informacija na mreži ili na računalu, a iste prikazuju kada su određene informacije stvorene, razmijenjene, izmijenjene ili izbrisane.

Slijedi nekoliko primjera kada se koriste vremenske oznake:

- Računalne datoteke sadrže vremensku oznaku koja pokazuje kada je datoteka stvorena i posljednji put promijenjena.
- Objave na društvenim mrežama sadržavaju datum i vrijeme kada je objava napravljena.
- Poslane poruke na pametnim telefonima ili u korištenim aplikacijama imaju vremenske oznake za bilježenje datuma i vremena kada je poruka poslana, primljena ili pregledana.
- Vremenske oznake koriste se na digitalnim ugovorima i potpisima kako bi se znalo kada je dokument potpisan.
- Tehnologija ulančanih blokova koristi vremenske oznake kako bi se osigurala valjanost transakcija, kao što je slučaj s kriptovalutama.

Upotreba vremenskih oznaka, primjerice u digitalnom potpisu, zahtijeva visok stupanj

pouzdanosti iz pravnih razloga. Pouzdana treća strana može generirati vremensku oznaku za dokument, u zamjenu za korištenje vremena s računala na kojem je taj dokument pohranjen. Treće strane su ovdje poznate kao autoriteti za vremensko označavanje (*eng. TSA-Time Stamping Authorities*). Autoriteti za vremensko označavanje koriste infrastrukturu javnog ključa – procese i tehnologije koji omogućuju šifriranje i potpisivanje podataka kako bi se osigurala valjanost i sigurnost od manipulacije te vremenske oznake.

2.6.7 Vremenske oznake u tehnologiji ulančanih blokova

Vremenske oznake su izuzetno važne u tehnologiji ulančanih blokova, posebno u upotrebi te tehnologije s kriptovalutama. Svaki blok u ulančanom bloku ima zaglavlje koje sadrži Unix vremensku oznaku trenutka kada je taj blok hashiran – na taj način je svakom bloku dana jedinstvena oznaka i sprječeno je dvostruko trošenje.

Vremenske oznake na temelju tehnologije ulančanih blokova koriste se i u vremenskom označavanju sadržaja, gdje vremenske oznake dokazuju da je sadržaj na određenoj stranici objavljen na taj datum vremenske oznake. Isto je moguće koristiti i na primjerice izborima kako bi se dokazala valjanost danih glasova, kao i u sprječavanju prijevare.

2.6.8 Rudarenje ulančanih blokova

Unix vremenske oznake koriste se i za prikazivanje koliko je vremena bilo potrebno za rudarenje određenog bloka, što određuje koliki prihod rudar dobiva – rudari ostvaruju prihod proizvodnjom blokova u kratkom vremenskom roku.

Iako je moguće da rudar bitcoina promijeni vremensku oznaku tijekom hashiranja s ciljem stvaranja dojma da je blok stvoren brže nego što je, postoje dva pravila koja to sprječavaju:

1. Pravilo o medijanu prošlog vremena – vremenska oznaka mora biti veća od medijana vremenskih oznaka prošlih 11 blokova, odnosno, trebalo bi izračunati hasheve 6 od posljednjih 11 blokova.
2. Pravilo o budućem vremenu – vremenska oznaka ne može biti više od dva sata unaprijed u odnosu na lokalno vrijeme računala rudara.

Prvo pravilo osigurava da se lanac kreće ravnomjerno naprijed, dok drugo onemogućuje da lanac ide predaleko unaprijed. Oba pravila sprječavaju mogućnost manipulacije vremenskih oznaka ulančanih blokova.

2.6.9 Pametni ugovori *eng. Smart Contracts*

Nick Szabo, američki računalni znanstvenik, prvi je predložio koncept pametnih ugovora 1994. godine. Također je izumio virtualnu valutu pod nazivom "Bit Gold" 1998. godine, deset punih godina prije nego što je predstavljen Bitcoin. Pametni ugovori su tehnologija koja je prethodila BTC-u, i iako nije u početku bila namijenjena bitcoin sustavu, relativno nedavno je implementirana u isti.

Razumijevanje Bitcoin pametnih ugovora

Implementacija pametnih ugovora (BCS, *eng. Bitcoin Smart Contract*) u Bitcoin sustav predložena je prvi put 2020. godine od strane autora (Hiro Midas) rada BSC: A Bitcoin Smart Contract Implementation. Pametni ugovor na Bitcoin mreži je samoizvršavajući ugovor programiran da automatski obavlja određene radnje kada se ispune određeni uvjeti.

U kontekstu Bitcoin mreže, pametni ugovori kombinacijom neograničenog kreativnog prostora pametnih ugovora i ogromnim mrežnim učinkom Bitcoina omogućuju razvoj decentraliziranih aplikacija (dapps) sposobnih za izvršavanje složenih financijskih transakcija bez posrednika. Decentralizirane aplikacije uključuju, ali nisu ograničene na imovinu, privatnost, igre, DEX i stabilni coin.

Dok se tradicionalni ugovori oslanjaju na pravne mehanizme provedbe kako bi osigurali usklađenost, pametni ugovori provode se pomoću samog koda, čineći ih transparentnijima, učinkovitijima i sigurnijima. Imaju potencijal automatizirati različite financijske transakcije, uključujući usluge jamstva, osiguravateljske zahtjeve i upravljanje lancem opskrbe.

Primjene Bitcoin pametnih ugovora obuhvaćaju raznolik spektar trenutnih i potencijalnih situacija, uključujući:

1. Kanal za plaćanja: bitcoin pametni ugovori omogućuju stvaranje kanala za plaćanja radi brzih i povoljnih transakcija, posebno korisnih za mikroplaćanja poput plaćanja pojedinačnih članaka ili videozapisa na mreži.
2. Usluge jamstva: mogu stvoriti usluge jamstva za online transakcije, sigurno i transparentno držeći sredstva dok se ne ispune uvjeti dogovora.
3. Decentralizirana tržišta: omogućuju stvaranje decentraliziranih tržišta, gdje kupci i prodavatelji mogu djelovati bez centralnog autoriteta, rezultirajući učinkovitijim i transparentnijim tržištima s manjim rizicima prevare i cenzure.
4. Upravljanje lancem opskrbe: mogu stvoriti transparentne i sigurne sustave za upravljanje lancem opskrbe, prateći kretanje dobara i pokrećući plaćanja kada se ispune određeni uvjeti, kao što su primitak dobara ili provjera kvalitete.
5. Upravljanje identitetom: mogu uspostaviti decentralizirani sustav upravljanja identitetom, čuvajući osobne podatke i omogućujući pojedincima kontrolu pristupa osobnim informacijama uz očuvanje privatnosti.

U budućnosti, Bitcoin pametni ugovori mogli bi revolucionirati različite industrije stvaranjem novih financijskih instrumenata, automatizacijom pravnih i regulatornih procesa te omogućavanjem novih oblika upravljanja, kao što su decentralizirane autonomne organizacije (DAO-ovi).

Pozitivne i negativne strane pametnih ugovora

Pozitivne strane:

1. eliminacija posrednika: pametni ugovori, slično tehnologiji lanca blokova, eliminiraju potrebu za posrednicima,
2. efikasnost: ubrzavaju izvršenje ugovora,
3. preciznost: eliminiraju ljudske greške,
4. nepromjenjivost: programiranje ostaje nepromjenjivo

Negativne strane:

1. trajnost: greške ne mogu biti ispravljene nakon što je ugovor implementiran,
2. ljudski faktor: vještina programera ključna je za osiguravanje da kod odražava uvjete ugovora,
3. rupe: ranjivosti u kodiranju mogu omogućiti izvršenje ugovora s lošom namjerom.

2.6.10 Dokaz radom - PoW (eng. *Proof of Work*)

Dokaz radom prvi je osmišljeni algoritam postizanja konsenzusa, koji zahtijeva određeni napor koji nije značajan, ali je dovoljno izvediv da odvrati napadače u distribuiranom sustavu. Ti akteri obično pokušavaju slati neželjene e-pošte i izvoditi napade uskraćivanja usluge (DoS). Koncept dokaza radom razvile su Cynthia Dwork i Moni Naor 1993., a kasnije (1997.) ga je Adam Back neovisno poboljšao i koristio u svojem sustavu protiv spama, HashCash. Nakamoto je implementirao ovaj način rada s manjim izmjenama u Bitcoin, 2009. godine.

Stvaranje i verifikacija bloka složeni su procesi koji uključuju kriptografiju i matematiku. U slučaju dokaza rada, izazov je korisnicima otežati stvaranje novog bloka u lancu blokova. Zadatak rudara je pronaći rješenje za postojeći matematički problem. Matematički je relativno lako pronaći odgovarajući rezultat (izlaz) za danu formulu (ulaz), ali obrnuti proces je izazovan. Najjednostavniji pristup je isprobati različite mogućnosti dok rezultat postane odgovarajuć – na taj način funkcionira rudarenje. Svaki rudar u mreži isprobava različite mogućnosti dok prvi ne pronađe rješenje. Ovdje je korisno pridonijeti značajnom računalnom snagom. Prema udjelu računalne snage u ukupnoj mreži, svaki rudar ima priliku pronaći ispravno rješenje. Recimo, ako korisnik posjeduje 10% ukupne računalne snage, u prosjeku mu treba 100 minuta da riješi blok. Ovdje postoji rizik jer korisnik može drugima pokušati predstaviti lažan blok, a ukoliko drugi rudari to ne primijete, korisnik bi mogao uspjeti dodati lažne daljne blokove u lanac blokova. Matematički gledano, vjerojatnost toga eksponencijalno opada, a opasnost se javlja samo kada pojedini korisnik ili grupa udruženih korisnika posjeduje minimalno 51% računalne snage u mreži, pri čemu se javlja mogućnost napada većine, koji će biti opisan u kasnijim poglavljima.

Unutar konteksta ulančanih blokova, PoW osigurava koordinaciju mreže i sigurnost podataka. To zahtijeva sudjelovanje čvorova ili rudara koji se natječu za poziciju kako bi odredili tko ima priliku izgraditi sljedeći blok. Pri tome koriste računalnu snagu kako bi pronašli određenu hash vrijednost. Ne postoji poznati prečac ili optimizirani pristup za otkrivanje hash-a osim postupnog povećavanja. Ovaj pristup zahtijeva veliku energiju i vrijeme da rudar pronađe ciljanu hash vrijednost, ali proces verifikacije je dovoljno jednostavan da drugi brzo provjere opravdanost tvrdnje.

Zbog potrebe ovog sustava za energijom i vremenom, postaje skupo za napadače pokrenuti napade spama u mreži. Isti ograničavajući faktor koji djeluje s kriptografskim načelima također štiti blockchain od izmjena. Napadači žele promijeniti unose, što je gotovo nemoguće izvesti zbog potrebe za ogromnom računalnom snagom. Značajke dokaza radom su:

- ulaganje rada s ciljem postizanja konsenzusa i osvajanja nagrade,
- ulaže se računalna snaga, ne fizički rad,
- rad, koji se sastoji od rješavanja računalne zagonetke, ulažu rudari (*Miners*).

Sustav nagrađivanja djeluje na način da onaj rudar koji prvi uspješno riješi matematički problem (zagonetku) validira blok. Rudar koji uspješno riješi zagonetku dobije nagradu i naknadu, a validirani blok se pohranjuje na lanac blokova i stvara se mogućnost za rješavanjem nove zagonetke.

2.6.11 Prednosti i nedostaci PoW-a

Prednosti: svatko može rudariti kriptovalute koje se zasnivaju na dokazu rada; nemogućnost prevare sustava od strane jednog rudara, jer svi drugi sudionici moraju validirati blok – ukoliko primijete da dodani blok nije valjan, odbacuju ga; vjerojatnost za napad je mala, jer je za isti potrebno posjedovati minimalno 51% računalne snage na cijeloj mreži.

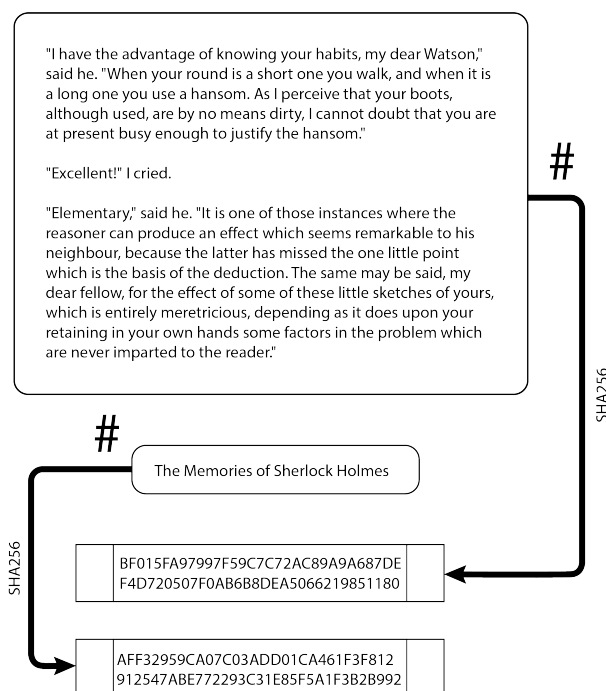
Nedostatci: relativno velika potrošnja energije i vremena; isplativost prisutna uz upotrebu profesionalne opreme, specijaliziranih procesora i grafičkih kartica.

2.6.12 Secure Hash Algorithm

SHA-2 i SHA-256

Postoji nekoliko algoritama koji se mogu koristiti za stvaranje hash funkcije: MD5, SHA-1, SHA-2, SHA-3, Whirpool i BLAKE. Kriptografska hash funkcija posebno je važna u kontekstu tehnologije ulančanih blokova, jer se njegova nepromjenjivost postiže korištenjem algoritma SHA-256 iz SHA-2 obitelji algoritama.

Slika 2.7 prikazuje klasičan primjer SHA-256 hash generiranja izvatka iz knjige „Memoari Sherlocka Holmesa“, odnosno razgovora između Sherlocka Holmesa i Johna Watsona, koju je napisao škotski autor Sir Arthur Conan Doyle.



Slika 2.7: Primjer SHA-256 hash generiranja izvatka iz knjige „Memoari Sherlocka Holmesa“. SHA-256 hash naslova knjige i SHA-256 hash razgovora rezultirao je hashevima iste duljine, iako je naslov mnogo manji od teksta njihova razgovora.

SHA-256 hash naslova knjige i SHA-256 hash razgovora rezultirao je hashevima iste duljine, iako je naslov mnogo manji od teksta njihova razgovora. U situaciji kada bi razgovor bio zamijenjen svim Doyleovim djelima, duljina hasheva bi i dalje bila ista. Ovdje je važno napomenuti kako bez obzira na veličinu ulaza – naslova knjige ili razgovora, hash funkcija uvijek rezultira izlazom fiksne veličine.

2.6.13 Generiranje hash-a

Posebnost bitcoina je da se prilikom izračuna hasha izračunava dva puta. Primjer dvostrukog SHA.256 hashiranja prikazan je u nastavku:

```

„pozdrav“; „hello“
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
prvi krug SHA256
9595c9df90075148eb06860365df33584b75bff782a510c6cd4883a419833d50

```

U ovom primjeru, originalni tekst prolazi kroz hash funkciju prvog kruga, dok hash funkcija drugog kruga koristi hash generiran u prvom krugu kao ulaz. Izrada Merkle stabla koje vodi do dobivanja Merkle korijena i generiranje hasha blokovske glave u Bitcoin protokolu slijede ovaj postupak.

SHA-2

SHA-2 (Secure Hash Algorithm 2), od kojega je SHA-256 dio, jedan je od najpopularnijih algoritama za hashiranje, a dizajniran je od strane NSA (Nacionalne sigurnosne agencije). SHA-2 algoritam je otvorenog koda te je poznat po svojoj sigurnosti (nije se rušio kao SHA-1) i brzini. U slučajevima gdje se ne generiraju ključevi, kao što je rudarenje bitcoina, brzi algoritam za hashiranje poput SHA-2 često dominira. SHA-256 generira sažetak od 256 bita (32 bajta).

SHA-2 vs. SHA-256

SHA-2 je algoritam, općenita ideja kako hashirati podatke. SHA-256 postavlja dodatne konstante koje definiraju ponašanje SHA-2 algoritma. Jedna takva konstanta je veličina izlaznog stringa. U SHA-256, "256" odnosi se na odgovarajuću veličinu izlaznog stringa u bitovima.

Upotreba SHA-256

SHA-256 se često koristi, brza je i sigurna funkcija sažimanja, a neki od najčešćih načina na koji se koriste su sljedeći:

- stvaranje autentikacijskih shema web stranica,
- stvaranje digitalnih potpisa,
- osiguravanje tehnologije ulančanih blokova,
- u antivirusnim programima, za usporedbu otisaka prstiju datoteka i programa,
- u sustavima za kontrolu – provjera je li došlo do promijene podataka

U sljedećem će se primjeru, za one koji žele znati više, razložiti svaki korak algoritma što je jednostavnije moguće i proći kroz stvarni primjer ručno. Primjer je preuzet s [12].

Primjer SHA-256:

SHA-256 „hello world“ („pozdrav svijete“); **Korak 1 - predobrada**

U prvom koraku je potrebno „hello world“ pretvoriti u binarni oblik:

```

01101000 01100101 01101100 01101100 01101111 00100000 01110111
01101111
01110010 01101100 01100100

```

a zatim treba dodati jednu jedinicu (1)

```
01101000 01100101 01101100 01101100 01101111 00100000 01110111
01101111
01110010 01101100 01100100 1
```

Zatim je nužno dodati nule (0) da podaci postanu višekratnik od 512, smanjen za 64 bita (448 bita u ovom slučaju):

```
01101000 01100101 01101100 01101100 01101111 00100000 01110111
01101111
01110010 01101100 01100100 10000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
```

Posljednje se mora dodati 64 bita, gdje su ti bitovi broj koji predstavlja dužinu originalnog unosa u binarnom obliku. U ovom slučaju 88, ili u binarnom obliku "1011000".

```
01101000 01100101 01101100 01101100 01101111 00100000 01110111
01101111
01110010 01101100 01100100 10000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
01011000
```

Sada je stvoren unos, koji će uvijek biti ravnomjerno djeljiv s 512.

Korak 2 – Inicijalizacija vrijednosti hasha (h)

U koraku 2 potrebno je stvoriti 8 hash vrijednosti. To su konstante koje predstavljaju prvih 32 bita decimalnih dijelova korijena brojeva 2,3,5,7,11,13,17,19.


```
h0 := 0x6a09e667
h1 := 0xbb67ae85
h2 := 0x3c6ef372
h3 := 0xa54ff53a
h4 := 0x510e527f
h5 := 0x9b05688c
h6 := 0x1f83d9ab
h7 := 0x5be0cd19
```

Korak 3 – Inicijalizacija Konstanti Kruga (k)

Kao u koraku 2, i u koraku tri je potrebno stvoriti određene konstante. Ovog puta ih ima 64. Svaka vrijednost (0-63) predstavlja prva 32 bita decimalnih dijelova korijena kubova prvih 64 prostih brojeva (2-311).

```
0x428a2f98 0x71374491 0xb5c0fbcf 0xe9b5dba5 0x3956c25b 0x59f111f1
0x923f82a4 0xab1c5ed5
0xd807aa98 0x12835b01 0x243185be 0x550c7dc3 0x72be5d74 0x80deb1fe
0x9bdc06a7 0xc19bf174
0xe49b69c1 0xefbe4786 0x0fc19dc6 0x240ca1cc 0x2de92c6f 0x4a7484aa
0x5cb0a9dc 0x76f988da
0x983e5152 0xa831c66d 0xb00327c8 0xbf597fc7 0xc6e00bf3 0xd5a79147
0x06ca6351 0x14292967
0x27b70a85 0x2e1b2138 0x4d2c6dfc 0x53380d13 0x650a7354 0x766a0abb
0x81c2c92e 0x92722c85
0xa2bfe8a1 0xa81a664b 0xc24b8b70 0xc76c51a3 0xd192e819 0xd6990624
0xf40e3585 0x106aa070
0x19a4c116 0x1e376c08 0x2748774c 0x34b0bcb5 0x391c0cb3 0x4ed8aa4a
0x5b9cca4f 0x682e6ff3
0x748f82ee 0x78a5636f 0x84c87814 0x8cc70208 0x90befffa 0xa4506ceb
0xbef9a3f7 0xc67178f2
```

Korak 4 — Petlja za blokove

Sljedeći koraci će se dogoditi za svaki 512-bitni "blok" podataka iz ranijeg unosa. U ovom slučaju, jer je "hello world" tako kratak, postoji samo jedan blok. Pri svakom prolasku kroz petlju, doći će do promjene vrijednosti hasha h0-h7, koje će biti konačni izlaz.

Korak 5 — Stvaranje poruke u rasporedu (w)

Korak 5 predstavlja kopiranje podatka unosa iz koraka 1 u novi niz gdje je svaki unos 32-bitna riječ:

[illegible]

Zatim se dodaju još 48 riječi inicijaliziranih na nulu, tako da postoji niz $w[0 \dots 63]$.

[illegible]

Iduće je potrebno izmijeniti indekse koji su postavljeni na nulu na kraju niza koristeći sljedeći algoritam:

```

Za i od w[16] For i from w[16...63]: s0 = (w[i-15] rightrotate 7) xor (w[i-15] rightrotate
18) xor (w[i-15] rightshift 3) s1 = (w[i-2] rightrotate 17) xor (w[i-2] rightrotate 19) xor
(w[i-2] rightshift 10) w[i] = w[i-16] + s0 + w[i-7] + s1...63]:

```

Ovdje će isto biti napravljeno sa w[16] kako bi bio prikazan princip rada:

```

w[1] rightrotate 7:
01101111001000000111011101101111 → 11011110110111100100000011101110
w[1] rightrotate 18:
01101111001000000111011101101111 → 00011101110110111101101111001000
w[1] rightshift 3:
01101111001000000111011101101111 → 00001101111001000000111011101101
s0=11011110110111100100000011101110 XOR 00011101110110111101101111001000 XOR
00001101111001000000111011101101
s0=11001110111000011001010111001011
w[14] rightrotate 17:
00000000000000000000000000000000 → 00000000000000000000000000000000
w[14] rightrotate 19:
00000000000000000000000000000000 → 00000000000000000000000000000000
w[14] rightshift 10:
00000000000000000000000000000000 → 00000000000000000000000000000000
s1=00000000000000000000000000000000 XOR 00000000000000000000000000000000 XOR
00000000000000000000000000000000
s1=00000000000000000000000000000000
w[16] = w[0] + s 0 + w[9] + s1
w[16] = 01101000011001010110110001101100 + 11001110111000011001010111001011 +
00000000000000000000000000000000 + 00000000000000000000000000000000
// addition is calculated modulo 232
w[16] = 00110111010001110000001000110111

```

Ostaje 64 riječi u rasporedu poruke (w):

```

01101000011001010110110001101100 01101111001000000111011101101111
01110010011011000110010010000000 00000000000000000000000000000000
00000000000000000000000000000000 00000000000000000000000000000000
00000000000000000000000000000000 00000000000000000000000000000000
00000000000000000000000000000000 00000000000000000000000000000000
00000000000000000000000000000000 00000000000000000000000000000000
00000000000000000000000000000000 00000000000000000000000000000000
00000000000000000000000000000000 00000000000000000000000000000000
00000000000000000000000000000000 00000000000000000000000000000000
0011011101000111000001000110111 100011011010000110000000110001
1101001101111010001000100001011 0111100000111110100011110000010
00101010100100000111110011101101 01001011001011110111110011001001
00110001111000011001010001011101 10001001001101100100100101100100
0111111011110100000011011011010 11000001011110011010100100111010
10111011111010001111011001010101 00001100000110101110001111100110
1011000011111100000110101111101 01011111011011100101010110010011
00000000100010011001101101010010 00000111111100011100101010010100
0011101101011111110010111010110 01101000011001010110001011100110
11001000010011100000101010011110 00000110101011111001101100100101
10010010111011110110010011010111 01100011111110010101111001011010
11100011000101100110011111010111 10000100001110111101111000010110
11101110111011001010100001011011 10100000010011111111001000100001
11111001000110001010110110111000 00010100101010001001001000011001
00010000100001000101001100011101 01100000100100111110000011001101
10000011000000110101111111101001 11010101101011100111100100111000
00111001001111110000010110101101 11111011010010110001101111101111
11101011011101011111111100101001 01101010001101101001010100110100
00100010111111001001110011011000 10101001011101000000110100101011
01100000110011110011100010000101 11000100101011001001100000111010
00010001010000101111110110101101 10110000101100000001110111011001
10011000111100001100001101101111 01110010000101111011100000011110
10100010110101000110011110011010 00000001000011111001100101111011
11111100000101110100111100001010 11000010110000101110101100010110

```

Korak 6 — Kompresija

U koraku 6 se inicijaliziraju varijable *a*, *b*, *c*, *d*, *e*, *f*, *g*, *h* i koje se postavljaju da budu jednake trenutnim vrijednostima hasha, redom *h0*, *h1*, *h2*, *h3*, *h4*, *h5*, *h6*, *h7*. Zatim se pokreće petlju kompresije. Petlja kompresije će mijenjati vrijednosti *a*...*h*. Petlja kompresije ide ovako:

```

1  for i from 0 to 63
2  S1 = (e rightrotate 6) xor (e rightrotate 11) xor (e
    rightrotate 25)
3  ch = (e and f) xor ((not e) and g)
4  temp1 = h + S1 + ch + k[i] + w[i]
5  S0 = (a rightrotate 2) xor (a rightrotate 13) xor (a
    rightrotate 22)
6  maj = (a and b) xor (a and c) xor (b and c)
7  temp2 := S0 + maj
8  h = g
9  g = f
10 e = d + temp1
11 d = c
12 c = b
13 b = a

```

```
14 a = temp1 + temp2
```

Primjer koda 2.1: *Petlja kompresije*

Koraci kroz prvu iteraciju, gdje se svi zbrojevi računaju modulo 2^{32} :

```
a=0x6a09e667=01101010000010011110011001100111
b=0xbb67ae85=10111011011001111010111010000101
c=0x3c6ef372=00111100011011101111001101110010
d=0xa54ff53a=10100101010011111111010100111010
e=0x510e527f=01010001000011100101001001111111
f=0x9b05688c=10011011000001010110100010001100
g=0x1f83d9ab=00011111100000111101100110101011
h=0x5be0cd19=01011011111000001100110100011001
e rightrotate 6:
01010001000011100101001001111111 → 11111101010001000011100101001001
e rightrotate 11:
01010001000011100101001001111111 → 01001111111010100010000111001010
e rightrotate 25:
01010001000011100101001001111111 → 10000111001010010011111110101000
S1=11111101010001000011100101001001 XOR 01001111111010100010000111001010 XOR
10000111001010010011111110101000
S1=00110101100001110010011100101011

e and f:
01010001000011100101001001111111
& 10011011000001010110100010001100 =
00010001000001000100000000001100
not e:
01010001000011100101001001111111 → 10101110111100011010110110000000
(not e) and g:
10101110111100011010110110000000
& 00011111100000111101100110101011 =
00001110100000011000100110000000
ch = (e and f) xor ((not e) and g)
= 00010001000001000100000000001100 XOR 00001110100000011000100110000000
= 00011111100001011100100110001100
// k[i] is the round constant
// w[i] is the batch
temp1 = h + S1 + ch + k[i] + w[i]
temp1 = 01011011111000001100110100011001 + 00110101100001110010011100101011
+ 00011111100001011100100110001100 + 1000010100010100010111110011000 +
01101000011001010110110001101100
temp1 = 01011011110111010101100111010100
```

```

temp2 = S0 + maj
= 11001110001000001011010001111110 + 00111010011011111110011001100111
= 00001000100100001001101011100101
h = 00011111100000111101100110101011
g = 10011011000001010110100010001100
f = 01010001000011100101001001111111
e = 10100101010011111111010100111010 + 01011011110111010101100111010100
= 00000001001011010100111100001110
d = 00111100011011101111001101110010
c = 10111011011001111010111010000101
b = 01101010000010011110011001100111
a = 01011011110111010101100111010100 + 00001000100100001001101011100101
= 01100100011011011111010010111001

```

a rightrotate 2:

01101010000010011110011001100111 → 11011010100000100111100110011001

a rightrotate 13:

01101010000010011110011001100111 → 00110011001110110101000001001111

a rightrotate 22:

01101010000010011110011001100111 → 00100111100110011001110110101000

S0 = 11011010100000100111100110011001 XOR 00110011001110110101000001001111 XOR
00100111100110011001110110101000

S0 = 11001110001000001011010001111110

a and b:

01101010000010011110011001100111

& 10111011011001111010111010000101 =

00101010000000011010011000000101

a and c:

01101010000010011110011001100111

& 00111100011011101111001101110010 =

00101000000010001110001001100010

b and c:

10111011011001111010111010000101

& 00111100011011101111001101110010 =

00111000011001101010001000000000

maj = (a and b) XOR (a and c) XOR (b and c)

= 00101010000000011010011000000101 XOR 00101000000010001110001001100010 XOR
00111000011001101010001000000000

= 00111010011011111110011001100111

Cijeli taj izračun se ponavlja još 63 puta, mijenjajući varijable a-h tijekom cijelog procesa. Taj dio neće biti rađen ručno, ali na kraju bi bilo dobiveno sljedeće:

```

h0 = 6A09E667 = 01101010000010011110011001100111
h1 = BB67AE85 = 10111011011001111010111010000101
h2 = 3C6EF372 = 00111100011011101111001101110010
h3 = A54FF53A = 10100101010011111111010100111010
h4 = 510E527F = 01010001000011100101001001111111
h5 = 9B05688C = 10011011000001010110100010001100
h6 = 1F83D9AB = 00011111100000111101100110101011
h7 = 5BE0CD19 = 01011011111000001100110100011001

```

```

a = 4F434152 = 001001111010000110100000101010010
b = D7E58F83 = 011010111111001011000111110000011
c = 68BF5F65 = 001101000101111110101111101100101
d = 352DB6C0 = 000110101001011011011011011000000
e = 73769D64 = 001110011011101101001110101100100
f = DF4E1862 = 011011111010011100001100001100010
g = 71051E01 = 0011100010000010100011111000000001
h = 870F00D0 = 010000111000011110000000011010000

```

Korak 7 – Modificiranje konačnih vrijednosti

Nakon petlje kompresije, ali još uvijek unutar petlje za blokove, mijenjaju se vrijednosti hash-a dodavanjem njihovih odgovarajućih varijabli, a-h. Kao i obično, sva zbrajanja su modulo 2^{32} .

```

h0 = h0 + a = 10111001010011010010011110111001
h1 = h1 + b = 10010011010011010011111000001000
h2 = h2 + c = 10100101001011100101001011010111
h3 = h3 + d = 11011010011111011010101111111010
h4 = h4 + e = 1100010010000100111011111100011
h5 = h5 + f = 01111010010100111000000011101110
h6 = h6 + g = 10010000100010001111011110101100
h7 = h7 + h = 11100010111011111100110111101001

```

Korak 8 – Spajanje konačnog hash-a

U posljednjem je koraku potrebno spojiti sve zajedno kako bi se dobilo sljedeće:

```

digest = h0 append h1 append h2 append h3 append h4 append h5 append h6
        append h7=

```

B94D27B9934D3E08A52E52D7DA7DABFAC484EFE37A5380EE9088F7ACE2EFCDE9

2.7 Digitalni potpis

Digitalni potpis je kriptografski ekvivalent ručnom potpisu i koristi se za potvrdu autentičnosti, integriteta i nenijekanja poruka ili dokumenata prenesenih digitalnim putem. Valjan digitalni potpis omogućuje da:

- primatelj potpisane poruke može potvrditi da poslana poruka nije pristigla od strane prevaranta – osigurava autentičnost,
- poruka ne bude manipulirana, odnosno da poruka tijekom prijenosa nije promijenjena – potvrđuje integritet,
- sprječi pošiljatelja da porekne slanje poruke – ukazuje na nenijekanje.

Digitalni potpis i ključno vezano uz njega – autentičnost, integritet i nenijekanje, još je jedno bitno kriptografsko načelo koje se koristi u izradi kriptovaluta i tehnologije ulančanih blokova.

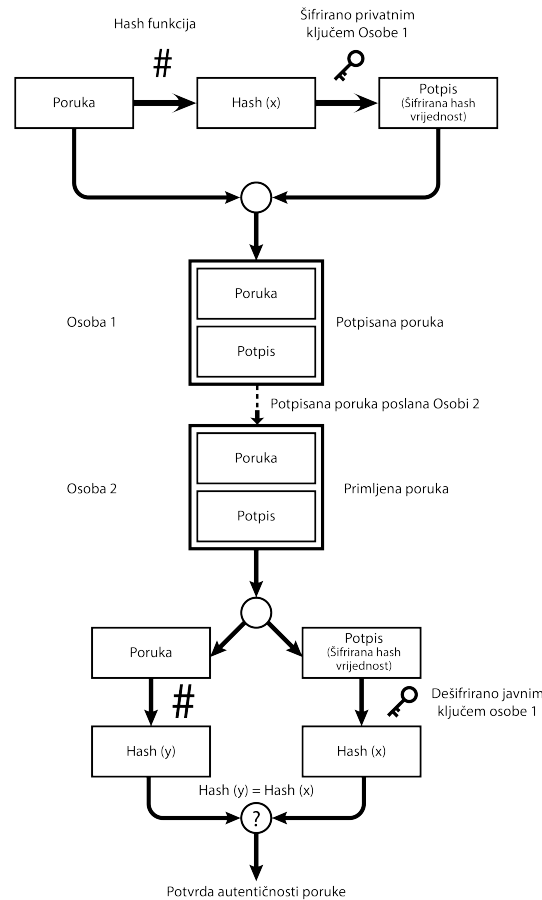
Obično digitalni potpis koristi potpisnik koji generira par privatnih i javnih ključeva, a zatim objavljuje svoj javni ključ sa pretpostavkom da će ga provjeritelj imati ili ga može dobiti prilikom provjere. Kada se javni ključ potpisnika utvrdi, digitalni potpis omogućuje potpisniku da potpiše ili certificira poruku na način da bilo koja druga strana koja poznaje potpisnikov javni ključ, i odgovarajući algoritam, može provjeriti da poruka potječe od potpisnika i da je nitko nije mijenjao u procesu slanja.

Jednostavnije rečeno, ključni parovi u kriptografiji s javnim ključem su komplementarni i mogu se učinkovito zamijeniti. Za normalno šifriranje - dešifriranje, javni ključ koristi se za šifriranje, a privatni ključ za dešifriranje. Ako se umjesto toga privatni ključ koristi za šifriranje, tada se rezultat može dešifrirati samo pomoću odgovarajućeg javnog ključa.

Mogućnost takvog koncepta opisana je prvi puta 1976. godine (Whitfield Diffie i Martin Hellman), prije izuma kriptografije s javnim ključem. Kasnije, kada je RSA (prvi poznati kriptosustav s javnim ključem - Ron Rivest, Adi Shamir i Leonard Adleman) postao dostupan, otvoren je put da digitalni potpis postane stvarnost. U nastavku navedeni primjer prikazuje korake jednostavnog RSA i potpisa temeljenog na hashu.

Neka se pretpostavi da Osoba 1 želi poslati poruku Osobi 2 koristeći RSA temeljen digitalni potpis, kako je prikazano na slici 8. Osoba 1 morala bi proći kroz sljedeće korake:

1. osoba 1 generira hash vrijednost poruke;
2. osoba 1 šifrira hash vrijednost koristeći svoj privatni ključ. Šifrirana hash vrijednost može se dešifrirati samo njegovim javnim ključem; stoga djeluje kao njegov potpis;
3. osoba 1 dodaje svoj potpis na dno izvorne poruke i šalje je Osobi 2 putem digitalnog komunikacijskog medija;
4. primivši poruku, Osoba 2 izvodi dva zadatka: prvo, dešifrira potpis Osobe 1 koristeći njezin javni ključ kako bi dobila hash vrijednost, a drugo, stvara hash vrijednost za izvornu poslanu poruku.
5. usporedbom dviju hash vrijednosti, Osoba 2 može potvrditi autentičnost poruke. Naime, ako netko u sredini promijeni poruku, nova hash vrijednost bit će različita od one pohranjene u potpisu Osobe 1. Zbog toga što je taj potpis šifriran, treća osoba ne bi mogla promijeniti potpis, ili bi svaki pokušaj modifikacije rezultirao oštećenim potpisom koji više nije moguće dešifrirati pomoću javnog ključa Osobe 1, otkrivajući tako nastale promjene.



Slika 2.8: *Primjer koraka u digitalnom potpisu*

2.7.1 Algoritam digitalnog potpisa s eliptičnom krivuljom - ECDSA

Postoji nekoliko algoritama digitalnog potpisa, od kojih Bitcoin koristi algoritam digitalnog potpisa s eliptičnom krivuljom (ECDSA – eng. *Elliptic Curve Digital Signature Algorithm*), čija je matematika prilično složena te iz tog razloga neće biti detaljno opisana u ovom priručniku. Temelj ECDSA-e leži u kriptografiji eliptičnih krivulja. Ovaj algoritam složeniji je od uobičajnijeg RSA kriptosustava s javnim ključem, ali se smatra sigurnijim za određenu duljinu ključa.

2.7.2 Kriptografija eliptičnih krivulja – ECC – Elliptic Curve Cryptography

ECC, ili kriptografija s eliptičnim krivuljama, je proces šifriranja podataka korištenjem javno dostupnih informacija, omogućujući dešifriranje samo određenoj osobi ili skupini ljudi koji posjeduju određene tajne. Stoga, ECC čini javni kriptosustav. Postoji mnogo kriptografskih tehnika u upotrebi, kao što su RSA i Diffie–Hellman (DH). Za razliku od RSA i DH, ECC je znatno složeniji i sigurniji.

2.8 Tehnologija ulančanih blokova (eng. *Blockchain*)

Iako je blockchain prvootno koncipiran za olakšavanje bitcoin transakcija, njegov potencijal seže daleko izvan okvira virtualnih valuta. Stručnjaci već sada smatraju ovu tehnologiju revolucionarnom, predviđajući da će promijeniti temelje mnogih postojećih industrija koje trenutno operiraju na sasvim drugačijim osnovama.

Opis tehnologije ulančanih blokova

Blockchain je nepromjenjivi javni registar za zapisivanje transakcija. Transakcije nazivamo "nepromjenjivima" jer, kada su jednom unesene, postaju trajne i ne mogu se retroaktivno mijenjati, čak ni od strane autora, bez promjene svih kasnijih transakcija. Formalna definicija blockchaina može se izraziti kao: „Blockchain je nepromjenjivi distribuirani registar osiguran kriptografskim tehnikama i upravljan od strane decentralizirane zajednice putem P2P mreže poticanjem“.

Tehnologija blockchaina koristi sigurnosne uređaje koji su znatno snažniji od onih u običnim računalnim datotekama.

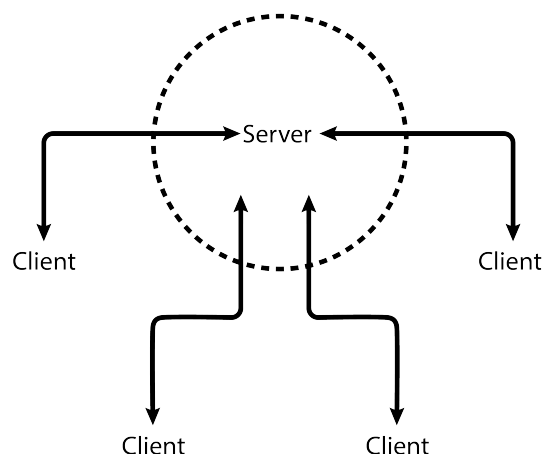
2.8.1 Ključna svojstva – četiri stupa tehnologije ulančanih blokova

1. decentralizacija (eng. *Decentralized*)
2. nepromjenjivost (eng. *Immutable*)
3. transparentnost (eng. *Transparent*)
4. sigurnost (eng. *Secure*)

Decentralizacija

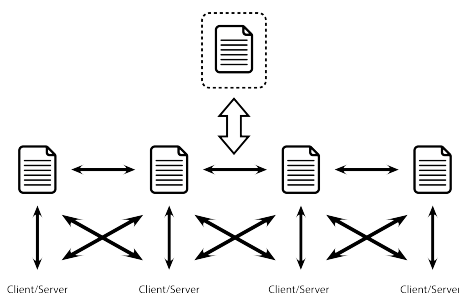
Centralizirana vs. decentralizirana arhitektura

Kako je i ranije opisano, na prvi pogled, tehnologija ulančanih blokova ne razlikuje se znatno od tehnologija web stranica ili aplikacija na pametnim telefonima, ali te razlike postaju primjetne u analizi arhitekture. Spomenute web stranice i aplikacije su dio centralizirane strukture u kojoj postoji centralni server, odnosno imaju arhitekturu poznatu kao klijent – poslužitelj (primatelj – davatelj), što je prikazano na slici 2.9.



Slika 2.9: Centralizirana klijent-server arhitektura u kojoj server ima apsolutnu moć pružanja ili uskraćivanja bilo koje usluge i podataka

S druge strane, blockchain (tehnologija ulančanih blokova) ima drugačiju arhitekturu, onu decentraliziranu (Slika 2.10). Ova arhitektura znatno se razlikuje od arhitekture klijent-poslužitelj, jer ovdje svaki sudjelujući čvor u ovoj arhitekturi djeluje kao klijent i poslužitelj, eliminirajući potrebu za centralnim autoritetom. Ovaj tip mreže naziva se peer-to-peer mreža, već ranije opisana, ili jednostavno P2P mreža. Blockchain prihvaća ovu mrežu kao svoj temeljni okvir za komunikaciju i operacije kako bi postigao niz ciljeva koji su temeljni za ovu tehnologiju.



Slika 2.10: *Decentralizirana struktura gdje svaki sudjelujući čvor istovremeno djeluje i kao poslužitelj (Server) i kao klijent (Client)*

Nepromjenjivost

Blockchain je nepromjenjiv javni registar za zabilježavanje transakcija. Transakcije nazivamo 'nepromjenjivima', jer nakon što su upisane ne mogu se modificirati ili brisati, čak ni od strane autora transakcije, bez izmjene svih kasnijih transakcija.

Transparentnost

Datoteke i transakcije na blockchainu su dostupne svima, javne su, te su pohranjene na više računala unutar mreže, a ne na jednom mjestu. Takav način pohrane omogućuje da bude čitljiv za sve korisnike, odnosno čini ga istovremeno transparentnim i teško izmjenjivim, eliminirajući slabosti koje bi mogle proizaći iz ljudskih ili IT pogrešaka.

Budući da je svaka transakcija u blockchainu provjerljiva, on stvara digitalno povjerenje. 'Otvorenost' blockchaina predstavlja i to da nema potrebe za kontrolom pristupa i lozinkama (uz pretpostavku da je blockchain javnog tipa).

Sigurnost

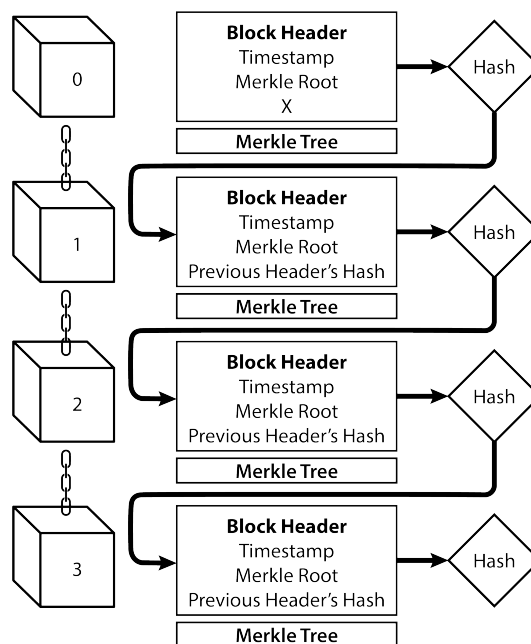
Tehnologija ulančanih lanaca opisuje se kao sigurna po dizajnu. Kao otvoren, decentraliziran sustav, blockchain ne zahtijeva posebnu zaštitu podataka od napada, jer su podaci već otvoreni i nema svrhe za manipulaciju njima jer će svaka takva promjena brzo biti ignorirana.

2.8.2 Konstrukcija lanca u tehnologiji ulančanih blokova

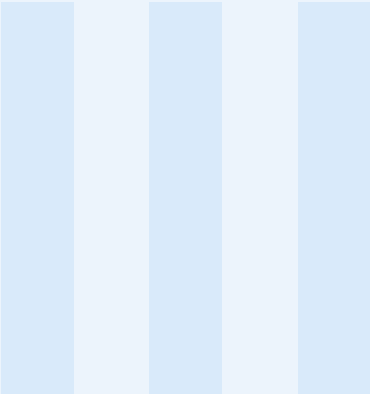
U tehnologiji ulančanih blokova, *genesis blok*, koji je ujedno i prvi blok lanca (slika 2.11), predstavlja poseban slučaj jer nema referencu na svoj prethodni blok – svaki drugi blok povezan je kriptografskim principima. *Genesis* blok gotovo je uvijek ugrađen u softveru aplikacija koje koriste tehnologiju ulančanih blokova.

Blockchain koristi dva elementa za povezivanje blokova. Prvi je Merkle korijen (eng. *Merkle root*) koji predstavlja sve transakcije bloka u hashiranom formatu. Svaki pokušaj

promjene jedne transakcije u listu stabla rezultirao bi novim Merkle korijenom otkrivajući promjenu. Drugi element je hash zaglavlje prethodnog bloka. Budući da je Merkle korijen dio tog zaglavlja, njegov hash učinkovito povezuje transakcije u mehanizmu povezivanja. Na kraju, hash zaglavlje prethodnog bloka smješta se u zaglavlje sljedećeg bloka kako bi se završilo povezivanje dva uzastopna bloka. Svaki put kada rudari putem rudarenja izgrade blok, što će biti detaljnije objašnjeno u četvrtom poglavlju, stavljaju ga na kraj ovog lanca; stoga lanac neprestano raste.



Slika 2.11: Svaki blok u lancu blokova povezan je jedan s drugim pomoću kriptografskih hashova. Stavljanje hash-a zaglavlja prethodnog bloka u zaglavlje sljedećeg bloka, koji također sadrži Merkleov korijen, stvara ultimativnu vezu za razvoj cijelog lanca.



Treći dio

3	Blockchain tehnologija ≠ kriptovalute 65
3.1	Blockchain više je od kriptovalute
3.2	Pregled primjene Blockchain tehnologije
3.3	Upravljanje lancima opskrbe
3.4	Decentralizirane financije
3.5	Preoblikovanje financijskih eko-sustava
3.6	Postoji li najbolji blockchain sustav za DeFi?
3.7	Cardano
3.8	Byron: Temeljni razvoj
3.9	Shelly: Decentralizacija kontrole
3.10	Gougen: era pametnih ugovora
3.11	Basho: skaliranje
3.12	Voltaire - Upravljanje
3.13	ADA - token Cardano mreže
3.14	Polkadot
3.15	Paralelni lanci blokova
3.16	Substrate - razvojno okruženje za Polkadot blockchain
3.17	Kusama - platforma za istraživanje i razvoj
3.18	Hyperledger Blockchain
3.19	Hyperledger Fabric
3.20	Fabric pametni ugovori - ChainCode
3.21	Sastavni dijelovi Hyperledger Fabric sustava
3.22	Hyperledger Sawtooth
3.23	Blockchain podrazumijeva transparentno poslovanje



3. Blockchain tehnologija ≠ kriptovalute

3.1 Blockchain više je od kriptovalute

Tehnološki napredak računarstva u protekla tri desetljeća odvijao se nevjerojatnom brzinom te se web preobrazio od onog prvotnog koji služi samo za čitanje do društvenog, participativnog weba 2.0 i konačno do weba 3.0 koji zarađuje svojim korisnicima za sudjelovanje u eko-sustavu. Blockchain tehnologija postala je revolucionarno otkriće sa širokim učincima na tržištu web 3.0 koje se stalno mijenja. Blockchain se često povezuje s kriptovalutama poput bitcoina, ali utjecaj ove tehnologije daleko nadilazi svijet financija. Ovo poglavlje će ispitati primjene ove decentralizirane tehnologije izvan bitcoin eko-sustava, dajući pri tome predodžbu o njezinim gotovo neograničenim mogućnostima integracije.

3.2 Pregled primjene Blockchain tehnologije

Prije samog pregleda upotrebe blockchain tehnologije, potrebno je proučiti osnovne značajke koje ju čine posebnom. Blockchain je u svojoj suštini distribuirana knjiga (baza podataka) koja bilježi transakcije na nekoliko računala. Nudi matematički garantiranu nepromjenjivost podataka koje čuva, sigurnost pohrane i transparentnost informacija. Blockchain se koristi u širokom rasponu industrija, uključujući opskrbe lance, zdravstvo, glasačke sustave, internet stvari, kibernetičku sigurnost, intelektualno vlasništvo i još mnogo toga, a najpoznatija primjena je područje kriptovaluta.

Blockchain tehnologija može ostvariti vanserijsku sigurnost i šifriranje medicinskih podataka, pružajući pojedincima potpunu kontrolu nad njihovim osobnim zdravstvenim podacima. Visoki stupanj pseudonimnosti i anonimnosti rezultira sigurnijom manipulacijom podataka i manjim troškovima njihove obrade.

Politički izbori koji su pouzdani, transparentni i zaštićeni od malverzacija mogu se ostvariti sustavima glasanja temeljenim na blockchain tehnologiji. Nepromjenjiva knjiga zapisa nazvana blockchain se može koristiti za bolju zaštitu prava intelektualnog vlasništva,

olakšavajući administriranje i provedbu zaštitnih žigova, autorskih prava i патената.

Osim toga, blockchain pruža primjenjive odgovore na ključne izazove s kojima se suočavaju financijska i bankarska industrija - fintech, posebno kada je riječ o sprječavanju prijevara i pranja novca (*eng. Anti Money Laundering - AML*). Korištenje blockchain tehnologije u bankarstvu stvara snažnu obranu od malicioznih napada hakera koji pokušavaju kompromitirati sustav i ubaciti svoje podatke. Pomoću ove tehnologije podaci se matematički kombiniraju u distribuiranu knjigu, a svaka transakcija dobiva vremensku oznaku i povezuje se s drugim blokovima. Obrana informatičkog sustava od pokušaja upada ojačana je vremenskim oznakama i jedinstvenim matematičkim otiskom svake informacije. Dodatno, blockchain smanjuje troškove postupka identifikacije korisnika (*eng. Know your customer – KYC*) za banke i ostale financijske institucije, što uvelike smanjuje učestalost pranja novca i distancira sumnjive pojedince podalje od bankarskog sektora.

3.3 Upravljanje lancima opskrbe

Blockchain značajno utječe na upravljanje opskrbnim lancima. Poduzeća sve više i više koriste blockchain za pažljivo praćenje i provjeru svake faze putovanja proizvoda. Time se tržište održava transparentnim i sprječava se ulazak krivotvorene robe. Blockchain poboljšava transparentnost opskrbnog lanca i povjerenje, što pomaže sektorima poput proizvodnje odjeće, hrane i lijekova. Vodeće tvrtke u sektoru, poput Walmarta, Coca-Cole, Forda, Nestléa i mnogih drugih, usvojile su blockchain tehnologiju kako bi poboljšale svoje aktivnosti upravljanja nabavom.

Na primjer, Walmart i IBM su 2018. najavili strateško partnerstvo za korištenje blockchain tehnologije za poboljšanje sljedivosti Walmartova lanca opskrbe hranom. Na sličan način, Ford, poznati proizvođač automobila, surađivao je s IBM-om tijekom covid pandemije kako bi koristio blockchain tehnologiju za praćenje izvora kobalta, bitne komponente njegovih baterija za električna vozila.

Danas je kupcima lako saznati odakle proizvodi dolaze i jesu li etički izrađeni što povećava otvorenost i pristup informacija te ima mogućnost promijeniti očekivanja potrošača i povećati povjerenje u brojnim industrijama.

Često je nemoguće identificirati pogreške u obradi podataka u stvarnom vremenu, kao što su pogreške u podacima o zalihama, pošiljke koje nedostaju i dvostruka plaćanja. Čak i kada se problem otkrije naknadno, praćenje slijeda događaja dokumentiranih u dostupnim unosima i dokumentima u glavnoj knjizi je dugotrajan i skup način za utvrđivanje uzroka pogreške i rješavanja iste. Identificiranje unosa u dnevnik (potraživanja, plaćanja, krediti za povrat, itd.) koji odgovaraju kojoj transakciji zaliha može biti izazov, iako moderni ERP sustavi pohranjuju sve vrste tokova novca i informacija. To posebno vrijedi za tvrtke koje prov

Ne pomaže niti činjenica da su radnje opskrbnog lanca često izuzetno složene, mnogo više nego što se može pomisliti na prvu. Narudžbe, pošiljke i plaćanja, na primjer, možda se neće savršeno uskladiti ako je narudžba podijeljena na nekoliko isporuka i povezanih faktura ili ako je nekoliko narudžbi spojeno u jednu isporuku.

Revizije, interne ili vanjske, su uobičajeni način provjere transakcija u opskrbnom lancu i poboljšanja poslovnih procesa. Iako je revizija ključna kako bi se osiguralo poštivanje odredbi ugovara, nije od velike pomoći u rješavanju operativnih nedostataka putem informiranog donošenja odluka. Revizija ili pregled inventara u trgovini može pokazati koliko

je artikala istekao, ali ne može dati objašnjenje zašto. Blockchain tehnologija može pružiti prave uvezane informacije iz kojih je moguće zaključiti o uzrocima poremećaja. Prema Walmartovom saznanju, uzroci poremećaja mogu uključivati nedostatke u bilo kojoj fazi opskrbnog lanca, kao što je neadekvatna rotacija polica (nemogućnost premještanja starijih proizvoda i zamjena novijima), slaba ili neredovita potražnja i neučinkovito uzvodno upravljanje zalihama. Praćenje svake poduzete radnje može pomoći u smanjenju isteka, a automatizacija poslovnog procesa koji se temelji na blockchain tehnologiji može gotovo izuzeti određene poteškoće iz spektra događaja. Isto izvješće upućuje na korištenje RFID oznaka ili elektroničkih kodova proizvoda koji slijede standarde GS1 — skup međunarodno priznatih smjernica za rukovanje podacima o opskrbnom lancu — za označavanje zaliha i integraciju u ERP sustav organizacije, umrežavanje s dobavljačima za stvaranje sveobuhvatne evidencije transakcija te razvoj metoda za povećanje pouzdanosti ulančanih poslovnih aktivnosti. U svakom poslovnom proces se integracijom blockchain tehnologije poboljšava sljedivost i eliminira se greška u izvršenju ponavljajućih zadataka. Međutim, integracija ERP sustava sa novom tehnologijom je najčešće skupa i dugotrajna. Zbog organizacijskih promjena, spajanja i akvizicija tijekom vremena, velike organizacije mogu imati više od 100 naslijeđenih ERP sustava. Ovi sustavi mogu čak različito definirati podatkovna polja jedna od drugih i često imaju poteškoća u međusobnoj komunikaciji.

Vođenje evidencije o dobavljačima i kupcima u blockchainu dodjeljuje jedinstvene identifikatore imovini kao što su teretnice, narudžbe, inventarne jedinice i zajmovi; ti identifikatori funkcioniraju kao digitalni tokeni, slično bitcoin tokenima. Osim toga, svaka osoba koja doprinosi blockchainu dobiva jedinstveni identifikator, poznat i kao digitalni potpis, koji koristi za potpisivanje novih blokova. Odgovarajući token se zatim prenosi s jednog sudionika na drugog, pri čemu se svaka faza transakcije dokumentira na blockchainu.

Primjerice, narudžbu najprije kreira trgovac i šalje je dobavljaču. U ovom trenutku ne bi bilo unosa u financijskoj knjizi jer nije bilo razmjene dobara ili usluga. S blockchain tehnologijom, s druge strane, trgovac prati digitalni token narudžbe. Nakon toga dobavljač zapisuje narudžbu i obavještava trgovca da je zaprimljena. Ta je radnja također dokumentirana na blockchainu, ali ne rezultira unosom u financijskoj knjizi. Nakon toga, dobavljač se obraća banci za kredit za obrtni kapital kako bi financirao proizvodnju robe. Banka odobrava zajam, bilježi digitalni token zajma na istom blockchainu i provjerava nalog na zajedničkom blockchainu.

Jedan od razloga zašto je blockchain tehnologija korisna očituje se u bilježenju informacija koje se ne nalaze u sustavu financijske knjige i činjenica da su svi zapisi nanizani kao kronološki niz blokova koji integrira sva tri oblika transakcijskih tokova. Svaki blok je dodatno kriptiran prije slanja svakom sudioniku, a svaki korisnik čuva svoje kopije blockchaine. Navedena svojstva omogućuju lancu blokova da na sveobuhvatan, pouzdan i nepromjenjiv način ponudi revizijski trag za sve tri vrste aktivnosti opskrbnog lanca.

Kao rezultat toga, blockchain značajno ublažava - ako ne i potpuno iskorjenjuje - probleme izvršenja, sljedivosti i koordinacije u lancu dobave. Svaka strana može provjeriti status transakcije, uočiti pogreške i pozvati druge strane na odgovornost za svoje postupke jer svaki sudionik ima jedinstvenu kopiju blockchaine. Budući da bi to zahtijevalo ponovno pisanje svih sljedećih blokova na svim dijeljenim kopijama blockchaine, nijedan sudionik ne može prebrisati prethodno unesene podatke.

Blockchain tehnologija može pomoći banci iz prethodnog primjera učinkovitije financi-

rati opskrbni lanac. Blockchain može služiti za provjeru transakcija između dobavljača i trgovca gdje banka može jednim uvidom u blockchain eliminirati potrebu za dugotrajnim fizičkim revizijama i financijskim pregledima koji oduzimaju puno vremena i skloni su ljudskim pogreškama, a koji su neophodni za donošenje boljih odluka o kreditiranju. Dodatno, uključivanjem podataka o plaćanjima, fakturama i stvarnom kretanju robe u blockchain, transakcije mogu postati manje rizične za sve uključene strane, lakše ih je revidirati i postaju isplativije.

Štoviše, pametni ugovori, koji su zapravo računalni programi koji koriste blockchain podatke za provjeru i potvrdu ugovornih obveza, ispunjenje uvjete plaćanja te koji su uvijek spremni za izvršenje, mogu automatizirati mnoge od navedenih zadataka i koraka poslovnih procesa. Kako bi se automatski izvršilo plaćanje, zabilježili unosi u glavnu knjigu i označili iznimke koje zahtijevaju ručnu intervenciju, pametni ugovori se mogu programirati za automatsku provjeru statusa transakcija.

Prilikom razmatranja upotrebe blockchaina kao tehnologije za primjenu u lancu opskrbe, ključno je zapaziti kako blockchain teško može zauzeti mjesto ERP sustava u pogledu obrade transakcija, računovodstva i kontrole upravljanja, uključujući izvještavanje, fakturiranje i obradu plaćanja. Zapravo, učinkovita pohrana nije moguća s šifriranim povezanim popisom lanca blokova ili lančanom strukturom podataka, niti je prikladna za brzu pohranu i dohvaćanje. Umjesto toga, blockchain bi komunicirao s postojećim sustavima koje koriste pojedine tvrtke. Iz svog internog ERP sustava svaka bi tvrtka proizvodila blokove transakcija koje bi potom dodavala u blockchain. Takav pristup bi mogao pojednostaviti integraciju različitih tokova transakcija i informacija među poduzećima.

3.4 Decentralizirane financije

Sljedeća razmatrana industrija na koju utječe blockchain tehnologija su decentralizirane financije ili DeFi. DeFi platforme koriste pametne ugovore, samoizvršujuće ugovore, koji sami aktiviraju potrebne radnje kada su zadovoljeni određeni kriteriji. Takve platforme eliminiraju potrebu za konvencionalnim posrednicima nudeći pri tome korisnicima financijske usluge poput pozajmljivanja, posuđivanja i trgovanja.

DeFi promiče financijsku inkluzivnost na demokratičan i troškovno učinkovit način. Takav pristup omogućuje svakome diljem svijeta pristup financijskim uslugama bez ovisnosti o tradicionalnim bankarskim sustavima. DeFi ima potencijal preokrenuti etabliranu financijsku industriju i pružiti alternativnu smjer razvoja financijske slobode.

Postupci KYC procesa su presudni u tradicionalnim financijskim sustavima, no često su u sukobu s temeljima blockchain tehnologije koja štiti privatnost. Nasuprot tome, DeFi predstavlja noviju ideju poznatu kao Know-Your-Transaction (KYT) mehanizam. Umjesto naglašavanja identiteta korisnika, ovaj se sustav fokusira na digitalne adrese i obrasce transakcija kako bi identificirao maliciozne radnje.

Upravljanje imovinom, analitika kretanja sredstava, upravljanje rizikom, nematerijalna imovina i sve njene izvedenice, posuđivanje nepoznatim korisnicima i posuđivanje između ravnopravnih korisnika te brojne opcije plaćanja neki su od značajnih slučajeva upotrebe decentraliziranih financija.

3.5 Preoblikovanje financijskih eko-sustava

U osnovi, blockchain je tehnologija distribuirane knjige iliti distribuirane baze podataka o transakcijama, što implicira da je nekoliko kopija istog zapisa o transakciji raspršeno kroz mrežu računala umjesto da jedan zapis čuva jedno središnje tijelo. Blok se dodaje lancu kronološkim, linearnim redoslijedom nakon što je blok ispunjen transakcijama. Takav pristup promiče okruženje povjerenja te se znatno otežava petljanje ili lažiranje transakcija.

Primjene za decentraliziranu strukturu blockchaina mogu se pronaći u mnogim domenama, kao što su provjera digitalnog identiteta i upravljanje opskrbnim lancem. Ali blockchain je incijalno uzeo zalet u financijskoj industriji.

Decentralizirane financije su platforme i digitalni eko-sustavi koji nemaju svoje središnje mjesto poslovanja već funkcioniraju na otvorenim blockchain sustavima kao što su Ethereum, Binance Smart Chain i mnogi drugi. Pametni ugovori, koji su samoizvršujući ugovori s odredbama i uvjetima kodiranim u specijaliziranim programskim jezicima, glavna su komponenta koja pokreće DeFi. Ekosustav DeFi platformi i usluga, sastoji se od:

- Platforme za pozajmljivanje i posuđivanje: Decentralizirane platforme omogućuju korisnicima da posuđuju međusobno novac bez ovisnosti o bankama.
- Decentralizirane razmjene: stranice na kojima korisnici mogu međusobno izravno trgovati imovinom, zaobilazeći potrebu za centraliziranim posrednikom.
- Stablecoin: Kako bi se održala stabilnost cijena, kriptovalute su povezane s konvencionalnim valutama ili imovinom.
- Yield farming i rudarenje likvidnosti: Tehnike za generiranje nagrada pružanjem likvidnosti DeFi protokolima.
- Tržišta derivata: Platforme koje korisnicima omogućuju predviđanje cijena imovine ili događaja u budućnosti poznate su kao tržišta derivata.

3.6 Postoji li najbolji blockchain sustav za DeFi?

Nisu svi blockchain sustavi koji podržavaju DeFi aplikacije isti, iako ih ima mnogo. Blockchain koji je savršen za DeFi trebao bi imati sljedeće značajke:

- Skalabilnost: Sposobnost brze obrade velikog broja transakcija.
- Sigurnost: snažan, matematički zaštićen i kriptografski osiguran sustav za zaštitu sredstava i informacija korisnika.
- Interoperabilnost: Sposobnost razmjene informacija i vrijednosti te međusobne interakcije između različitih blockchain sustava.
- Dizajn prilagođen korisniku: omogućiti početnicima jednako kao i naprednim korisnicima korištenje svih pogodnosti DeFi platforme.

Ethereum pametni ugovori učinili su taj eko-sustav najboljim blockchain sustavom za defi projekte u ranim fazama razvoja fintech industrije. No kako se DeFi primjena širi, nastaju konkurentski blockchain sustavi poput Cardano, Polkadot i Binance Smart Chain koji su specijaliziraniji i donose neke pojedinačne prednosti.

3.7 Cardano

Cardano je blockchain platforma otvorenog koda koja se obično koristi za podržavanje decentraliziranih aplikacija (DApps) i sustava na globalnoj razini. Pokreću ga tokeni istoimene kriptovalute, oznake ADA. Charles Hoskinson, jedan od osnivača Ethereum sustava, osnovao je Cardano ekosustav 2015. godine.

Za razliku od bitcoin eko sustava, Cardano nije imao pregledni tehnički rad kojim bi se utvrdil glavne značajke i mjesto na tržištu kriptovaluta. Umjesto toga, Hoskinson je zamislio stvaranje slojeva sustava za rješavanje problema koji se javljaju u drugim ekosustavima kriptovaluta.

Kako bi to postigao, Hoskinson je osnovao tri pravna subjekta zajedno s partnerima u Švicarskoj i Japanu: Cardano Foundation, Input Output (IOHK) i Emurgo. Njihova je svrha bila stvoriti blockchain ekosustav temeljen na delegiranom (*delegated*) i ne-skrbničkom (*non-custodial*) protokolu konsenzusa s dokazima o udjelu (*proof of stake*).

Cardano ekosustav dizajniran je kao blockchain platforma treće generacije koja se temelji na modelu proširenog nepotrošenog transakcijskog izlaza (UTXO) koji kombinira značajke Ethereum računovodstvenog modela s arhitekturom bitcoin eko-sustava koja se temelji na transakcijama.

Cardano blockchain pokreću umreženi čvorovi i sastoji se od četiri različite komponente ili sloja. Cardano-čvor, koji se sastoji od međusobno povezanih komponenti, glavni je proizvođač blokova i ulazna točka mreže.

- Sloj nagodbe (*settlement*) temeljni je sloj na kojem se grade sve ostale komponente. Ovdje se odlučuje o entitetima blockchain sustava i upravljanju sustavom.
- Konsenzusni protokoli kategorije Ouroboros proof-of-stake (PoS), koji pružaju i poboljšavaju proof-of-work sigurnost uz mali dio troškova energije, implementirani su u sloj konsenzusa.
- Mrežni sloj je peer-to-peer mrežni stog s protokolom koji podržava multipleksiranje i razne zaštite od zlonamjernih uređaja u sustavu.
- Plutus skriptni jezik, koji je dio skriptnog sloja, daje mreži mogućnost korištenja pametnih ugovora.

Cardano se razvija u pet epoha Byron, Shelley, Goguen, Basho i epoha Voltaire. Razvoj slijedi proces u kojem svaka epoha predstavlja set funkcionalnosti koje se implementiraju slijedno tijekom vremena.

3.8 Byron: Temeljni razvoj

Dvije godine razvoja (2015. – 2017.) poznate kao Byronova era dovele su do izdanja ADA tokena i početne iteracije Cardano blockchaine. ADA token je dobio ime po engleskoj matematičarki Ada Lovelace, koja je poznata po tome što je bila među prvim računalnim programerima u svijetu.

IOHK i Emurgo su izradili službene novčanike za ADA token, nazvane Daedalus desktop wallet i Yoroi light wallet, a izlazak novčanika tempiran je istovremeno s lansiranjem Cardano blockchaine odnosno ADA tokena. Cilj Byronove ere bio je stvoriti zajednicu, uključiti ljude u izgradnju budućeg blockchaine i distribuirati kovanice na pravedan i raznolik način, što je doprinijelo prvim značajnim tehnološkim naprecima.

3.9 Shelly: Decentralizacija kontrole

Širenje i poboljšanje tadašnjeg Cardano ekosustava fokus je Shelleyeve ere. Tijekom Byronove ere mreža je bila udružena; međutim, kako je Shelleyeva era napredovala, od 2020. do 2021., dogodio se planirani postupni prijelaz na 100%-e blokove koje su proizveli stakepooli, a ne čvorovi inicijalne zajednice

Cardano zajednica sada pokreće i protočne i proizvodne čvorove. Protočni služe kolanju informacija, a proizvodni proizvode nove blokove. Kako bi se povećala sigurnost i operativna otpornost, jedan od primarnih ciljeva ove faze bio je decentralizirati mrežu čvorova uključivanjem većeg broja sudionika u mreži.

Nakon izdavanja Shelley, drugi novčanici su se pridružili tržištu i, pružajući određene značajke, privukli znatnu bazu korisnika. Nekoliko značajnijih ADA novčanika, osim Yoroi i Daedalus, su sljedeći: Eterni za dApps, Nami za NFT tokene, AdaLite za delegaciju u više zajednica (poolova) te Typhoon sa najvećom hardversom kompatibilnošću.

3.10 Goguen: era pametnih ugovora

Na Cardano blockchainu pametni ugovori i DApps su prvi put predstavljani tijekom Goguen ere. Ova faza razvoja, koja podsjeća na Shelleyjevo razdoblje, usredotočena je na razvoj Plutusa, izvršne platforme i programskog jezika posebno dizajniranog za pametne ugovore.

Programeri mogu koristiti Plutus za pisanje i pokretanje pametnih ugovora na Cardano mreži. Marlowe, jezik specifičan za domenu (DSL) za financijske ugovore temeljen na Plutus, također je uveden u to doba i odlikuje ga vizualni editor u stilu blokova koji vam omogućuje da dizajnirate automatiziranu logiku bez potrebe za pisanjem koda.

Nadalje, viševalutna knjiga biva podržana tijekom Goguen ere, omogućujući korisnicima stvaranje novih izvorno podržanih zamjenjivih i nezamjenjivih tokena (NFT). U tom smislu, "nativni" se odnosi na činjenicu da su svi ovi tokeni - uključujući sigurnosnu arhitekturu i UTXO mogućnosti - implementirani na istom sloju 1 kao i ADA token. Pametni ugovori ih ne dizajniraju i ne stvaraju.

3.11 Basho: skaliranje

Cilj Bashoove ere je poboljšati temeljnu operativnost, skalabilnost i optimizaciju mreže Cardano. Temeljni razvoj odnosi se na već postojeće pametne ugovore i povezivanje zaglavlja blokova, dvije tehnologije koje imaju potencijal uvelike povećati mogućnosti mreže. U ovoj eri nastaju i paralelne sidechain implementacije.

Bočni lanci su vrsta dijeljenja koja povećava kapacitet mreže prebacivanjem rada s glavnog lanca na bočni, pomoćni, lanac. Osim toga, omogućuju testiranje novih značajki bez ugrožavanja sigurnosti glavnog blockchaina.

3.12 Voltaire - Upravljanje

Cilj Cardano ere Voltaire je stvoriti samoodrživu upravljačku strukturu koju podržavaju korisnici mreže. Sustavi glasovanja i riznice bit će uvedeni u ovoj fazi, omogućujući korisnicima financiranje predloženih razvoja i dijeljenje ažuriranja i poboljšanja parametara

protokola. Dio svih naknada za transakcije i drugi dio svih nagrada za uloge će se kombinirati nakon postupka glasovanja kako bi se stvorio novac za razvojne inicijative.

Nakon što se uspostave mehanizam glasanja i riznice, završetak ove faze navijestit će dolazak istinski decentralizirane mreže Cardano, koja će raditi neovisno o inženjerskim i istraživačkim timovima IOHK-a. Umjesto toga, budućnost Cardana odredit će zajednica, koja će imati sve resurse potrebne za rast i promjenu mreže zbog sigurne, decentralizirane osnove koju pruža IOHK.

3.13 ADA - token Cardano mreže

Smješten na sloju nagodbe u Cardano sustavu, ADA je interni token Cardano blockchaina. 45 milijardi tokena maksimalna je količina ADA koja se može proizvesti; oni će se kovati i distribuirati postupno. Atribut deflacije osiguran je za ADA ograničenjem ukupne ponude tokena. No, ekosustav će pokazivati inflacijski trend sve dok značajan dio rezervi ne bude pušten u optjecaj, što se predviđa da će početi 2030. godine.

ADA se može čuvati u novčanicima za kriptovalute i mijenjati za fiat valute poput američkog dolara. Osim Cardanoovih internih rješenja novčanika, kao što su Yoroi i Daedalus, postoje i novčanici trećih strana koji mogu olakšati ADA prijenose i pohranu jer podržavaju i ostale valute.

Dodatno, ADA se može sigurno čuvati u toplim i hladnim novčanicima. Izgrađen na temelju zbirke konsenzusnih protokola blockchaina s dokazom o udjelu pod nazivom Ouroboros, ADA je namijenjen funkcioniranju kao sigurno sredstvo razmjene vrijednosti. Cardano blockchain također može podržavati DApps, NFT, pametne ugovore i dodatne kriptovalute.

3.14 Polkadot

Polkadot je ekosustav koji nudi pješčanik nazvan blockspace za razne Web3 projekte, a riječ je o blockchain mreži sljedeće generacije. Podržava ga zajednica programera i privukao je interes korisnika, a sastoji se od heterogenog višelančanog okvira. Smatra se jednim od najinventivnijih projekata u industriji kriptovaluta.

Polkadot ekosustav, kojeg pokreće DOT, izvorna valuta i token mreže, ima za cilj riješiti mnoga ograničenja povezana s lancima blokova, poput skalabilnosti, posloženosti i sigurnosti. Posebne značajke Polkadota izdvajaju ga od konkurencije i omogućuju širok raspon slučajeva korištenja u stvarnom svijetu.

Projekt je zamišljen 2016. godine, a DOT token je ušao na tržište u kolovozu 2020. godine, nakon objave osnivača Gavina Wooda o tehničkoj spremnosti. DOT je uvršten na mjenjačnicu Coinbase u lipnju 2021.

Polkadot se smatra inovativnim iz nekoliko razloga. Blockchaini se odlikuju svojom decentralizacijom, brzinom i sigurnošću u okruženju bez povjerenja. Dok većina blockchaina pruža jednu - ili ponekad dvije - od ovih razlikovnih karakteristika, njihova arhitektura nije dizajnirana da podržava sve značajke u isto vrijeme. Na primjer, Ethereum je najpopularnija platforma za decentralizirane aplikacije (DApps). Međutim, trenutno nije jako skalabilan i ima izuzetno visoke naknade, posebno kada je promet na platformi velik. EOS, s druge strane, osigurava jeftine transakcije nauštrb decentralizacije.

Sve ove mreže izolirane su jedna od druge i razmjenjuju malo ili nimalo informacija. Razmotrite banke kojima nije dopuštena interakcija; ne bismo mogli glatko prenijeti novac iz jedne banke u drugu. E-pošta je još jedan primjer. Zbog njihove interoperabilnosti, možemo prenijeti podatke s Yahoo računa na Gmail račun, na primjer. Trenutačno nedostatak interoperabilnosti sprječava široku primjenu blockchain tehnologije. Polkadot ima za cilj ispuniti ovu prazninu.

Polkadot je blockchain ekosustav s jezgrenom mrežom — Relay Chain — putem koje se drugi blockchaine i njihove odgovarajuće DApps povezuju i komuniciraju. Relejni lanac ugošćuje lance blokova dok istovremeno upravlja njihovom sigurnošću i transakcijama, omogućujući nesmetan rad međulančanog slaganja transakcija (modularna komunikacija između različitih lanaca blokova).

Protokol relejnog lanca određuje zajedničku sigurnost mreže, konsenzus i interoperabilnost između lanaca. To je pogon koji drži cijelu infrastrukturu na okupu, povezuje druge sudionike mreže i osigurava dovršetak transakcije.

Relejni lanac je namjerno dizajniran da ima minimalnu funkcionalnost. Pametni ugovori, na primjer, nisu izravno podržani, a primarna odgovornost lanca je koordinacija sustava u cjelini, uključujući parachaine. Ovo oslobađa kapacitet delegiranjem funkcionalnosti odgovarajućim paralancima.

Polkadot pokušava riješiti jedan od glavnih nedostataka blockchaine kroz interoperabilnost. Umjesto da postoje kao zasebni entiteti koji djeluju neovisno, blockchaine mogu postati dio istog ekosustava u kojem se ne samo informacije i novac, već i računalni programi mogu sigurno razmjenjivati na skalabilan način.

Polkadot čak rješava komunikaciju između dvije različite vrste mreža, privatne i javne, unatoč činjenici da privatni lanci blokova imaju malo drugačije tehničke protokole od javnih lanaca blokova. Prilagodljiva i fleksibilna mrežna arhitektura Polkadota pojednostavljuje proces uključivanja u nova Web3 poduzeća, omogućujući programerima da iskoriste prednosti skalabilnosti, interoperabilnosti i sigurnosti. Kao rezultat toga, Polkadotova mreža predstavlja značajan napredak za programere i poduzetnike koji žele izgraditi bilo koji Web3 projekt iz temelja u kratkom vremenskom razdoblju.

Kada pokušavaju stvoriti novi blockchain, programeri moraju stvoriti jedinstveni state machine i konsenzusni algoritam, a oboje je teško implementirati i zahtijevaju značajnu količinu vremena i truda. Temeljna arhitektura Polkadota ima za cilj riješiti ovo eliminiranjem potrebe za izgradnjom zajedničkih komponenti blockchaine od temelja.

Blockchain temeljen na Polkadotu koristi modularni okvir Substrate, koji korisnicima omogućuje da uključe značajke koje su im potrebne, dok im također omogućuje da ih mijenjaju prema potrebi. Nadalje, programerima omogućuje prilagodbu arhitekture lanca i odabir specifičnih komponenti koje zadovoljavaju njihove potrebe. Također se mogu povezati s drugim ekosustavima, poput Ethereuma i Bitcoina, preko softverskih mostova između ekosustava ako to žele.

3.15 Paralelni lanci blokova

Pojam parachain je skraćenica za paralelne lance. Svaki parachain je vlastiti blockchain, sa svojom logikom i značajkama. Djeluju autonomno sa svojim tokenima i upravljanjem te pružaju specifične slučajeve upotrebe. Međutim, parachaine koriste i imaju koristi od sigurnosti i interoperabilnosti relejnog lanca za konačnost transakcije. Korištenje relejnog

lanca omogućuje besprijekorno funkcioniranje svakog sustava parachaina, omogućujući programerima i korisnicima da se usredotoče na druge specifične ciljeve kao što su privatnost ili skalabilnost, kao i na svoje specifične aplikacije. U biti, parachaini dobivaju pristup jednoj od najznačajnijih prednosti mreže: korištenje uspostavljene sigurnosti Polkadota uz velike i skalabilne brzine transakcija.

3.16 Substrate - razvojno okruženje za Polkadot blockchain

Polkadot's Substrate moćan je blockchain okvir koji značajno pojednostavljuje stvaranje novog blockchaina. Namijenjen je pomoći programerima u stvaranju vlastitog blockchaina dok se povezuju na Relay Chain i iskorištavaju njegovu sigurnost, brzinu i učinkovitost. Dizajn omogućuje programerima da se usredotoče na dodavanje vrijednosti svojim projektima umjesto da troše resurse i sredstva na izgradnju svakog dijela infrastrukture iz temelja. Svi lanci koji koriste Substrate kompatibilni su s Polkadotom i imaju pristup interoperabilnom ekosustavu parachaina, aplikacija i resursa.

Substrate su stvorili pioniri blockchain industrije koji su zamislili sustav koji bi mogao prevladati ograničenja mreža prethodne generacije. Namjeravali su programerima pružiti komplet za razvoj softvera koji bi eliminirao potrebu za izgradnjom i optimizacijom blockchaina od temelja.

Polkadot i Substrate nisu međusobno ovisni, unatoč sinergiji. Polkadot parachaini mogu se izgraditi i održavati pomoću softvera koji nije Substrate, dok Substrate lanci ne moraju biti povezani s Polkadotom ili Kusamom.

3.17 Kusama - platforma za istraživanje i razvoj

Polkadotova mreža Kusama koristi se za implementaciju u ranoj fazi, kao živo predprodukcijско okruženje i kao eksperimentalna mreža. Programeri tada mogu pokrenuti svoje lance ili DApps na Kusami za smanjenje rizika i testiranje rada pod živim, stvarnim uvjetima prije nego što počnu živjeti kao proizvodna mreža na Polkadotu nakon prve implementacije na testnim mrežama.

Kusama ima nižu ekonomsku prepreku za ulazak od Polkadota, što ga čini puno lakšim i zahtijeva manje DOT-a za pokretanje parachaina ili postajanje validatorom.

Upravljanje Kusamom kreće se bržim tempom od upravljanja Polkadotom kako bi se omogućilo testiranje novih značajki u borbi prije nego što se rasporede na Polkadot. Kusama može u performansama biti čak četiri puta bolja od Polkadot sustava. Imateljima tokena treba samo sedam dana za glasovanje na referendumu, nakon čega slijedi osmodnevno razdoblje validacije, nakon čega će referendum biti ratificiran u lancu.

Kusamin moto je "očekujte kaos" jer njegova brža stopa nadogradnje može doći nauštrb stabilnosti, što znači da zainteresirane strane moraju ostati na oprezu kako bi pratile sve prijedloge, referendume i nadogradnje. U isto vrijeme, Kusama validatori se često moraju ažurirati u kratkom roku.

3.18 Hyperledger Blockchain

Hyperledger je sveobuhvatna zbirka projekata otvorenog koda koji su posebno dizajnirani za olakšavanje napretka distribuiranih knjiga temeljenih na blockchainu. Njegov primarni cilj je uspostaviti bitne okvire, standarde, alate i biblioteke potrebne za izgradnju blockchaina i povezanih aplikacija. Odgovornost za podršku, održavanje i hosting ovih projekata leži na Zakladi Hyperledger, organizaciji koja je bila ključna u pokretanju razvoja ove tehnologije.

Od svog početka 2016. pod okriljem Linux Foundationa, Hyperledger je prikupio doprinose istaknutih organizacija kao što su IBM, Intel, Samsung, Microsoft, Visa, American Express, kao i raznih blockchain startupa poput Blockforcea. Ovaj zajednički napor obuhvaća širok raspon industrija, uključujući bankarstvo, upravljanje opskrbnim lancem, internet stvari (IoT), proizvodnju i proizvodne sektore.

Hyperledger služi kao središnje središte za različite okvire i biblioteke distribuiranih knjiga. Korištenjem ove platforme, tvrtke mogu koristiti jedan od okvira Hyperledgера za poboljšanje učinkovitosti, performansi i transakcijskih mogućnosti svojih operativnih procesa.

Funkcioniranje Hyperledgера vrti se oko pružanja potrebne infrastrukture i standarda za razvoj blockchain sustava i aplikacija. Programeri koriste Hyperledger Greenhouse, koji sadrži okvire i alate koji čine Hyperledger, za stvaranje blockchain projekata prilagođenih njihovim specifičnim poslovnim zahtjevima. Naime, svi sudionici mreže unutar ekosustava Hyperledger međusobno su priznati i mogu se aktivno uključiti u procese izgradnje konsenzusa.

Tehnologija temeljena na Hyperledgeru djeluje kroz nekoliko slojeva, uključujući sloj konsenzusa koji potvrđuje redoslijed i točnost transakcija u bloku, sloj pametnog ugovora koji obrađuje i autorizira zahtjeve za transakcije, komunikacijski sloj koji upravlja prijenosom P2P poruka, API koji omogućuje komunikaciju s blockchainom i usluge upravljanja identitetom koje potvrđuju identitet korisnika i sustava.

Među najistaknutijim okvirima Hyperledgера su Hyperledger Fabric i Sawtooth.

3.19 Hyperledger Fabric

Hyperledger Fabric, razvijen u suradnji s IBM-om i Digital Assetom, dopuštena je blockchain infrastruktura koja olakšava stvaranje proizvoda, softvera i aplikacija temeljenih na blockchainu. Može se pohvaliti modularnom arhitekturom koja definira uloge čvorova, pametno izvršenje ugovora i konfigurabilne usluge konsenzusa. Fabric također podržava različite programske jezike i konsenzusne protokole koji se mogu priključiti. Obično se koristi u integracijskim projektima koji zahtijevaju distribuiranu knjigu.

Fabric arhitektura daje prioritet nekoliko ključnih značajki koje ga čine atraktivnom opcijom za mnoge industrije. Jedna od tih značajki je privatnost, koja se održava putem "dopuštenog" sustava članstva. Sva računala unutar mreže moraju biti identificirana i pridružiti se putem pružatelja usluga za članstvo (MSP). Međutim, Fabric ne zahtijeva dopuštenje za sve dijelove blockchaina, što omogućuje fleksibilnost u dizajnu mreže.

Još jedna važna značajka Fabric okvira je mogućnost dijeljenja knjiga u "kanale". To omogućuje članovima mreže stvaranje zasebnih skupova transakcija koje nisu vidljive široj mreži. Ova segregacija osjetljivih podataka pruža dodatni sloj sigurnosti i kontrole.

Skalabilnost je također ključna karakteristika Fabric okvira koja privlači veća poduzeća. Mreža se može brzo skalirati dodavanjem više čvorova, dok je i dalje sposobna obraditi velike količine podataka s manjim skupom resursa. Ova fleksibilnost omogućuje uravnotežen pristup, gdje se blockchain može inicijalno stvoriti s malim skupom čvorova, a zatim skalirati na zahtjev.

Konačno, Fabric arhitektura dizajnirana je imajući na umu modularnost. To znači da se zasebne komponente mogu dodati ili implementirati u različito vrijeme, dajući tvrtkama moć odabira onoga što je potrebno za njihove specifične potrebe. Izborne komponente, kao što su metode konsenzusa, usluge članstva, pohrana glavne knjige, pristupni API-ji i integracija lančanog koda, mogu se izostaviti ili uvesti kasnije bez utjecaja na cjelokupnu funkcionalnost sustava. Ovaj modularni pristup pruža fleksibilnost i prilagodljivost tvrtkama koje koriste Fabric.

Ključno je razumjeti što Hyperledger Fabric nije, uz ono što pruža. Hyperledger Fabric je blockchain okvir koji surađuje s drugim Hyperledger projektima na stvaranju skalabilne podatkovne platforme. To je platforma za razvoj aplikacija, a drugi članovi ekosustava, kao što su Composer, Quilt i Explorer, konzumiraju podatke iz Fabric mreža. Hyperledger nije projekt kriptovalute, i namjerno je dizajniran na ovaj način. Ne koristi kriptovalute ni u kojem obliku, a primarni cilj mu je unaprijediti blockchain tehnologiju i pružiti robusnu implementaciju visoko skalabilne tehnologije pohrane podataka. Fabric je samo jedan od blockchain okvira u sklopu projekta Hyperledger.

Blockchain tehnologija pruža temelj za nepromjenjivu bazu podataka s distribuiranom knjigom, koja se može koristiti za razvoj decentraliziranog oblika valute. Međutim, blockchain sam po sebi nije Bitcoin ili kriptovaluta općenito. Hyperledger Fabric uzima temelj blockchaina i pruža okvir povrha njega, koristeći njegove kvalitete kao mreže.

Za razliku od blockchain okvira pod Ethereumom, Fabric se ne oslanja na sustav "dokaz rada" koji uključuje rudarenje bitcoina i ne oslanja se ni na jedan oblik kriptovalute. Zbog toga je Fabric privlačniji poduzećima koja žele usvojiti novi oblik umrežavanja transakcija između poduzeća umjesto potpuno nove valute.

3.20 Fabric pametni ugovori - ChainCode

Unutar Hyperledger Fabric pametni ugovori se nazivaju lančani-kod i smatraju se jednom od najvažnijih komponenti Fabric mreže. Djelujući kao virtualni odvjetnici, pametni ugovori olakšavaju razmjenu imovine unutar blockchain mreže postavljanjem cijena, opisivanjem sporazuma i delegiranjem radnji na temelju određenih zahtjeva. Ovi ugovori mogu varirati od jednostavnih zadataka poput plaćanja određenog iznosa do složenijih radnji poput izdavanja digitalnih potvrda ili pružanja povrata za neisporučenu robu.

U Fabric okviru pametni ugovori igraju opipljiviju ulogu budući da predstavljaju stvarne ugovore dogovorene između dva profesionalna subjekta tijekom trgovine. Automatiziranjem procesa i upravljanjem razmjenama plaćanja, pametni ugovori značajno pojednostavljaju proces trgovanja. Dok kod pametnog ugovora izvršava sve potrebne radnje, lančani kod implementira pametni ugovor u mrežu, čineći ih dvije različite, ali komplementarne komponente mreže Fabric.

3.21 Sastavni dijelovi Hyperledger Fabric sustava

Hyperledger Fabric, kao i druge tehnologije ili platforme temeljene na blockchainu, konstruiran je pomoću nekoliko ključnih elemenata. To uključuje distribuiranu knjigu koja bilježi sve podatke koji se odnose na transakcije, više ravnopravnih računala ili čvorova i pametne ugovore koji upravljaju logikom transakcije. Slično većini blockchain mreža, provjera valjanosti transakcija u Fabric okviru zahtijeva konsenzus svih čvorova koji sudjeluju u glavnoj knjizi, što se naziva odobrenjem.

Čvorovi, koji predstavljaju organizacije i članove, igraju ključnu ulogu unutar blockchain mreže. Oni pohranjuju kopije knjiga i pametnih ugovora, što ih čini ključnim za olakšavanje transakcija i ukupnog tijeka transakcija. Kada se transakcija pokrene, mora proći potvrdu od strane većine članova mreže, poznatih kao *endorser* članovi, ili unutar određenog kanala mreže. Ovaj postupak provjere valjanosti osigurava integritet i točnost transakcije.

Osim konsenzusa, ravnopravni korisnici ispunjavaju i druge odgovornosti unutar tijeka transakcije. Unutar kanala služe kao komponente i osiguravaju potrebnu infrastrukturu za kretanje i obradu podataka.

Konačno, Hyperledger Fabric CA, također poznat kao Fabric Certificate Authority, služi kao pružatelj usluga članstva za Hyperledger Fabric. Njegove primarne odgovornosti uključuju upravljanje registracijom članova, upravljanje procesima certificiranja i nadzor nad regulacijom čvorova unutar mreže. Obavljajući ove zadatke, tijela za izdavanje certifikata igraju ključnu ulogu u uspostavljanju Fabrica kao dopuštenog blockchain sustava. Oni su odgovorni za registraciju članova, održavanje evidencije identiteta unutar mreže i uklanjanje zastarjelih računa.

Kako bi se olakšala komunikacija s različitim komponentama Fabric mreže, Hyperledger Fabric CA poslužitelj koristi REST API-je. Ovi API-ji omogućuju interakciju između poslužitelja i Fabric SDK-a integriranog u klijentsku aplikaciju ili specijalizirane instance Fabric CA klijenta. Važno je napomenuti da je Fabric CA opcijaska i modularna komponenta, koja pruža fleksibilnost u implementaciji unutar mrežne arhitekture.

3.22 Hyperledger Sawtooth

Hyperledger Sawtooth, blockchain platforma koju je razvio Intel, dizajnirana je za organizacije koje se bore s implementacijom blockchain tehnologije. Pruža dopušteno i modularno rješenje za implementaciju, pokretanje i izgradnju distribuiranih knjiga. Sawtooth nudi različite značajke kao što su dinamički konsenzus, transakcijske obitelji i paralelno izvršavanje transakcija, koje omogućuju stvaranje pojedinačnih lanaca. Dodatno, podržava Ethereum pametne ugovore i pruža komplete za razvoj softvera (SDK) za više programskih jezika uključujući Python, Go, JavaScript, Rust, Java i C++. Ova je platforma posebno prilagođena tvrtkama kojima je potrebna dopuštena blockchain platforma.

Važno je napomenuti da Hyperledger ima raznolik raspon projekata i alata izvan samo Hyperledger Sawtooth i Hyperledger Fabric. Ti su projekti trenutačno aktivni ili u fazi inkubacije, što znači da prolaze kroz rigoroznu procjenu i testiranje prije nego što budu proglašeni aktivnima i spremnima za proizvodnju. Hyperledgerov portfelj uključuje razne inovativne projekte koji imaju za cilj rješavanje različitih slučajeva upotrebe i industrijskih zahtjeva unutar blockchain prostora, poput:

1. Hyperledger Iroha je blockchain okvir koji je dizajniran za integraciju s postojećim mrežama. Ima modularni dizajn, pristup temeljen na kontroli, pristup mnogim knjižnicama, kao i upravljanje imovinom i identitetom. Naširoko se koristi u raznim područjima kao što su financijske usluge, zdravstvo i obrazovanje.
2. Hyperledger Indy, s druge strane, okvir je koji je posebno napravljen za decentralizirane identitete. Dolazi s komponentama, setovima alata i bibliotekama te uključuje samostalnu suverenost koja sigurno pohranjuje svu dokumentaciju temeljenu na identitetu.
3. Hyperledger Besu je baza Ethereum koda otvorenog koda koja može raditi na privatnim platformama s dopuštenjem ili javnoj mreži Ethereum. Sadrži Ethereum Virtual Machine (EVM), algoritme konsenzusa, API-je okrenute prema korisniku i nadzor.
4. Hyperledger Explorer je uslužni alat nadzorne ploče koji korisniku omogućuje praćenje, pretraživanje i održavanje blockchaina i povezanih podataka. Organizacijama omogućuje provjeru čvorova, blokova, transakcija i pametnih ugovora, a također omogućuje korisnicima da mijenjaju kod.
5. Hyperledger Cello je set alata blockchain-as-a-service koji se koristi za stvaranje, ukidanje i upravljanje blockchain uslugama.
6. Hyperledger Burrow je dopušteni Ethereum čvor blockchain pametnog ugovora koji upravlja transakcijama i izvršavanjem koda pametnog ugovora na EVM-u.
7. Hyperledger Bevel je akcelerator za implementaciju tehnologije distribuirane knjige (DLT). Omogućuje postavljanje DLT-a, implementaciju i integraciju s novim organizacijama.
8. Hyperledger Firefly je softverski skup srednjeg softvera otvorenog koda za Web3 aplikacije.
9. Hyperledger Cacti je okvir interoperabilnosti za povezivanje i izvođenje transakcija preko više heterogenih knjiga.
10. Hyperledger Solang je Solidity kompajler koji omogućuje prijenos pametnih ugovora.
11. Hyperledger Aries je alat za kreiranje, prijenos i pohranjivanje digitalnih vjerodajnica i decentraliziranog upravljanja ključevima.
12. Hyperledger Anoncreds je provjerljiva vjerodajnica koja ne ovisi o glavnoj knjizi.
13. Hyperledger Caliper je blockchain benchmark alat koji se koristi za procjenu performansi blockchain implementacija. Međutim, ne dolazi sa predefiniranim standardima jer je riječ o alatu za suviše heterogene eko-sustave.

Godine 2022. Hyperledger je donio odluku da prekine četiri projekta, naime Avalon, Burrow, Explorer i Quilt, stavljajući ih u status kraja životnog vijeka (End of Life - EOL).

Projekt Hyperledger osnovala je The Linux Foundation 2015., godinu dana prije službenog pokretanja, a Brian Behlendorf preuzeo je ulogu izvršnog direktora. Behlendorf je naglasio da projekt Hyperledger neće razviti vlastitu kriptovalutu. Projekt je počeo prihvaćati prijedloge za inkubaciju baze koda i tehnologije temeljnih elemenata 2016. godine, a Hyperledger Fabric i libconsensus bili su među prvim prihvaćenim bazama koda blockchaina. Kasnije je također inkubirana Intelova Sawtooth distribuirana knjiga. Sawtooth 1.0, verzija spremna za proizvodnju, predstavljena je 2018., a 2019. najavljena je dugoročna verzija Hyperledger Fabric s podrškom. U listopadu 2021.

Daniela Barbosa preuzela je dužnost izvršne direktorice, a tijekom istog mjeseca Hyperledger je doživio rebranding u The Hyperledger Foundation, s ciljem uspostavljanja jasnije razlike između organizacije i pojedinačnih Hyperledger projekata, kako je navedeno u postu na blogu organizacije.

3.23 Blockchain podrazumijeva transparentno poslovanje

Uspon blockchain tehnologije uvelike se pripisuje njezinoj upotrebi u svijetu kriptovaluta, posebice s pojavom bitcoina. Međutim, kako se tehnologija nastavlja razvijati, postoji sve veća potreba za naprednijim i sigurnijim aplikacijama koje mogu podnijeti česte promjene u dijeljenju informacija uz održavanje visoke razine kriptografske sigurnosti. Jedna od ključnih prednosti blockchaina je njegov otvoreni i decentralizirani dizajn koji omogućuje transakcije u stvarnom vremenu bez potrebe za posrednicima. Posljednjih godina raste interes za korištenje blockchaina za promatranje Zemlje, a Kina razvija protokol temeljen na CCSDS (*Consultative Committee for Space Data Systems*) formatu za poboljšanje dijeljenja podataka i komunikacije između satelita. Još jedno obećavajuće područje za blockchain je razmjena medicinskih podataka, iako će stvaranje modela za to vjerojatno biti složen i izazovan zadatak.

Za praćenje udaljenih pacijenata u zdravstvenoj industriji ključno je koristiti odgovarajuće nosive uređaje koji uključuju sigurnu simetričnu enkripciju ključeva kako bi se osigurala sigurna razmjena podataka. Kada je riječ o osiguranju zdravstvene skrbi, blockchain tehnologija se pokazala vrlo korisnom za praćenje i bolničke i izvanbolničke skrbi, osobito u kombinaciji s pametnim nosivim uređajima. Međutim, u području promatranja Zemlje, blockchain tehnologija igra još kritičniju ulogu i češće se koristi. Izazov leži u istraživanju načina za sigurno dijeljenje i pružanje medicinskih vjerodajnica pacijenata bez ugrožavanja njihove sigurnosti, što je posebno izazovno u brzo rastućem području medicine. Kako bi se to riješilo, upotreba kripto prostornih koordinatnih sustava postaje neophodna, gdje se vremenske serije i prostorno indeksiranje pohranjuju kao dio zapisa.

Integracija umjetne inteligencije (AI) i blockchain tehnologije također je značajno napredovala u predviđanju i predviđanju pacijenata i zdravstvene industrije u cjelini. Ova integracija omogućuje čest nadzor iz dana u dan. Osim toga, razvoj blockchaina proteže se na razna druga područja, uključujući zemljišni pokrov i upravljanje njime. U tom kontekstu, znanjima o zemlji u stvarnom vremenu, kao što su vegetacija, tlo, posjed i klimatske promjene, može se pristupiti putem aplikacija koje su paralelne s čestim pristupom podacima blockchaina.

Blockchain tehnologija omogućuje pohranjivanje dodatnih transakcijskih zapisa u zajedničkoj i nepromjenjivoj glavnoj knjizi, olakšavajući praćenje, provjeru valjanosti i osiguranje tih zapisa. Unutar IBM-a, tradicionalne prakse vođenja evidencije pretvorene su u inovativna blockchain rješenja, osiguravajući povjerenje i transparentnost u prirodi upravljanja podacima.

Kako bi povećali transparentnost u pogledu potreba kupaca, tvrtke moraju usvojiti otvoreniji pristup. Međutim, implementacija blockchain tehnologije predstavljala je značajan izazov za osiguravatelje zbog faktora starenja u digitalnoj transformaciji, zahtijevajući dodatnu pomoć. Unatoč tome, prihvaćanjem blockchaina poduzeća mogu postići smanjene troškove i učinkovitije poslovati, u konačnici poboljšavajući pristup korisnicima. Štoviše, zadovoljenje potreba kupaca može se postići ponudom skrojenih, pojednostavljenih i

transparentnih proizvoda, iako s politikama koje su namjerno složenije za razumijevanje u tradicionalnom smislu. Ova namjerna složenost može frustrirati kupce i učiniti klijentima većim izazovom opetovano davanje podataka za višefaktorsku provjeru. Posljedično, dijeljenje podataka s trećim stranama ili dobivanje dopuštenja klijenta postaje neophodno. Takvi izazovi svojstveni su blockchain tehnologiji. Kako bi se riješili ti problemi, relevantno tijelo trebalo bi olakšati autentifikaciju klijenta putem procesa upoznaj svog kupca (KYC), čime se eliminiraju nepotrebna kašnjenja u pristupu podacima o klijentu ili samom klijentu.

Geoprostorni objekti odnose se na pojave koje se nalaze na zemljinoj površini, u rasponu od cesta do prirodnih katastrofa i siromaštva. Kako bi se prikupile sve dostupne informacije, geoprostorni podaci popraćeni su zemaljskim koordinatama. Većina dostupnih geoprostornih podataka je besplatna i uključuje ceste, lokalitete i javne sadržaje.

Razvoj GIS tehnologije, osiguranje, cijene i suvremena elektronička uporaba kod ljudi mogu uvelike doprinijeti visokim performansama upravljanja bazom podataka u strojevima za kodiranje. Korištenjem formata zemljopisne širine i dužine korisnika postaje lakše identificirati adrese ili regije korisnika ili korisnika s većom preciznošću i specifičnošću. Napredak pametne komunikacijske tehnologije, poput pametnih telefona i pametnih satova, to može dodatno poduprijeti.

Geoprostorne aplikacije ne samo da štede novac korisnicima, već i poboljšavaju učinkovitost u smislu transportnih procesa, kao što je dostava kamionom. Pronalaženjem najbolje rute za transfer korisnička služba postaje korisnija nego inače. GIS također može pomoći logističkim organizacijama u identificiranju lokacije imovine s manje kašnjenja i preciznijim odgovorom u slučaju opasnosti.

Blockchain predstavlja brojne izazove koji imaju implikacije na prošlost, sadašnjost i budućnost. Unutar područja zdravstvene skrbi pružatelji usluga susreću se s mnoštvom scenarija koji zahtijevaju pažljivo razmatranje. Jedna od najstrašnijih prepreka napretku medicine je integracija napredne zdravstvene tehnologije, koja obuhvaća krajolik novih bolesti poput koronavirusa koji se neprestano razvija. U tom kontekstu, aspekti softvera i hardvera predstavljaju posebno složene izazove, budući da stalna evolucija ovih komponenti otežava točno predviđanje dijagnoza. Kako bi se to riješilo, algoritmi umjetne inteligencije i strojnog učenja mogu ponuditi automatizirane prijedloge korištenjem dobro održavanih softverskih aplikacija za upravljanje unutar bolničkog sustava upravljanja. Usvajanjem pristupa vođenih tehnologijom, rast i napredak medicinskog razvoja mogu se značajno poboljšati.

Pandemija COVID-19 izazvala je globalnu epidemiju infekcija, što je rezultiralo jednom od najtežih medicinskih kriza u ljudskoj povijesti. Nedostatak odgovarajućih lijekova i cjepiva učinio je izazovom za vlade i glavne zdravstvene ustanove nositi se s pandemijom. Štoviše, praćenje slučajeva COVID-19 i upravljanje podacima generiranim tijekom pandemije pokazalo se iznimno teškim. Pristup i prikupljanje privatnosti podataka također predstavlja izazov pri rukovanju podacima o bolesti COVID-19.

Blockchain tehnologija nudi različite značajke kao što su decentralizacija, anonimnost, kriptografska sigurnost, pametni ugovori i distribuirani okvir koji može pomoći korisnicima i entitetima da učinkovitije rukuju podacima o bolesti COVID-19. Izbijanje je stvorilo moralnu krizu u kliničkim i administrativnim centrima, što je rezultiralo padom u ponudi točnih informacija. Stoga je ključno omogućiti brz i točan uvid u situaciju.

Mnoge službene studije naglašavaju potrebu obrade podataka o bolesti COVID-19 kako

bi se stekli aspekti kao što su sigurnost podataka, integritet podataka, rukovanje podacima u stvarnom vremenu i upravljanje podacima kako bi se pacijentima pružile sve pogodnosti koje su im uskraćene uslijed dezinformacija. Stoga je upravljanje podacima o bolesti COVID-19 korištenjem blockchain okvira ključno. Korištenjem blockchain tehnologije možemo osigurati da se podacima o bolesti COVID-19 postupa sigurno, točno i učinkovito, što u konačnici koristi pacijentima i društvu u cjelini.

Cijeli put bolesti se može pratiti korištenjem blockchain tehnologije. Kako bi se osigurao integritet sustava, ključno je imati osobe od povjerenja koje mogu prijaviti transakcije na blockchainu na svakoj pristupnoj točki. Ti akteri od povjerenja, uključujući proizvodnu tvrtku, nadzor zračne luke, prijevoznicičke tvrtke i bolnicu, također bi trebali uključiti relevantne digitalne dokumente kao što su teretni list ili potpis kad god je to moguće.

Kako bi se osigurala sigurnost dijeljenja informacija s većim i multinacionalnim korporacijama, ključno je da svi pojedinci koji imaju pristup informacijama također budu sigurni. Ovo je osobito važno u zdravstvenoj industriji, gdje se podaci o pacijentima moraju čuvati u tajnosti i sigurnosti. Povjerenje i pouzdanost također su ključni za zdravstvene tvrtke i pružatelje usluga. Osim toga, budućnost zdravstva mora biti napredna i zadovoljiti potrebe svih korisnika, s prvenstvenom brigom za sigurnost.

Arhitektura sustava zdravstvene skrbi uključuje četiri ključna sudionika: pacijenta, kliniku te nadzornike laboratorija i strojeva. Blockchain tehnologija predložena je kao rješenje za rješavanje važnih zdravstvenih problema, kao što je sigurno dijeljenje medicinske dokumentacije i usklađenost sa zakonima o privatnosti podataka. Sudionici se registriraju putem klijentske aplikacije i podnose zahtjev za potvrdu o registraciji putem Pružatelja usluga (SP). Certifikacijsko tijelo tada izdaje certifikat i osobni ključ s novim ID-om. Sve transakcije distribuiraju se kroz Hyperledger fabric blockchain mrežu, osiguravajući da je svaka mrežna transakcija distribuirana u bilo koji dio sustava i da neovlašteni korisnici ne mogu promijeniti ili izbrisati svaku transakciju.

Korisnici mogu obavljati samo transakcije s vremenskom oznakom iz prethodne. Mreža je sigurna na blockchainu, a pružatelji usluga poput kliničara i hash mogu pristupiti potrebnim podacima. Zapisi su modificirani i dostupni laboratorijskom osoblju. Pacijenti mogu pregledavati i ažurirati svoje zapise na mreži zdravstvene knjige, a kliničari ili sudionici laboratorija mogu pregledavati i ažurirati dokumente o pristanku pacijenata. Shema podjele zdravstvene skrbi ima četiri skupine sudionika: administraciju, pacijente, liječnike i laboratorijske radnike.

Certifikacijsko tijelo zahtijeva administratorsku potvrdu o registraciji, koja administratoru daje potpunu kontrolu nad okvirnom regulativom, uključujući objavljivanje, pregled, nadogradnju i povlačenje korisnika. Legitimni liječnici, pacijenti ili laboratorijsko osoblje mogu dobiti relevantni ID kako bi administratoru omogućili pristup blockchain mreži.

Ako se aktivnost sudionika ocijeni nezadovoljavajućom, administrator ga može ukloniti s mreže porukom na blockchain mreži Hyperledger.

IV

Četvrti dio

4	Bitcoin eko sustav	85
4.1	Bitcoin eko sustav - najpoznatija primjena <i>blockchain</i> tehnologije	
4.2	Prethodnici Bitcoin kriptovalute	
4.3	Arhitektura	
4.4	Problem dvostrukog trošenja (<i>eng. Double-spending Problem</i>)	
4.5	Vlasništvo	
4.6	Novčanici za kriptovalute	
4.7	Podjela novčanika na vruće i hladne novčanike	
4.8	Transakcije	
4.9	Kreiranje Bitcoina i značenje rudarenja	
4.10	Napadi na Bitcoin, blockchain mreže i novčanike	



4. Bitcoin eko sustav

4.1 Bitcoin eko sustav - najpoznatija primjena *blockchain* tehnologije

U četvrtom poglavlju, Bitcoin eko sustav – najpoznatija primjena blockchain tehnologije, priručnika prvo će biti obrađena tema *Prethodnici Bitcoin kriptovalute* koja se sastoji od podtema *Bit Gold kriptovaluta*, *Trostruko knjigovodstvo* (eng. *Triple Entry Accounting*) i *Javne transakcije – B-money digitalna valuta*. Kao prvi uvodni primjer, kriptovaluta Bit Gold, koju je osmislio tvorac pametnih ugovora Nick Szabo, bila je među prvim pokušajima stvaranja digitalne decentralizirane valute, čiji je nastanak inspiriran neučinkovitim tradicionalnim financijskim sustavom. Iako sama valuta i njezin koncept, nikada nije bila implementirana, mnogi ju smatraju izravnim prethodnikom Bitcoin protokola. Osim navedenog, u ovom poglavlju bit će objašnjene i teme vezane uz *Arhitekturu*, *Vlasništvo* i *Transakcije* kriptovalutom Bitcoin, kao i *Problem* i *Rješenje problema dvostrukog trošenja* – mogućnosti da korisnik isti novac potroši više od jednom.

Veliki dio ovog poglavlja odnosi se na Novčanike za kriptovalute, gdje su pojašnjeni pojmovi novčanik, klijent, ključevi – javni i privatni, te mogućnosti vezane za odabir novčanika koji odgovara potrebama samog korisnika. Uz to, tema se bavi podjelom novčanika prema odnosu ključeva – deterministički, hijerarhijski deterministički, nedeterministički, ali i podjelom novčanika na vruće – softverske (desktop, online, mobilni), i na hladne (papirnat, hardverski) novčanike.

Značajna tema poglavlja je *Kreiranje Bitcoina* i *značenje rudarenja*, u kojoj je objašnjen proces rudarenja – način na koji je moguće, kao nagradu za rješenu matematičku zagonetku, dobiti bitcoine, mogućnosti rudarenja – solo rudarenje i rudarenje u rudarskim bazenima (zadugama), i naposljetku, oprema koja je potrebna kako bi se rudarenje moglo provesti.

Obradom raznih tema u priručniku postaje jasno kako je tehnologija ulančanih blokova zbog decentralizirane arhitekture, nepromjenjivosti, povjerenja i verificiranih tvrdnji izuzetno sigurna tehnologija, ali i kao takva ipak nije otporna na napade od strane zlonamjernih napadača. U posljednjoj temi ovog poglavlja opisani su najpoznatiji, ali i oni manje poznati, napadi koje je moguće podijeliti na napade na P2P mrežu, na konsenzus i ledger, na pametne ugovore i na novčanike.

4.2 Prethodnici Bitcoin kriptovalute

4.2.1 Bit Gold Kriptovaluta

Bit Gold kriptovaluta bila je jedna od prvih pokušaja stvaranja decentralizirane digitalne valute, koja unatoč tome nikada nije bila implementirana, se često smatra izravnim prethodnikom Bitcoin protokola Satoshija Nakamota. Nick Szabo, vodeći znanstvenih računalstva, pionir u području tehnologije ulančanih blokova i tvorac koncepta pametnih ugovora, predložio je Bit Gold 1998. godine. Szabo je napisao tehnički izvještaj, tzv. bijelu knjigu (eng. *White paper*) za teoretski decentraliziranu digitalnu valutu, ali ista nikada nije bila objavljena.

Stvaranje Bit Golda inspirirano je neučinkovitošću tradicionalnog financijskog sustava, kao i nedostacima vezanim uz upotrebu plemenitih metala kao sredstava razmjene. Neučinkovitost tradicionalnog financijskog sustava, prema tvorcu Szabo, leži u tome da isti od uključenih strana zahtijeva veliko povjerenje kako bi se transakcije mogle izvršiti – korisnik, klijent banke, mora vjerovati da je njegov novac pravilno osiguran i da neće doći do pronevjere, odnosno protupravnog prisvajanja novca, što je moguće kod svih fiat valuta. Nastanak Bit Golda krije se i u pokušaju replikacije ekonomskih svojstava zlata, uz poboljšanje svojstava sigurnosti, koja prema mišljenju tvorca zlatu nedostaje.

Bit Gold prijedlog je revolucionaran, jer se koristio naprednim načelima računalnih znanosti - poput enkripcije, kako bi osmislio novi financijski sustav u kojem nije potrebno povjerenje u treću stranu.

Dva ključna obilježja ovakvog Bit Gold sustava su:

1. Neovisnost o financijskim institucijama – korisnici bi mogli samostalno i sigurno obavljati transakcije bez potrebe za vjerovanjem ili plaćanjem financijskoj instituciji za upravljanje tim transakcijama. Mreža Bit Golda samostalno bi nudila funkcionalnost točnog praćenja stanja korisničkih računa i obrade legitimnih transakcija. Uz to, korisnici bi posjedovali privatne ključeve kojim bi štitili svoja sredstva, što pruža monetarnu suverenost.
2. Jednostavna i brza transakcija preko državnih granica – za razliku od banaka, koje moraju proći vrlo strog i reguliran proces slanja novca drugim financijskim institucijama u drugim državama, decentralizirana mreža Bit Golda i Bitcoina stvara mogućnost obrade brzih i sigurnih transakcija između država u roku od nekoliko minuta. Obzirom da Bit Gold model nikada nije bio implementiran, te pogodnosti s njime nisu ostvarene, ali se danas ostvaruju putem Bitcoin protokola.

4.2.2 Usporedba Bit Golda i Bitcoina

Brojne su sličnosti između arhitekture prijedloga vezanog uz Bit Gold i Bitcoina, posebno u tehničkim mehanizmima namijenjenim obradi transakcija i osiguravanju decentralizirane mreže.

I Bitcoin i Bit Gold pokreće konsenzusni algoritam koji se temelji na dokazu radom (eng. *Proof of Work - PoW*), pri čemu dolazi do potrošnje računalne snage za rješavanje kriptografskih zagonetki. Rješenje zagonetki potom prolazi kroz P2P mrežu, nakon čega nastaje kriptografski lanac hasheva s ciljem povezivanja rješenja najnovije zagonetke s ishodom sljedeće zagonetke, čime dolazi do potvrde blokova transakcije. Ovaj postupak za objavu transakcija na mrežu dosljedan je između Bitcoina i Bit Golda. Jedna od glavnih razlika je u tome što u vrijeme njegova nastanka, Bit Gold prijedlog nije mogao riješiti problem dvostrukog trošenja, dok Bitcoin može, na način da je uvedena potvrda blokova. Bit Gold prijedlog zasnivao se na metodi koja se oslanjala na kvorum mrežnih adresa, umjesto na kvorum računalne snage. Upravo to je Bit Gold mrežu učinilo iznimno ranjivom na Sybil napade, također opisane u ovom priručniku.

Szabo je zamislio da će se težina rudarenja Bit Golda mijenjati tijekom vremena, gdje ne bi nužno postajalo lakše ili teže, ali bi svakako došlo do fluktuacija u količini Bit Golda koje bi se moglo stvoriti u različitim vremenskim trenucima. S druge strane, Bitcoin je dizajniran tako da s vremenom sigurno postaje teže rudariti Bitcoine, a postoji i ograničena opskrba Bitcoinima.

4.2.3 Ključne karakteristike i spoznaje Bit Golda

- Bit Gold bio je prvi prijedlog decentralizirane financijske mreže.
- Tvorac Nick Szabo osmislio je Bit Gold s ciljem rješavanja nedostataka tradicionalnog financijskog sustava i korištenja plemenitih metala kao valuta.
- Decentralizirana financijska mreža (Bit Gold) mogla bi ukloniti ovisnost o financijskim institucijama i istovremeno osigurati sigurne i brze transakcije između država.
- Vizija i namjera Bit Golda ostvarena je Bitcoinom više od desetljeća kasnije, a oba protokola dijele vrlo sličnu arhitekturu, uz veće mogućnosti vezanih uz Bitcoin.

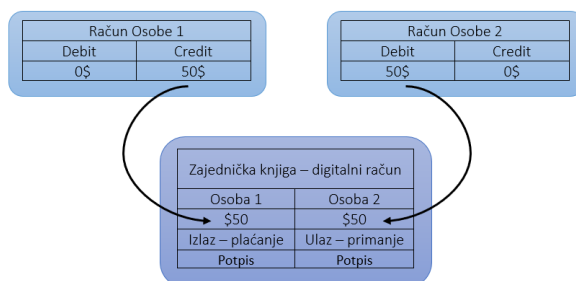
4.2.4 Trostruko knjigovodstvo (eng. *Triple Entry Accounting*)

Izraz *trostruko knjigovodstvo* korišten je po prvi put 1986. godine od strane Yuji Ijirija, stručnjaka za računovodstvo. Ijirij je predložio da se osim knjiženja na dug (*debit*) i potraživanje (*credit*) uvede i treći sloj knjiženja s novim skupom računa s ciljem objašnjavanja promjena u prihodima, nazvan *trebit*. Godine 2005., financijski kriptograf Ian Grigg ponovno definira trostruko knjigovodstvo, te kao alternativu prevarama u transakcijama, predlaže ideju da se digitalno potvrđen račun podržan financijskim kriptografom između dvije strane, može smatrati trećim unosom.

Predložio je rješenje za postupanje s nenamjernim pogreškama i prevarama u računovodstvu. Treća strana, kriptografski siguran unos, može se zabilježiti istodobno za transakcije između subjekata. U ovom trećem unosu, zaduženje zabilježeno od strane jednog subjekta, predstavlja zapravo potraživanje zabilježeno od strane drugog subjekta.

Jednostavan primjer je sljedeći (Slika 4.1): transakcija se provodi između Osobe 1 i Osobe 2. Osoba 1 treba platiti Osobi 2 50 dolara za određenu uslugu. Osoba 2 će napisati potvrdu na treću zajedničku knjigu s potpisom, koju će istovremeno vidjeti Osoba 1, te će potvrdu odobriti i također potpisati. Nepromjenjivim zabilježavanjem trećeg

unosa u zajedničku knjigu, ni Osoba 1 ni Osoba 2 ne mogu zabilježiti drugačiji iznos u vlastitim knjigama, niti kasnije mogu promijeniti nastali zapis. Treći unos ovdje automatski potvrđuje nastalu transakciju.



Slika 4.1: *Primjer trostrukog knjigovodstva*

Treća knjiga na lancu blokova – distribuirana knjiga s ugrađenim pametnim ugovorima

U trenutku Griggova prijedoga, nije bilo jasno tko ili što bi djelovalo kao pouzdana i neutralna treća strana za kontrolu treće, zajedničke knjige korisnika. Tri godine nakon Griggova prijedloga nastaje kriptovaluta Bitcoin i osnovni protokol kriptovalute – tehnologija ulančanih blokova, što je dokazalo kako pouzdana i treća neutralna strana nije nužno potrebna za sigurnost transakcije, obzirom da se treća javna knjiga Grigga može decentralizirati, učiniti nepromjenjivom, sigurnom i automatiziranom, upotrebom upravo tehnologije ulančanih blokova.

Dok tradicionalna baza podataka zahtijeva centraliziranog administratora za upravljanje podacima/zapisima, a istovremeno je ovlaštena, tehnologija ulančanih blokova ne zahtijeva centralnog administratora. Svaki sudionik na lancu blokova ima sigurnu kopiju svih zapisa i promjena, tako da svaki korisnik može vidjeti porijeklo podataka dijeleći sve zapise. Baza podataka lanca blokova je decentralizirana, replicirana i dijeljena – čineći tako distribuiranu knjigu. Intuicija arhitekture tehnologije ulančanih blokova krije se u tome što svaki sudionik baze podataka ima pristup istom primjerku cjelokupne knjige, zbog čega više ne postoji potreba za centralnom vlasti, poput banke, koja bi pratila informacije o sudionicima. Nastankom zapisa o promjeni vlasništva nad imovinom, zajednička knjiga se ažurira i dijeli svima. Dakle, ova distribuirana knjiga unutar tehnologije lanaca blokova odgovara mehanizmu trostrukog unosa koji je predložio Grigg, jer se svaka transakcija između dvije osobe, dva entiteta bilježi u trećoj javnoj knjizi, a obje osobe ili oba entiteta imaju pristup ažuriranoj knjizi. Obzirom da su sve transakcije zabilježene u trećoj javnoj knjizi, idealno neće postojati potreba za revizijom ili usklađivanjem s primjerice bankama.

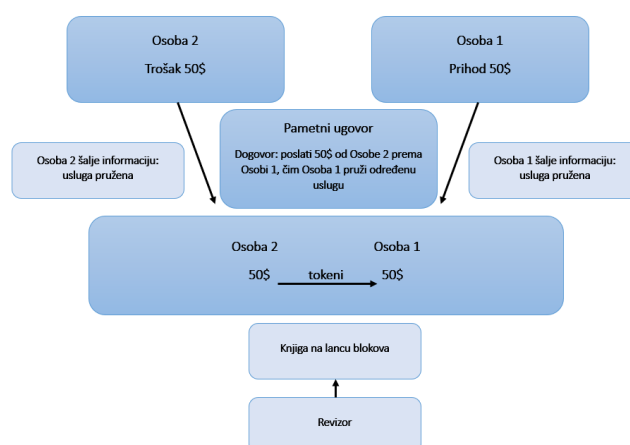
Važan koncept koji dodatno unaprjeđuje trostruko knjigovodstvo je korištenje pametnog ugovora (*eng. Smart contract*), osmišljenog od strane Nicka Szabe 1994. godine, opisanog u drugom poglavlju. Grigg je 2004. godine unaprijedio Szabov koncept i predložio Richardian ugovor, svoju verziju pametnog ugovora, koja predstavlja ugovor koji sadržava sve potrebne uvjete i klauzule, koji je čitljiv istovremeno i za ljude i za računalne programe,

a računalni programi mogu izvršiti ugovor ukoliko je potrebno. S ugradnjom pametnih ugovora, treća knjiga, stvorena na lancu blokova, može se automatski izvršavati i/ili samostalno provoditi sporazume potpisane između dvije strane. Može odgovarati na i slati informacije, a može djelovati i poput tradicionalne banke – preuzima skrb nad imovinom klijenata i izvršava prijenos vrijednosti, koje se umjesto korištenja fiat valuta, koriste u obliku tokena. Dakle, „razbija“ tradicionalni bankarski sustav jer djeluje samostalno na temelju prethodno određenih programskih kodova, slanja i bilježenja informacija te izvršavanja transakcija.

Primjer trostrukog knjigovodstva korištenjem pametnih ugovora

U tradicionalnom knjigovodstvu i postupcima revizije (dvostruko knjigovodstvo), nakon što Osoba 1 obavi određene usluge za Osobu 2, Osoba 2 bi zatražila od banke izdvajanje čeka za Osobu 1. Po obavljanju provjere transakcije, banka prenosi 50 dolara s bankovnog računa Osobe 2, na račun Osobe 1, istovremeno izdvajajući dva primjera primitka, za obje osobe. Po primanju primitka, obje osobe ažuriraju svoje interne unose prema primitku. U ovakvom načinu kriju se mogućnosti pogreške i/ili prevare – informacije nisu dovoljno transparentne (jedna od osoba može „promijeniti“ informacije koje revizor mora provjeravati), a moguće je i da Osoba 2, koja mora isplatiti Osobi 1, nema dovoljno sredstava na bankovnom računu kako bi izvršila plaćanje, što opet dovodi do toga da revizori moraju provjeravati informacije putem različitih izvora (provjera izvornih dokumenata, uskađivanje iznosa plaćanja s bankom, verifikacija dokumenta s drugom osobom).

Suprotno navedenom, a u skladu sa sustavom trostrukog knjigovodstva s tehnologijom ulančanih blokova i pametnih ugovora (Slika 4.2), smanjuje se mogućnost za prevarama ili pogreškama. Osoba 1 i Osoba 2 ovdje unaprijed određuju pravila plaćanja putem samopokretnog digitalnog ugovora – Osoba 2 će platiti Osobi 1 50 dolara, čim Osoba 1 pruži određenu uslugu. Obje osobe potpisuju ugovor na nastaloj trećoj knjizi. Po završetku usluge, obje osobe potpisuju ugovor, treća knjiga se ažurira, a računalni program samostalno šalje 50 dolara Osobi 1.



Slika 4.2: Transakcija između Osobe 1 i Osobe 2 u trostrukom računovodstvenom sustavu s tehnologijom ulančanih blokova.

Dakle, u Griggovom sustavu trostrukog knjigovodstva tri strane – pošiljatelj, primatelj i treća strana, posjeduju kopiju potvrde, a svaka od kopija je dovoljan dokaz transakcije. Treća strana je u Griggovu prijedlogu pouzdana vlast koja bi izdavala novac i koja bi provjeravala ima li pošiljatelj dovoljno sredstava za plaćanje. U vrijeme predloženog koncepta nije bilo jasno tko bi djelovao kao treća pouzdana strana koja bi kontrolirala zajedničku, treću knjigu. Pojavom Bitcoina i tehnologije ulančanih blokova ukazuje se na to kako treća strana iz ovog prijedloga nije nužno potrebna kako bi sama transakcija bila sigurna, upravo zato što je treću javnu knjigu Grigga, kako je ranije opisano, moguće decentralizirati, učiniti nepromijenjivom, sigurnom i automatiziranom, korištenjem tehnologije ulančanih blokova. Kako je opisano u ovom poglavlju, svaka transakcija Bitcoinima emitira se u mrežu, provjerava od strane rudara te se bilježi u lancu blokova. Postupkom verifikacije osigurava se i da je svaka transakcija legitimna, te se sprječava dvostruko trošenje bitcoina. Upotreba kriptografije također osigurava sigurnost transakcija i sprječava njihovo manipuliranje.

Prednosti trostrukog knjigovodstva:

- Plaćanje se provodi pomoću kriptovalute (tokena), eliminirajući tako tradicionalni bankarski sustav.
- Transakcija plaćanja koja se provede zabilježena je kronološkim redoslijedom, a nastali zapis je trajan bez mogućnosti promjene. U slučaju izmjene, potrebno je stvoriti novi zapis
- Centralni poslužitelj ne održava nastali zapis, smanjujući tako moguće prijetnje sigurnosti.
- Zapis stvara poveznicu između internih zapisa Osobe 1 i Osobe 2, što smanjuje podložnost greškama i prevarama.
- Zapis je provjerljiv, stvarajući revizijsku evidenciju.

4.2.5 Javne transakcije

Neki od principa koje Bitcoin koristi za održavanje decentraliziranog registra temelje se na prijedlogu digitalne valute osmišljene 1998. godine, od strane Wei Daia, nazvane „B-money“.

Wei Dai, svjetski poznati računalni inženjer, znatno je doprinio kriptografiji i kriptovalutama, načinom da je razvio kriptografsku biblioteku Crypto++, stvorio sustav B-money te je bio jedan od predlagatelja algoritma za autentifikaciju poruka VMAC. Tijekom studija u 1990-im godinama Dai postaje nadahnut kripto-anarhijom koju je zagovarao Timothy May, a koja se temeljila na uvjerenju da kriptografija i softver mogu bolje osigurati političku i ekonomsku slobodu od bilo kojeg postojećeg sustava vlasti. Iako je već ranije bio poznat u kriptografskom svijetu, njegovo ime dobiva na stvarnoj težini 1998. godine, kada je osmislio digitalnu valutu B-money, za koju je rekao kako se nada da je korak prema tome da kripto-anarhija postane i teoretska i praktična mogućnost.

B-money

Kako je poznato, uobičajeni digitalni sustavi novca koriste centralnu knjigu za praćenje stanja računa, bilo da se radi o centralnoj ili komercijalnoj banci ili pak nekom drugom poslužitelju plaćanja – negdje centralno kontrolirana baza podataka prati tko što posjeduje. S gledišta Daija i kripto-anarhista, problem ovdje je taj što se omogućuje vladama da kontroliraju protok novca kroz regulaciju, a sami sudionici sustava moraju biti identifi-

cirani. Motivacija za stvaranje B-moneya upravo leži u tome – cilj mu je bio omogućiti online ekonomije koje su potpuno dobrovoljne, koje se ne mogu oporezivati ili regulirati prijetnjom sile. Dai je stoga osmislio dvije alternativne solucije.

U prvoj soluciji, umjesto centralnog entiteta koji kontrolira glavnu knjigu, svi sudionici održavaju zasebne kopije iste knjige. Svaki puta kada se objavi nova transakcija, svi sudionici ažuriraju svoje zapise. Ovakve knjige sastoje se od javnih ključeva s pripadajućim iznosima, ali bez pravih imena stvarnih osoba. Ovakav decentralizirani sustav i pristup srpiječava bilo koji pojedinačni entitet da blokira transakcije, dok istovremeno pruža određenu razinu privatnosti svim korisnicima.

Jednostavan primjer ovoga je sljedeći: pretpostavka je da su Osoba 1 i Osoba 2 korisnici b-moneya i obje osobe imaju javni ključ: Osoba 1 posjeduje javni ključ „A“, a Osoba 2 javni ključ „B“, za koje obje osobe kontroliraju svoje jedinstvene privatne ključeve. Oba njihova ključa sadrže b-money jedinice, primjerice 5 jedinica svaka osoba.

Ako Osoba 2 želi primiti dvije b-money jedinice od Osobe 1 (jer joj prodaje određeni proizvod), onda Osobi 1 šalje svoj javni ključ „B“. S pretpostavkom da Osoba 1 želi kupiti taj proizvod od Osobe 2, ona stvara transakciju u obliku poruke „2 b-money od A prema B“, gdje A označava javni ključ Osobe 1, a B javni ključ Osobe 2. Zatim Osoba 1 potpisuje poslanu poruku svojim privatnim ključem, koji odgovara javnom ključu A. Napisana i poslana poruka, kao i kriptografski potpis se potom šalju svim korisnicima b-moneya. Takva potpisana poruka će korisnicima dokazati da pravi vlasnik A svojim izborom šalje dvije b-money jedinice B-u. Svi korisnici obzirom na to ažuriraju svoje knjige – pripisuju ukupno 3 b-money jedinice „A“, i ukupno 7 b-money jedinica „B“, na znajući tko se krije iza tih ključeva.

Ovakvo rješenje čuvanja identiteta i slanja sigurne i potvrđene transakcije trebalo bi biti poznato, jer je otprilike tako i Nakamoto osmislio Bitcoin 10 godina kasnije.

Drua verzija B-money

U ovoj drugoj verziji ne održava svaki korisnik verziju glavne knjige, već bi postojala dva tipa korisnika – obični korisnici i „poslužitelji“. Ovdje samo poslužitelji koji su povezani putem mreže za prijenos mogu održavati glavne knjige, a kako bi se provjerilo je li transakcija prošla kako treba, obični korisnici ju moraju provjeriti nasumičnim podskupom tih podlužitelja.

U teoriji bi svatko mogao biti poslužitelj, ali bi za to morao uplatiti određen iznos novaca na poseban račun, koji bi se onda koristio za potencijalne nagrade ili kazne za dokaz o zloupotrebi. Poslužitelji bi morali i periodično objavljivati i kriptografski potvrđivati vlasničke baze podataka u ovoj verziji.

Dai je u svojim prijedlozima obuhvatio i ranu verziju rješenja pametnih ugovora. Njegov oblik pametnog ugovora najviše podsjeća na kombinaciju sustava dokaza o udjelu i arbitražnog sustava, gdje obje strane ugovora i arbitar moraju položiti određena sredstva na poseban račun. Ovakvi pametni ugovori nisu imali ugrađen sustav rješavanja eventualnih sporova – u slučaju sporova bilo bi moguće da različiti korisnici, ili poslužitelji, prilagode vlastite knjige na različite načine, zapravo ostavljajući stanje knjiga na mreži van konsenzusa. Vjerojatno bi potencijalne kazne za varanje bile previsoke, da bi uopće bilo isplativo to riskirati.

Monetarna politika vezana uz B-money

Upravo je najveća razlika između B-moneya i Bitcoina vezana uz predloženu monetarnu politiku Daija. Monetarna politika Bitcoina smatra se vrlo jednostavnom – kako bi se kriptovaluta uvela u opticaj, 2009. godine kada je provedeno prvo rudarenje, dobivano je po 50 bitcoina kao nagrada za rudarenje bloka. Nagrada bitcoinima se mijenja, tako je primjerice nagrada smanjena za polovinu (*eng. halving*) nakon što je izrudareno 210 000 blokova, te je tada iznosila 25 bitcoina. Trenutno se za rudarenje dobije nagrada od 6.25 bitcoina, a idući, četvrti halving dogodit će se u travnju 2024. godine, kada će nagrada iznositi 3.125 bitcoina. Broj će se dalje samo smanjivati, do nešto više od stotinu godina od danas, kada će posljednji Bitcoin biti izrudaren, a količina ukupno izdanih bitcoina bude nešto ispod 21 milijun. Idealnost monetarne politike bitcoina čest je predmet rasprave, ali je jasno kako do danas nije proizvela stabilnu vrijednost valute.

Zanimljivosti vezane uz bitcoin *halving* i ostalu statistiku moguće je pratiti na stranici *Bitcoin Block Reward Halving Countdown*, [13]

Suprotno tome, stabilna vrijednost je izričito bila dio Daijeva prijedloga. Kako bi se ta stabilnost postigla, vrijednost B-moneya trebala bi biti povezana s vrijednošću teorijske košarice robe. Primjera radi, 50 jedinica B-moneya vrijedile bi za jednu košaricu robe, što bi trebalo osigurati stabilnu vrijednost jer bi se sa istih 50 jedinica moglo kupiti istu košaricu u prošlosti, sadašnjosti i budućnosti, odnosno neovisno o vremenu koje prođe. A kako bi se izdali novi novčići, krosnici bi trebali odrediti koliko neka košarica robe vrijedi, košta, u odnosu na rješenje računalnog problema PoW (dokaza rada).

Jedan od najvažnijih problema B-moneya koji je ostao neriješen ili nedovoljno specificiran je taj što model suglasnosti ovog prijedloga nije bio dovoljno robustan, što najbolje pokazuje predloženo rješenje pametnih ugovora.

Dakle, u Daijevom predloženom sustavu svaki sudionik održava zapisnik o tome koliko novaca pripada svakom pseudonimu (korisniku), a prijenos novca ostvaruje se putem javnog objavljivanja digitalno potpisane poruke. Navedeno se koristi i u sustavu Bitcoina. Također, način na koji Bitcoin stvara novac na temelju ulaganja računalnog vremena sličan je Daijevom, gdje rješavanje zahtjevnog računalnog problema predstavlja dokaz rada koji bude nagrađen novcem.

Iako Daijev prijedlog nikada nije bio implementiran i korišten, nije bio zaboravljen – B-money postao je prvom referencom u Bitcoin bijeloj knjizi, dokumentu koji predstavlja izvorni nacrt za stvaranje Bitcoina – prve decentralizirane digitalne valute. Unatoč sličnostima dizajna B-moneya i Bitcoina, postoji mogućnost da Satoshi Nakamoto uopće nije bio inspiriran Daijevom idejom – sam Dai smatra kako je izumitelj Bitcoina do ideje došao neovisno o njegovoj.

Zanimljivost: Prema Wei Daiu je nazvana najmanja denominacija ethera, kriptovalutnog novčića koji se koristi u Ethereum mreži. Jedan ether jednak je 1.000.000.000.000.000 **wei** (10^{18}), odnosno, jedan wei je jedna bilijuntina ethera.

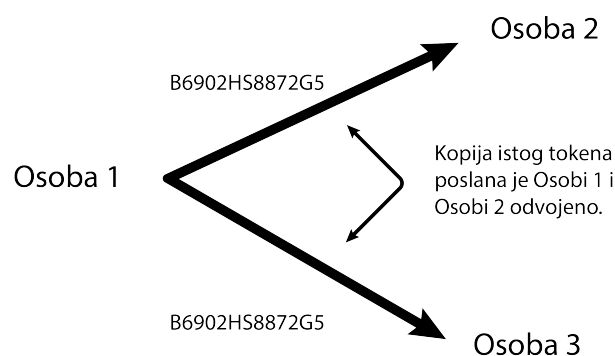
4.3 Arhitektura

Bitcoin se oslanja na peer-to-peer mrežu (P2P) računala nazvanu čvorovi. Čvorovi imaju zadaću procesuiranja transakcija i održavanja svih evidencija o vlasništvu. Svaka osoba može preuzeti besplatni otvoreni Bitcoin softver i postati čvor. Svi čvorovi se tretiraju jednako – nijedan od njih nije pouzdan. No, sustav se temelji na pretpostavci da će većina

računalne snage dolaziti od ispravnih čvorova. Evidencije o vlasništvu su replicirane na svakom punom čvoru. Nakon provjere, transakcije se šalju drugim čvorovima u peer-to-peer mreži. Ostali čvorovi će ponoviti provjeru i prenijeti transakciju drugim čvorovima. U nekoliko sekundi, transakcija bi trebala doseći većinu čvorova u mreži. Transakcije se zatim čuvaju u bazama podataka čvorova, čekajući da budu unesene u blok-lanac, koji je javni zapis svih transakcija koje su ikad nastale u Bitcoin mreži. Blok-lanac nije samo jednostavan popis potvrda transakcija. Posebno je osmišljen kako bi riješio problem dvostrukog trošenja u P2P mreži s nepouzdanim čvorovima. Cilj je odrediti kronološki redoslijed transakcija kako bi se prva uplata mogla prihvatiti, a druga odbaciti. Stoga P2P mreža mora imati način dogovaranja o redoslijedu transakcija, iako neki čvorovi mogu pokušati sabotirati sustav.

4.4 Problem dvostrukog trošenja (eng. *Double-spending Problem*)

Problem vezan za transakcije nije u samom slanju kriptovalute, već u tome koliko puta isti novac može biti poslan, uz što je vezan problem dvostrukog trošenja. Ovaj problem ukazuje na propust u sustavu koji omogućuje korisniku da potroši isti novac više puta. U idealnom svijetu, isti novac moguće je potrošiti samo jednom, a kako bi se zadovoljio ovaj zahtjev, postoje mehanizmi koji sprječavaju korisnika da kopira, ili ponovno stvara novac iznova i iznova. Novčanice i kovanice bilo koje valute imaju posebne značajke koje potvrđuju njihovu autentičnost, te se iste ne mogu krivotvoriti. Ovakav koncept je teže prilagoditi digitalnom svijetu, jer se datoteke, ili konkretnije bitovi, mogu jednostavno kopirati. Primjerice (Slika 4.3), Osoba 1 ima 50 Bitcoina koje želi poslati Osobi 2. Prije provođenja te transakcije, Osoba 1 napravi kopiju i šalje te iste tokena (B6902HS8872G5) Osobi 3. Obzirom da Osoba 2 i Osoba 3 nisu svjesne drugih transakcija koje Osoba 1 provodi, postaju žrtve krivotvorenja te postoji mogućnost urušavanja sustava.



Slika 4.3: *Primjer dvostrukog trošenja gdje Osoba 1 šalje kopije istog tokena Osobi 2 i Osobi 3.*

4.4.1 Rješenje problema dvostrukog trošenja

Rješenje dvostrukog trošenja krije se u blockchainu, koji bilježi sve provedene transakcije. S gledišta podataka, on predstavlja neprestano rastuću listu zapisa povezanih jedan za drugim, u nizu. Svaki od ovih zapisa nazvan je blokom, koji sadrži transakcije, a blokovi su vezani kriptografskim principima – ukoliko je jedan blok uređen izvan reda, ruši se

cijeli lanac. Ovo zapravo blockchain čini nepromjenjivim, gdje transakcije ne mogu biti mijenjane ili prepisane. Ovakav raspored sprječava ranije spomenutu Osobu 1 u slanju 50 Bitcoina Osobi 3, jer blockchain već sadrži provedenu transakciju Bitcoina prema Osobi 2. U slučaju da Osoba 1 napravi kopije tokena i pokuša ih poslati Osobi 3, blockchain otkriva da Osoba 1 više nema token (poslan je Osobi 2) te će to dovesti do odbijanja transakcije. Navedeno rješava problem dvostrukog trošenja, korištenjem tehnologije ulančanih blokova, čime je uspješno osigurana mogućnost prijenosa novca putem digitalnog medija, a bez prisutnosti središnjeg entiteta.

4.5 Vlasništvo

Postoje dva načina praćenja vlasništva nad valutom:

1. Posjedovanje tokena koji neovisno predstavlja vrijednost (npr. papirnati novac ili kovanica).
2. Posjedovanje ključa koji kontrolira pristup zapisima u registru (npr. čekovi, kreditne kartice, Paypal i Bitcoin).

Dizajniranje decentralizirane valute je izazovno jer nije očito kako bilo koja od ovih metoda može biti korištena bez nekog pouzdanog autoriteta poput banke. U prvom načinu praćenja, netko mora izdavati tokene, a u drugom načinu netko mora održavati registar. Ako bilo tko može izdavati tokene ili uređivati registar, sustav će sigurno s vremenom propasti. Bitcoin koristi metodu temeljenu na registru, ali uspijeva zahvaljujući inovativnoj metodi koja omogućuje distribuiranoj mreži nepouzdanih sudionika održavanje pouzdanog registra.

Bitcoinov registar, poznat kao blok-lanac, može se shvatiti kao zapis potvrda za sve transakcije koje su ikada nastale u Bitcoin sustavu. Za razliku od tipičnog bankovnog registra, ne sadrži stanje računa. Umjesto bilježenja količine bitcoina za svakog vlasnika, zapisuje vlasnika za svaku količinu bitcoina koja se prenese. Vlasnik je jednostavno primatelj naveden u potvrdi transakcije u blok-lancu (dok se bitcoini iz te transakcije ne potroše). Da bi potrošio bitcoine, vlasnik stvara novu transakciju koja uzima bitcoine iz prethodne transakcije (one koje su mu poslone) i dodjeljuje ih nekome drugome. Vlasnik je jedini koji ima sposobnost stvaranja takve transakcije jer je potreban njegov digitalni potpis.

Prethodna transakcija iz koje se uzimaju bitcoini naziva se unosom. Kada se transakcija koristi kao unos, kažemo da je ta transakcija potrošena jer će sva njena vrijednost biti poslana primateljima i ta transakcija se više nikada ne može koristiti kao unos. Ako je vrijednost unosa veća od željenog iznosa plaćanja, to nije problem – transakcije omogućuju više primatelja, pa vlasnik može poslati dio vrijednosti unosa natrag na svoju adresu kao povrat.

4.6 Novčanici za kriptovalute

Novčanik za kriptovalute, kibernetički novčanik ili e-novčanik je ustvari digitalna torbica za digitalne valute. Bitcoin novčanik ne pohranjuje bitcoine, već samo digitalne ključeve koji su potrebni za pristup, primanje i potpisivanje transakcija s vlastitim bitcoinima. Dakle, kriptovalute se ne nalaze u novčaniku, već su pohranjene u lancu blokova, a sam novčanik je potreban kako bismo imali pristup kriptovalutama.

Novčanik za kriptovalute je ustvari skup jedinstvenih javnih adresa, obično kombinacija slova i brojeva, što možemo usporediti s IBAN računom u banci. Adrese su kôdovi od 27-34 znaka, osjetljivi na velika i mala slova, koji izgledaju ovako:

1pZlBMKKNHCIIvxlh4rwO2SzGfvLyl77yY

Sam novčanik je zapravo medij koji pohranjuje privatni ključ, potreban za pristup kriptovalutama i korištenje u osobne svrhe. Dakle, novčanik ne pohranjuje fizički kriptovalute, već čuva ključeve potrebne za slanje kriptovaluta.

Ključevi u novčaniku su kriptografski kôdovi koji omogućuju prijenos bitcoina s adresa korisnika na druge adrese. Ključevi izgledaju poput adresa, ali su dulji i sadrže 51 znak. Ako netko drugi dobije pristup ključevima u novčaniku korisnika, moguće je da će korisniku ukrasti bitcoine prijenosom na svoju adresu. Ako zlonamjerni napadač može provaliti u računalo korisnika, vjerojatno će moći dobiti i njegove ključeve. Neki se korisnici iz sigurnosnih razloga ne osjećaju sigurno držati svoj novčanik na osobnom računalu. Srećom, dostupni su sigurniji načini čuvanja novčanika.

Kako bi korisnik imao pristup kriptovalutama putem novčanika, potrebne su dvije vrste ključa – javni i privatni ključ.

Javni ključ smije se dijeliti javno, iz njega se generira adresa za primanje kriptovaluta, a sam se generira iz privatnog ključa. **Privatni ključ** ne smije se dijeliti javno, zapisan je u obliku nasumičnih slova i brojeva te se njime potpisuju transakcije.

Dakle, javni ključ omogućuje primanje kriptovaluta, dok privatni ključ omogućuje transakcije, odnosno trošenje kriptovaluta. Samo osoba koja posjeduje oba ključa, javni i privatni, može upravljati novčanikom, odnosno ovjeravati i potpisivati transakcije. Kako bi se provelo plaćanje bitcoinima, u osnovi je potreban samo privatni ključ i adresa primatelja, odnosno javni ključ primatelja. U praksi je rijetko kada potrebno unijeti tu drugu adresu – prikladnije je skenirati QR kod.

4.6.1 Odabir novčanika

Kakav novčanik će netko odabrati ovisi o tome što netko želi postići s novčanikom. Desktop novčanik, primjerice, za brzo plaćanje u pokretu nije najpraktičnije rješenje. S druge strane, hardverska rješenja koja nisu povezana s internetom mogu poslužiti kao sigurna opcija, ali nisu prikladna za brze transakcije. Ovisno o tome kako netko želi koristiti svoje Bitcoine, mogu stvoriti jedan ili više novčanika s različitim pružateljima usluga. Kako bi korisnik odabrao adekvatan novčanik, nužno je zapitati se na što stavlja naglasak – anonimnost, prilagođenost korisniku i praktičnost, brzina i, često najvažnije, sigurnost. Većini korisnika je sigurnost intuitivno najvažnija, jer se radi o stvarnom novcu.

Ovisno o vrsti novčanika (Desktop, Mobilni, Papirnati itd.) postoje različite stvari koje je potrebno uzeti u obzir.

4.6.2 Sigurnost ovisno o vrsti novčanika – naglasak na desktop novčanike

Ukratko, što se tiče desktop novčanika, vlastito računalo je najveći izvor opasnosti. Ne samo da ga je moguće kompromitirati, već se jednostavno može pokvariti. S druge strane, kod web i mobilnih novčanika korisnik često nema puno kontrole nad tim gdje se podaci pohranjuju i kako se točno provjeravaju update.

Tradicionalno, Bitcoin novčanici pohranjuju se kao datoteka (wallet.dat) na lokalnom računalu. Tu datoteku treba redovito održavati pažljivim sigurnosnim kopijama. To se

posebno odnosi na desktop novčanike i ima prednost što korisnik ima kontrolu nad samim novčanikom. Međutim, to zahtijeva stvaranje redovitih sigurnosnih kopija i, naravno, osiguravanje da je softver novčanika instaliran na računalu bez zlonamjernog softvera.

Za razliku od drugih vrsta novčanika, desktop novčanici imaju niz sigurnosnih aspekata koje treba uzeti u obzir. Pogledajmo ih prvo prije nego što se usredotočimo na mobilne i online novčanike.

Pravila za osiguranje novčanika

Na Bitcoin.org moguće je vidjeti popis s važnim faktorima za sigurnost desktop novčanika:

1. **Napraviti sigurnosnu kopiju:** ključno je napraviti sigurnosnu kopiju digitalnog novčanika. Budući da postoje različiti pružatelji usluga, važno je pažljivo se informirati o tome kako i što treba spremiti. U većini slučajeva, datoteka wallet.dat trebala bi biti prava. Ovisno o pružatelju usluga kojeg odaberete, ova datoteka može imati drugačije ime ili možda ne postoji.
2. **Šifriranje:** jednostavno spremanje wallet.dat datoteke ili lozinke nije dovoljno za stvaranje sigurne sigurnosne kopije. Stoga je ključno ne zaboraviti šifrirati sigurnosnu kopiju. To je važno, posebno ako korisnik planira pohraniti podatke online, primjerice, u Dropboxu.

Korištenje različitih mjesta za pohranu

Nerazumno je sve, uključujući sigurnosne kopije, pohranjivati na istom sustavu. Dobra mjesta za pohranu su tzv. "cold storages", odnosno ona koja nisu povezana s internetom - vanjski tvrdi diskovi, USB uređaji ili CD-ovi, a čak je i papir sjajna opcija. Preporučljivo je također fizički razdvojiti sigurnosne kopije, na primjer, pohraniti ih kod prijatelja.

Sigurnosne kopije i njihovo ažuriranje

Potpisivanje ili provjera transakcija važan je aspekt. Kao što je ranije napisano, s tradicionalnim desktop novčanicima, korisnik mora sam brinuti o sigurnosnoj kopiji ove datoteke. Mnogi trenutni novčanici koriste različita rješenja koja su puno jednostavnija, a opet jednako sigurna. Trenutačno se koriste dva tipa novčanika, gdje se pitanje sigurnosne kopije praktički automatski rješava.

Ovisno o tome koliko često se korisnik koristi svojim Bitcoinima, sigurnosne kopije brzo zastarjevaju. Prema vlastitoj upotrebi, korisnik bi se redovito trebao podsjećati da svoj novac ponovno osigura.

Ometanje i obmanjivanje

Sigurnosna kopija i šifriranje je minimalno što je nužno napraviti u svrhu zaštite računa, ali ometanje i obmanjivanje mogućeg napadača predstavljaju proširene mogućnosti zaštite računa. Nešto što se preporuča je primjerice koristiti i održavati veći broj Bitcoin novčanika, jer u slučaju kompromitiranja sustava, to može zbuniti napadača. Moguće je postaviti veći broj računa s malim iznosima koji su lako vidljivi, a budući da su ti računi povezani drugim „mamac“ računima, brzo je moguće saznati je li netko dobio pristup sustavu. Dakle, ne može naštetiti imati veći broj računa. Preporuka je i na samom početku poslati samome sebi nekoliko malih iznosa naprijed-natrag, sa različitih računa, kako biste se upoznali s radom i sustavom obavijesti.

4.6.3 Sigurne transakcije

Kod transakcija obično vrijedi sljedeće: tko god ima pristup osobnom privatnom ključu za novčanik, ima i pristup osobnom novcu. Kako bi se to izbjeglo, moguće je koristiti novčanike koji omogućuju samostalno upravljanje i lokalno pohranjivanje privatnog ključa. S druge strane, pohrana ključeva na serveru se obično ne preporuča, zbog manjka povjerenja.

Važno je i da se upravljanje ključem odvija lokalno, ali i da se pojedine transakcije potpisuju lokalno. Samo takvim načinom su transakcije dovoljno zaštićene.

Osim pitanja upravljanja ključem, važno je paziti i na to kako su računi zaštićeni i kako se odobravaju plaćanja kod pružatelja usluga novčanika. Iako je obično potrebna barem lozinka ili PIN, takva jednostavna zaštita je ranjiva. Većina novčanika koji se trenutno koriste nude kvalitetnija, višeslojna sigurnosna rješenja.

4.6.4 Dvofaktorska autentifikacija

Dvofaktorska autentifikacija je poznata zbog bankovnih računa. U ovom procesu se prijava provodi s brojem računa i PIN-om, a zatim se potvrđuju pojedinačne transakcije s TAN listom ili SMS kodom. Osnovna ideja je imati dva neovisna načina autentifikacije. Prilikom pokušaja kompromitiranja računa, napadač mora dobiti pristup više uređaja (na primjer, lozinke i fizičke TAN liste). Bitcoin novčanici obično ne koriste TAN listu, već je česta kombinacija korištenja lozinke ili PIN-a te SMS-a, e-pošte ili Google Authenticatora.

4.6.5 Multi-potpis

Multi-Signature računi, ili skraćeno Multi-Sig, predstavljaju važan aspekt u smislu sigurnosti novčanika. Ukratko, riječ je o adresi koja za izvršenje transakcija zahtijeva više od jednog ključa. Primjerice, novčanik može imati tri ključa, od kojih su za svaku transakciju potrebna najmanje dva. Moguće je imati i više ključeva, npr. pet od sedam. Tehnički, ovaj postupak poznat je kao "pay-to-script-hash" (P2SH) i implementiran je u Bitcoin-Coreu od 2012. godine. Omogućava izvršenje transakcija putem skripti umjesto jednog privatnog ključa. Ove adrese lako je prepoznati jer svaki Multi-Sig novčanik započinje s brojem tri umjesto s brojem jedan.

Iako ovo zvuči tehnički zahtijevno, postoje praktične prednosti koje su lako razumljive. Multi-Sig omogućuje da transakciju uvijek bude potpisana barem na dvama različitim mjestima. U najboljem slučaju, to su različiti uređaji, ali mogu biti i različite osobe. Ideja je smanjiti rizik od kompromitiranih uređaja.

Za tvrtke i pružatelje usluga novčanika, ovo otvara niz novih opcija sigurnosti. Na primjer, mogu svaku transakciju su-potpisati i istovremeno provjeriti postoji li vjerojatnost prevare. Istodobno, korisnici su zaštićeni, jer čak i ako su poslužitelji tvrtke hakirani, nitko ne može pljačkati račun korisnika bez njegova potpisa. Ovo također olakšava implementaciju računa s više sudionika, poput korporativnih računa. Multi-Sig novčanici su stoga preporuka za korištenje, jer su sigurnosni i prilagođeni korisnicima.

4.6.6 Razlika između Novčanika i Klijenta

Novčanik – skup podataka (npr. privatno-javni ključni par korisnika i njegova adresa/e) koji omogućuje korisniku primanje i slanje kriptovaluta putem ulaznih i izlaznih transakcija. Novčanik obuhvaća i mehanizme koji upravljaju tim podacima.

Klijent – softver koji povezuje korisnika s mrežom za određenu kriptovalutu. On obrađuje komunikaciju i ažurira sustav, suštinski pretvarajući računalo u čvor.

Neki novčanici za kriptovalute zahtijevaju samo pristup internetu dok drugi zahtijevaju instaliran softver, a postoje i oni koji koriste određenu aplikaciju i dodatni hardware, primjerice USB stick.

4.6.7 Podjela novčanika prema odnosu ključeva

Novčanici se prema odnosu ključeva dijele u tri kategorije:

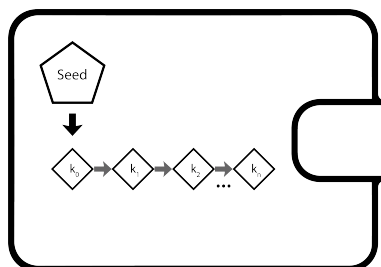
1. Deterministički novčanik
2. Hijerarhijski Deterministički novčanik (HD)
3. Nedeterministički novčanik

Deterministički novčanik

Deterministički novčanik (Slika 4.4) odnosi se na mogućnost obnavljanja novčanika pomoću matičnog sjemena (*eng. Seed*). Ova opcija predstavlja vrstu rješenja za sigurnosne kopije novčanika. Kako točno to funkcionira može zvučati apstraktno. Prije nego što je postojala ova deterministička metoda, novčanici su generirali nove adrese za Bitcoin transakcije, što je zahtijevalo česte sigurnosne kopije. Također, datoteka wallet.dat neprestano se povećavala kako bi zadržala sve te adrese. Deterministički postupak rješava ovaj problem omogućujući izračunavanje budućih adresa iz matičnog sjemena. Dakle, nije potrebno raditi sigurnosnu kopiju nakon svake transakcije, već je dovoljno zapamtiti dugi niz od dvanaest riječi koji se zatim proširuje za svako sljedeće pojavljivanje (niz +1, niz +2, itd.), što nije najpraktičnije rješenje.

Kod determinističkog novčanika dakle:

- svi ključevi proizlaze iz matičnog sjemena
- duljina *seed*-a je nepraktična
- koristi se mnemonička fraza.



Slika 4.4: Deterministički novčanik

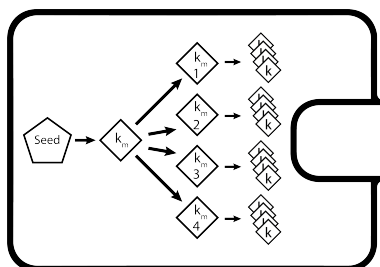
Hijerarhijski deterministički novčanik

Baš kao i kod determinističkog novčanika, hijerarhijski deterministički (HD) novčanik (Slika 4.5) generira se pomoću matičnog sjemena. Za korisnika je ova verzija praktičnija jer se u ovom slučaju *seed* ne mora proširivati. Bitna razlika je u tome što hijerarhijski deterministički novčanik stvara hijerarhijski uređeno stablo koje se može jednostavno obnoviti pomoću *seed*-a, odnosno novčanik sadrži ključeve izvedene u strukturi stabla. Za korisnika je to sigurno i jednostavno. Na primjer, na temelju jednog *seed*-a korisnik može stvoriti različite novčanike ili dodijeliti različita prava različitim korisnicima pomoću različitih privatnih ključeva (roditelj i dijete). Potonje omogućava zajedničke ili poslovne račune. Zbog jednostavnosti i sigurnosti mnogi novi pružatelji usluga preferiraju hijerarhijski determinističke novčanike. Ključno je za sigurnost korisnika da se *seed* generira

i upravlja lokalno, a ne da se čuva na nekom serveru. Većina današnjih novčanika za kriptovalute su upravo hijerarhijski deterministički novčanici.

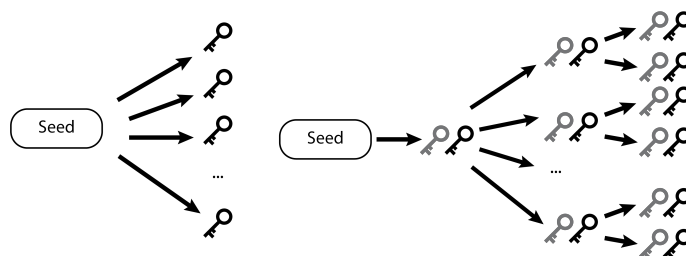
HD novčanik:

- ključevi su izvedeni u strukturi stabla
- nadređeni ključ može izvesti niz podređenih ključeva
- mogućnost lakšeg praćenja adrese novčanika



Slika 4.5: *Hijerarhijski deterministički novčanik*

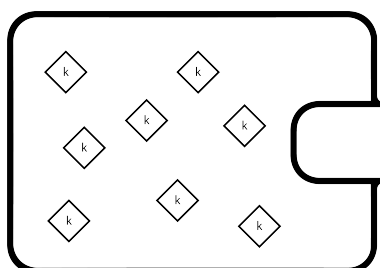
Iduća slika prikazuje usporedbu determinističkog (lijevo) i hijerarhijsko determinističkog (desno) novčanika (Slika 4.6):



Slika 4.6: *Usporedba determinističkog i hijerarhijsko determinističkog novčanika*

Nedeterministički novčanik

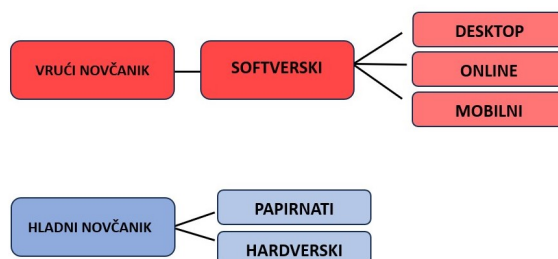
Nedeterministički novčanik (Slika 4.7) ne smatra se praktičnim za korištenje, jer je svaka adresa novi privatni ključ koji se mora sigurnosno kopirati. U suprotnom se riskira gubitak kriptovaluta kojima novčanik upravlja.



Slika 4.7: *Nedeterministički novčanik*

4.7 Podjela novčanika na vruće i hladne novčanike

Osim prve podjele, koja se temelji na odnosu ključeva, postoji i podjela (Slika 4.8) na vruće i hladne novčanike. Vrući novčanici su softverski (Desktop, Online i Mobilni novčanik), dok su hladni podijeljeni na Papirnate i Hardverske.



Slika 4.8: Podjela novčanika na vruće i hladne

Vrući novčanici - Softverski novčanici

Softverski novčanici su danas najčešće korištena vrsta kriptonovčanika, a naziv ukazuje na to da su dostupni kao bilo koja druga softverska aplikacija. Pripadaju skupini vrućih novčanika zbog povezanosti s internetom, što osigurava njihovu bolju dostupnost. U softverske novčanike spadaju Desktop, Online i Mobilni novčanici.

Desktop novčanici

Pristup desktop novčaniku omogućen je putem softvera instaliranog na računalo, bilo prijenosno ili stolno, što ga čini jednostavnim i preporučljivim za korištenje. Ovaj novčanik koristi se i za kratkotrajnu pohranu, kao i za čuvanje manjih iznosa kriptovaluta.

Međutim, zanimljivo je primijetiti da su desktop novčanici kritizirani zbog "ranjivog okruženja". To se obično odnosi na činjenicu da su računala općenito online i izložena opasnostima od zlonamjernog softvera. Stoga je važno obratiti pažnju na sigurnosne mehanizme i redovito raditi sigurnosne kopije.

Desktop novčanik preuzima se s interneta, a prvi korak u osiguravanju novčanika je postavljanje lozinke putem postavki. Funkcionalnost klijenta je jednostavna i lako razumljiva.

Neki od poznatijih desktop novčanika su Bitcoin Core, Exodus, Electrum, Guarda i dr.

Prednosti desktop novčanika leže u tome što privatni ključevi i javne adrese nisu pohranjeni na poslužitelju treće strane, kao i to da ako računalo nije povezano s internetom sama pohrana je sigurna. Suprotno tome, nedostatak desktop novčanika je u tome što ukoliko je isti povezan s internetom, njegova sigurnost je smanjena. Također, ukoliko dođe do kvara računala i nije napravljena sigurnosna kopija, postoji mogućnost gubitka kriptovaluta.

Primjer Desktop novčanika - Bitcoin Core

Bitcoin Core, ranije poznat i kao BitcoinQT, može se smatrati majkom svih Bitcoin novčanika. To je prvi Bitcoin klijent koji je originalno razvio osnivač Satoshi Nakamoto. Trenutno, zajednica aktivno podržava i dalje razvija ovaj klijent, a opasnost od sigurnosnih

propusta smatra se niskom. Klijent zapravo nije Bitcoin novčanik, ali uključuje jedan u svom programskom opsegu. Naime, Bitcoin Core je potpuni čvor u Bitcoin mreži koji, kako je opisano u prethodnim poglavljima, validira transakcije. Međutim, nije moguće koristiti ga za samostalno rudarenje.

Online (WEB) novčanici

Pri korištenju online (web) novčanika potrebna je prijava putem web preglednika, a spremanje se vrši na poslužitelja u vlasništvu treće strane, odnosno novčanik nije lokalno pohranjen kao datoteka na računalo. Osim što postoji u web pregledniku, dostupan je i kao aplikacija za pametne telefone. Kod online novčanika postavlja se pitanje vrši li se validacija transakcija putem interneta i - posebno važno - pohranjuju li se privatni ključevi na poslužitelju. Često je to slučaj. Vezano uz to potrebno je biti na oprezu, jer većina internetskih usluga zahtijeva određenu mjeru povjerenja. Ipak, ne smiju se zanemariti njihove prednosti. Najuočljivija prednost je dostupnost novčanika čim je korisnik online. Često nude i dodatne funkcionalnosti, poput trgovinskih platformi ili mjenjačnica.

Prednost Online novčanika je jednostavan pristup novčaniku i sredstvima putem web preglednika ili mobilne aplikacije, kao i to što treća strana ima odgovornost za sredstva i ključeve. Upravo u toj trećoj strani krije se nedostatak ovog novčanika – potrebno je povjerenje da neće doći do krađe sredstava od treće strane i da će sredstva biti čuvana od napada.

Neki od poznatijih Online (web) novčanika su Coinbase, Binance, Trust wallet, Meta-mask i dr.

Primjer Online (web) novčanika - Coinbase Online novčanik

Coinbase se smatra jednim od glavnih pružatelja usluga na tržištu Bitcoina. Početkom 2015. godine, tvrtka je otvorila Coinbase Exchange, prvu državno reguliranu Bitcoin burzu u Sjedinjenim Američkim Državama. Ovo pruža dodatnu sigurnost, posebno s obzirom na značajnu financijsku podršku ulagača u tvrtku. Coinbase olakšava korisnicima kupnju ili prodaju Bitcoina, a za to je potrebno samo povezati račun s bankovnim računom. Međutim, ova mogućnost dostupna je samo korisnicima iz određenih zemalja.

Coinbase također nudi alat za trgovce koji im omogućuje prihvaćanje Bitcoina i trenutnu konverziju u lokalnu valutu. To pomaže trgovcima izbjeći valutne rizike i jednostavno integrirati Bitcoine u svoje poslovanje. Iako Coinbase ima mnogo korisnika, također privlači značajan broj kritika. Glavna kritika odnosi se na to da Coinbase, strategijom usmjeravanja prema širem krugu korisnika, snažno centralizira svijet Bitcoina i gubi na anonimnosti. Korisnici moraju pristati na više uvjeta korištenja nego kod drugih pružatelja usluga. Također, kod Coinbasea korisnici nemaju izravnu kontrolu nad svojim ključevima jer ih čuva tvrtka, a korisnik ih ne može vidjeti. Ovaj nedostatak izaziva sumnje u privatnost podataka korisnika.

Mobilni novčanici i Bitcoin aplikacije

Mobilni novčanici odlični su za korištenje dok je korisnik u pokretu, jer je pristup jednostavan – putem aplikacije instalirane na pametnom telefonu.

Pored sigurnosti, za mobilni novčanik posebno su važni brzina i jednostavna upotreba. Međutim, ovdje je ključno pitanje prave platforme. Mnoge mobilne aplikacije podržavaju samo iOS ili Android, dok je samo nekoliko njih dostupno na više platformi.

Prednosti mobilnog novčanika su brz i jednostavan pristup, kao i veća sigurnost korištenja u odnosu na online novčanik, a nedostatak je upravo smanjenje sigurnosti ukoliko je uređaj povezan s internetom, kao i rizik od gubitka kriptovaluta ukoliko dođe do oštećenja ili gubitka uređaja (gubitak mnemoničke fraze).

Primjer mobilnog novčanika - GreenAddress aplikacija

GreenAddress s bogatim značajkama i visokim sigurnosnim standardima, ozbiljna je konkurencija drugim novčanicima. Korisnici dobivaju hijerarhijski deterministički novčanik s Multi-Sig značajkom.

Prilikom prvog pokušaja stvaranja računa, korisnici dobivaju dugačku lozinku (24 riječi) koju trebaju zapamtiti. Najbolje je odmah koristiti opciju dodatne zaštite lozinke za tu frazu. Nakon toga, korisnici moraju odabrati kako će se 2-faktorska autentifikacija izvršiti - putem SMS-a, telefona, Google Authenticatora ili e-pošte. S odgovarajućim kodom, korisnici se prvi put prijavljuju i sada postavljaju još jednu lozinku koju mogu koristiti umjesto duge lozinke.

Za plaćanja, GreenAddress koristi Multi-Sig, ali ovdje radi s 2-2 ključa. Jedan ključ posjeduje korisnik, a drugi GreenAddress. U cilju katastrofalne situacije (npr. ako GreenAddress odjednom nestane), osmislili su nešto zanimljivo pod nazivom "nLockTime transakcije". Praktički, sredstva na novčaniku sama "ističu" s vremenom. Stoga je potrebno redovito prenositi sredstva kako bi se novčanik mogao dalje koristiti. Ako GreenAddress nestane, korisnik bi samo trebao čekati do tog datuma isteka.

Ako 2-2 ključa nisu dovoljna, korisnici mogu jednostavno stvoriti 2-3 račun pritiskom na gumb. Međutim, time se gubi zgodna značajka "instant transakcija". Podsjetnik: budući da se Bitcoin transakcije uvijek moraju provjeravati od cijele mreže, to traje određeno vrijeme. To je nužno kako bi se spriječilo višestruko trošenje Bitcoina. GreenAddress to ubrzava tako da djeluje kao pouzdani posrednik uz pomoć posebnog Co-Signature-a (supotpisa).

Kao i kod drugih računa, korisnici mogu postavljati vlastita ograničenja, prijavljivati se putem Facebooka u Watch-Only modu i čak slati novac SMS-om. Ono najbolje: za razliku od većine drugih ponuda, GreenAddress je dostupan na više platformi, bilo pametnom telefonu ili na stolnom računalu.

Zaključno, GreenAddress nudi izvrstan novčanik koji je siguran, praktičan i stvarno jednostavan za korištenje, a posebno je pogodan za pametne telefone. Ono što se GreenAddressu zamjera je što sprema osobne podatke poput IP adrese. No, korisnici ipak ne moraju davati svoj broj telefona za 2-faktorsku autentifikaciju.

Hladni novčanici

Općenito vrijedi da svaki novčanik koji je na bilo koji način povezan s internetom podložan je ranjivosti. Kako bi se ta mogućnost smanjila, stvorena su tzv. Cold Storage rješenja (skupina hladnih novčanika). To su u osnovi novčanici koji ne pohranjuju ništa na internetu, računalu ili pametnom telefonu, što ih čini sigurnijima, ali se ne smatraju i praktičnima ili korisniku prilagođenima. Cold Storage se smatra dobrim rješenjem kao dodatni novčanik. U hladne novčanike spadaju papirnati i hardverski novčanici.

Papirnati novčanik: BitAddress

Zvuči iznenađujuće, ali Bitcoin novčanik ne mora nužno biti digitalan. U osnovi, ispisani javni i privatni ključ potpuno su dovoljni - i upravo zato što takav ispis nije online, smatra

se posebno sigurnom alternativom svim dosad navedenim mogućnostima. Novčanik se brzo stvara, pri čemu se dobije javni i privatni ključ koje je moguće ispisati. Kako bi se prenijeli Bitcoin na novčanik, koristi se javni ključ kao i uvijek, a da bi se ponovno povukli, stvori se novi korisnički račun, primjerice na Blockchain.info, gdje se unese privatni ključ i Bitcoin su opet tu. Kodovi koji su dobiveni pri ispisu šifri ključeva na papiru, moraju se skenirati kako bi se transakcija mogla izvršiti. Iako papirnati novčanik nije najpraktičniji, pogotovo ako ne želite svoj novčanik stvarno koristiti za plaćanja, smatra se dobrim odabirom za isprobavanje i dodatno sigurnosno rješenje. Što se hladnih novčanika tiče, papirnati novčanik manje je siguran u odnosu na hardverski.

Prednosti papirnato novčanika leže u izoliranost od vanjskih utjecaja, uključujući napada od zlonamjernog napadača, u pogodnosti za sigurnosnu kopiju te je omogućeno sigurno generiranje privatnog ključa i adrese. Nedostatci su, s druge strane, moguća degradacija materijala, kao i kompliciranija upotreba gdje je nužno učitavanje privatnog ključa u računalo.

Hardware novčanici: Trezor i Ledger Wallet

Naposljetku, postoje i hardverske varijante novčanika, koje također spadaju u hladnu skupinu novčanika, unutar koje su najsigurnija opcija. Hardverski novčanici se koriste primarno za pohranu kriptovaluta, obzirom da se sa samog uređaja ne može izvršiti transakcija ili kupovina.

Postoje primjerice Trezor i značajno jeftiniji Ledger Wallet. Oba su vrlo praktična. Trezor se napaja putem Micro-USB kabela, dok manji Ledger Wallet više nalikuje USB-u.

Za oba uređaja potreban je poseban kod kako bi se odobrilo plaćanja. Kod Trezor novčanika se prikazuje na minidispleju na uređaju, dok kod Ledger novčanika korisnik dobiva zasebnu sigurnosnu karticu.

U različitim usporedbama možda se ne čini nužno tako, ali tester su uglavnom mišljenja da integrirani zaslon Trezora pruža dodatnu zaštitu od zlonamjernog softvera na računalo. Tom riziku su novčanici izloženi kada ih se poveže s računalom.

Plaćanja su očito kompliciranija u usporedbi s mobilnim novčanicima, jer ih uvijek treba potpisati s uređajem i odgovarajućim softverom. Prema tome, oni su namijenjeni više korisnicima koji žele osigurati značajne iznose, za što su izvrsni, ali postoje početna ulaganja.

Koraci za inicijalizaciju hardverskog novčanika:

- Preuzimanje potrebnog softvera – aplikacija ili browser
- Spajanje novčanika na računalo
- Pokretanje softvera kojim se upravlja novčanicom
- Ažuriranje ugrađenog programa (engl. Firmware) na novčanicu
- Odabiranje PIN koda
- Zapis mnemoničke fraze (24 riječi) koja će se koristiti

Prednosti hardverskog novčanika su te što je jedan od najsigurnijih načina pohrane kriptovaluta te je relativno praktičan i jednostavan za upotrebu. Nedostatak je taj što je cijena uređaja, koji zahtijeva spajanje na računalo, visoka, te je ovakav novčanik podložan prirodnim i drugim opasnostima.

Obzirom na mnoge pružatelje usluga, odabir novčanika nije lak, pogotovo jer postoji mnogo dobrih rješenja. Opća preporuka je isprobati nekoliko različitih novčanika, kao i unaprijed razmisliti o tome što korisnik očekuje od, i za što želi koristiti novčanik, a pitanje

koliko Bitcoin korisnik želi pohraniti na svom novčaniku važan je kriterij za donošenje odluka.

Ako, primjerice, korisnik planira pohraniti samo manje iznose na Bitcoin računu, dobro je razmisliti o većoj praktičnosti, a manjoj sigurnosti novčanika. S druge strane, ako korisnik namjerava pohraniti i koristiti veće iznose ili ulagati uštedevinu, nužno je okrenuti se novčanicima s većom sigurnosti. Prednost se zbog praktičnosti često daje mobilnim novčanicima, a putem njih je moguće i jednostavno vježbati transfer Bitcoin, ako se stvore primjerice dva novčanika.

4.7.1 Popunjavanje novčanika

Nakon odabira novčanika, idući korak je napuniti ga kriptovalutom Bitcoin. Najjednostavnija opcija za punjenje novčanika je korištenje usluga koje prihvataju određenu valutu, primjerice euro ili američki dolar, te ih šalje u obliku Bitcoin na adresu koju korisnik navede. Ako je korisniku cilj postići najbolju ponudu, preporuka je koristiti burzu, koja omogućuje podnošenje naloga za kupnju ili prodaju Bitcoin po određenim cijenama ili jednostavno izvršavanje naloga po trenutnoj tržišnoj cijeni, koje mogu biti izražene u različitim valutama.

Još jedan način za dobivanje Bitcoin, onaj kojim se Bitcoin inicijalno stavljaju u opticaj, je rudarenje. Prilikom rudarenja korisnik je plaćen Bitcoinima za pokretanje računala koje obrađuje transakcije za Bitcoin mrežu.

4.7.2 Slanje plaćanja

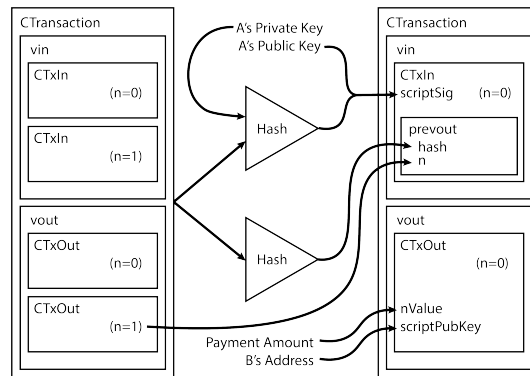
Nakon što Bitcoin postoje u novčaniku korisnika, stanje je moguće provjeriti na kartici „Pregled“ u Bitcoin klijentu. Upravo se Bitcoin klijent koristi kako bi se provelo slanje sredstava bilo kojem drugom korisniku Bitcoin, za što je potrebna jedna od njihovih adresa. Nakon odabira odredišne adrese, ista se unosi u karticu „Pošalji“, uz iznos koji se namjerava poslati primatelju. U ovom procesu se pošiljatelj ne mora brinuti o unosu pogrešne adrese, jer postoji ugrađena provjera – ako postoje pogreške, klijent će ih otkriti i odbiti namjeravanu transakciju odnosno plaćanje. Mreži je nakon slanja potrebno otprilike sat vremena za potvrdu transakcije, a kada ista bude dovršena, primatelj će vidjeti porast stanja u novčaniku. Zbog dugog vremena potvrde transakcije, Bitcoin nije idealan za transakcije u trgovinama, ali trgovci i dalje mogu slobodno prihvatiti djelomično ili nepotvrđene transakcije.

4.8 Transakcije

Svaka pojedinačna transakcija mora biti zabilježena u blockchainu. Putem blockchaina sudionici uspostavljaju suglasnost o statusu sustava. One transakcije koje su potvrđene stoga moraju biti implementirane u blok.

Kada Bitcoin korisnik pokrene plaćanje, klijent stvara poruku transakcije i šalje je P2P mreži. Transakcija sadržava sljedeće informacije, prikazane u nastavku s CTxIn i CtxOut:

```
class CTransaction
{
    int nVersion;
    std::vector<vin> vin;
    std::vector<vout> vout;
    unsigned int nLockTime
}
```



Slika 4.9: Dijagram prikazuje prijenos Bitcoina gdje A šalje bitcoine B-u. Na lijevoj strani transakcije prikazani su višestruki ulazi (CTxIn) u vin i višestruki izlazi (CTxOut) u vout kako bi se ilustriralo da su vin i vout nizovi. Oznake "(n=0)" i "(n=1)" označavaju poziciju u nizu. Sadržaj ulaza (CTxIn) i izlaza (CTxOut) s lijeva su skriveni radi pojednostavljenja dijagrama.

U osnovi, poruka transakcije nabraja skup ulaza (vin) koji se odnosi na prethodne transakcije, i skup izlaza (vout) koji određuje određene adrese. To omogućuje transakciji da povuče novac iz više izvora, objedini ga, a zatim ga distribuira prema više odredišta. Naravno, bilo koja transakcija koja distribuira više novca nego što povlači bit će smatrana nevažećom i bit će ignorirana. Varijabla nVersion je broj verzije transakcije kako bi P2P mreža i dalje mogla funkcionirati čak i kada različiti čvorovi pokreću različite verzije Bitcoin koda. Varijabla nLockTime može se koristiti kako bi se spriječilo procesuiranje transakcije prije određenog vremena, što je korisno za sklapanje ugovora.

```
class CTxIn
    COutPoint prevout;
    CScript scriptSig;
    unsigned int nSequence;
class COutPoint

    uint256 hash;
    unsigned int n;
```

Ulaz (CTxIn) referencira izlaz prethodne transakcije (prevout), koji je izlaz koji će biti potrošen. Da bi se jedinstveno referencirao izlaz, dovoljno je pružiti sažetak transakcije u kojoj se izlaz nalazi (hash) i indeks izlaza unutar vout vektora te transakcije (n). Upravo su ti podaci sadržani u COutPoint, vrsti prevout. Ovaj izlaz koji se referencira u prevout bit će potpuno potrošen. Ako korisnik želi potrošiti samo dio prethodnog izlaza, može stvoriti dodatni izlaz u novoj transakciji koji upućuje natrag na vlastiti novčanik, slično kao primitak promjene u gotovinskoj transakciji.

Ulazi također specificiraju scriptSig koji sadrži javni ključ vlasnika i potpis kako bi se dokazalo da potrošač posjeduje izlaz koji se troši. Tip CScript proširuje std::vector<unsigned char>, pa je vrsta klase niza znakova. Varijabla nSequence, zajedno s nLockTime, koristi se za sklapanje ugovora.

```
class CtxOut
    int64 nValue;
    CScript scriptPubKey;
```


Jednostavan izlaz transakcije (CTxOut) specificira adresu (u scriptPubKey) i iznos koji će biti poslan toj adresi (nValue), određen u satoshima, najmanjoj jedinici Bitcoin valute, vrijednoj 1/100.000.000 bitcoina. Skripta je prilagodljiva, pa može biti složenija od jednostavnog određivanja odredišne adrese. Kompleksnije skripte mogu se koristiti za stvaranje prilagođenih ugovora koji sprječavaju završetak transakcije dok se ne ispune određeni uvjeti.

4.8.1 Verifikacija transakcije

Nakon slanja nove transakcije u P2P mrežu od strane korisnika, ostali čvorovi u mreži nastojat će je ugraditi u blok lanac. Prvi korak u ovom procesu je osigurati da je poslana transakcija valjana, a bitno je poduzeti sljedeće:

1. Osiguravanje da transakcija prođe kroz razne provjere ispravnosti – provjere granica, sintaktička ispravnost i slično.
2. Odbijanje ako je ta određena transakcija već prisutna u blok lancu ili bazenu transakcija koje čekaju obradu. Ovo sprječava da jedna transakcija bude obrađena dva puta.
3. Za svaki unos ulančati scriptSig skript unosa sa scriptPubKey skriptom izlaza na koji se odnosi – izvršiti skript i verifikirati da je dobiveni rezultat „True“. Ako su skripti standardnog formata, potvrđuje se da je vlasnik bitocina pokrenuo transakciju.
4. Odbijanje ako je bilo koji od izlaza transakcije navedenih u unosima već korišten u drugoj transakciji blok lanca – sprječavanje dvostrukog trošenja.
5. Osiguravanje da je zbroj vrijednosti unosa veći, ili jednak zbroju vrijednosti izlaza. Ukoliko su unosi veći, razlika je naknada za transakciju, koja se plaća rudaru te transakcije.

4.9 Kreiranje Bitcoina i značenje rudarenja

Dok su za stvaranje „normalnih“ valuta poput eura ili američkog dolara (tzv. fiat novac) odgovorni monopolisti, odnosno centralne banke koje kontroliraju opskrbu novcem prema potrebi, posebno vezano uz inflacijsku stopu te prateći koliko se novca tiska i stavlja u opticaj, kod kriptovalute Bitcoin nije takva situacija. Ovdje nema državnog monopola koji upravlja proizvodnjom i količinom, već to generiraju korisnici, a nastanak kriptovalute Bitcoin vezan je uz postupak rudarenja (engl. Mining). Iako postoji gornja granica dostupnih količina kriptovalute Bitcoin – 21 milijun, ista će se postići tek otprilike u 2140. godini.

4.9.1 Rudarenje i postupak rudarenja

Proces stvaranja novih blokova naziva se rudarenje (eng. *Mining*), a čvorovi (engl. *Nodes*) koji obavljaju rudarenje nazivaju se rudari (engl. *Miners*). Rudarenje se sastoji od sljedećih koraka koji se izvode u kontinuiranoj petlji:

1. Prikupljanje transakcija koje su emitirane na P2P mreži u blok. Svaki rudar može proizvoljno odlučiti koje će transakcije uključiti u svoj blok. Transakcije obično imaju naknadu koju će rudar primiti ako se njegov blok prihvati, pa rudari imaju poticaj uključiti što je više transakcija moguće, do ograničenja veličine bloka od 1 megabajta.
2. Verifikacija da su sve transakcije u bloku valjane.

3. Odabir najnovijeg bloka na najdužem putu u lancu i umetanje sažetka njegova zaglavlja u novi blok.
4. Pokušaj rješavanja problema dokaza rada za novi blok i istovremeno praćenje dolaska novih blokova od drugih čvorova.

Ako se pronađe rješenje problema dokaza rada, novi blok dodaje se lokalnom blok-lancu i emitira na P2P mrežu, a ako drugi čvor prvi riješi problem dokaza rada, provjeravaju se dokazi rada i transakcije u njihovu bloku na valjanost. Ako provjere prođu, njihov blok dodaje se lokalnoj kopiji blok-lanca i prenosi se mreži – u suprotnom se njihov blok odbacuje.

Svi rudari istovremeno pokušavaju stvoriti nove blokove, a gotovo sav njihov napor usmjerava se na rješavanje problema dokaza rada. Budući da čvorovi ne mogu trenutačno komunicirati, mogu postojati blage razlike u verzijama blok-lanca između različitih čvorova u bilo kojem trenutku. No, u normalnim okolnostima, većina čvorova bit će suglasna. To je zato što se novi blokovi stvaraju reguliranim tempom od otprilike svakih 10 minuta, dok širenje novog bloka traje samo sekunde. Dakle, obično postoji razdoblje od, u prosjeku, 10 minuta u kojem svi čvorovi rješavaju problem dokaza rada, sve dok ga jedan nasumični čvor uspije riješiti. Nakon toga se novi blok emitira, a u roku nekoliko sekundi svi čvorovi ga prihvaćaju i počinju raditi na sljedećem bloku. Ako se dva čvora slučajno poklope u stvaranju novog bloka otprilike u isto vrijeme, čvorovi se možda neko vrijeme razdvajaju oko toga koji koristiti, ali "pravilo najdužeg lanca" brzo će ponovno uspostaviti suglasnost.

Nema jamstva da će svi rudari istovremeno obrađivati isti skup transakcija jer rudari proizvoljno odabiru transakcije za uključivanje u svoje blokove, ali će vjerojatno postojati znatno preklapanje u skupovima transakcija koje rudari obrađuju. Pri dodavanju novog bloka u blok-lanac, neki dio transakcija koje su bile u procesu obrade možda nisu uključene u novi blok – te transakcije se čuvaju u bazenu neprocesuiranih transakcija kako bi rudari odlučili hoće li ih uključiti u sljedeći blok.

U slučaju da pojedini rudar samostalno rješava računalnu zagonetku, on zapravo provodi solo rudarenje te se naziva solo rudarom (*engl. Solo miner*). U toj situaciji, ukoliko ispravno riješi zagonetku, dobije nagradu i naknadu, koja ide isključivo njemu. U situaciji kada više rudara zajedničkim snagama računala rješava zagonetku, tada se radi o rudarima u rudarskom bazenu, što je opisano u sljedećem dijelu priručnika.

4.9.2 Rudarenje u rudarskim bazenima (*eng. Mining pools*)

Rudarenje funkcionira na način da jedna jedinica računalne snage radi na rješavanju matematičke zagonetke s ciljem osvajanja nagrade. Mogućnost osvajanja nagrade (rješavanjem zagonetke) s jednom jedinicom je niska, a s ciljem postizanja stabilnije nagrade, rudari ponekad osnivaju bazene u kojima rudari surađuju u rješavanju problema i dijele nagradu.

Prvo i najvažnije, bazeni se razlikuju po hash brzini koju doprinose ukupnoj Bitcoin mreži. Što je njihov udio u hashu veći, to je veća vjerojatnost da će određeni bazen riješiti matematički problem i tako osvojiti nagradu Bitcoina (otprilike svakih 10 minuta).

Na prvi pogled, može se reći da ima smisla pridružiti se najvećem rudarskom bazenu jer to obećava najveći profit. Međutim, iz različitih razloga često se odvrća od te ideje. Prije svega, veliki rudarski bazen ukazuje na visok broj korisnika, što znači da će pojedinačni profiti morati biti podijeljeni s mnogima. Uvjeti također igraju važnu ulogu. Različite platforme naplaćuju različite naknade, uključujući vrste naknada za obračun dobivene kroz su-rudarenje, kao i druge naknade, poput troškova za održavanje poslužitelja ili povlačenja

Bitcoina. Ove naknade variraju u rasponu od 0 posto do 13 posto.

Naknade ovise o načinu nagrađivanja ili isplate udjela, što je opet složeno pitanje koje se rješava različitim distribucijskim ključevima. Osnovni princip bazena je jednostavan: korisnici doprinose računalnim kapacitetom zajednici (bazenu), i kada se pronađu novi Bitcoin, korisnici dobivaju svoj udio.

Vremenski intervali u kojima određeni bazen pronalazi nove bitcoine variraju - ponekad se otkriju brže, ponekad sporije. Kako bi stekli prednost, neki korisnici mogu skakati između različitih bazena, uvijek u nadi da će sudjelovati u kratkoj rundi. To bi učinilo njihove doprinose rudarenju vrijednijima.

Centralni server koordinira rudarske bazene te dodjeljuje posao i nagrade svim sudionicima bazena kada jedan od rudara stvori novi blok. Glavni izazov ovdje je pravedno izračunati postotak nagrade koji će biti dodijeljen svakom članu bazena.

U pravednom bazenu oni članovi koji su doprinijeli više računalne snage trebali bi osvojiti veću nagradu, tako da se doprinos računalne snage mjeri i prati od strane centralnog servera. Praćenje se provodi bilježenjem broja rješenja koje rudari pronađu za jednosavniju verziju problema dokaza o radu. Što više računalne snage rudar doprinese, češće će pronalaziti rješenja i zarađivati udjele. Kada rudar u bazenu riješi stvarni problem, server dijeli nagradu svim rudarima proporcionalno broju udjela koje su zaradili od posljednje isplate nagrade.

Najčešće se u svrhu pravedne raspodjele u rudarskom bazenu koriste tri metode:

1. Pay-per-Share (PPS) - Rudar unosi udjele u bazen, koji su zapravo hashevi koji bi pronašli blok pri niskom stupnju težine, što znači da se računaju samo ispravni izračuni. Ovisno o računalnoj snazi, korisnici postupno dobivaju udjele. PPS metodom korisnik dobiva fiksnu isplatu za svaki udio, neovisno o vremenu runde, bez obzira na to hoće li ranije izaći i prijeći u drugi bazen.
2. Pay-per-last-N-Shares (PPLNS) - Ovaj sustav više-manje odgovara proporcionalnoj raspodjeli udjela – svaki sudionik dobiva udjele prema svom doprinosu. Kako bi skakanje između bazena učinili neprivlačnim, sudionici se ne isplaćuju iz trenutne runde, već se isplate na temelju posljednjih udjela koje su doprinijeli.
3. Double Geometric Method (DGM) - Ova metoda kombinira PPLNS s tzv. geometrijskom metodom. Bit je izjednačiti različite duljine rundi tijekom kojih se novi bitcoini pronalaze u bazenu. Operater uvodi dodatnu varijabilnu naknadu koja je visoka u kratkim rundama, a vraća se u dugim rundama. Cilj je održati konstantnu visinu isplata po udjelu tijekom vremena.

Važno je napomenuti da se sva tri postupka smatraju pravednima jer se uglavnom može isključiti mogućnost da pojedini korisnici steknu prednost.

4.9.3 Rudarska oprema

U početku se rudarenje provodilo koristeći osobno računalo, ali danas su CPU-ovi (*eng. Central processing unit*) zamijenjeni učinkovitijom rudarskom opremom. Grafički procesorski uređaji (*eng. Graphics processing unit*) dizajnirani su za obavljanje velikog broja jednostavnih izračuna paralelno, i znatno su brži u odnosu na CPU.

Godine 2013. dolazi do velike promjene rudarenja, kada su osmišljeni i razvijeni integrirani krugovi specifični za aplikaciju (*eng. ASIC – Application-specific integrated circuit*), koji su znatno brži od GPU-ova. ASIC je namjensko izrađen hardver s ciljem optimiziranja rudarenja, a sama oprema sadrži integrirane krugove koji su posebno optimizirani za SHA-256 algoritam, koji podupire dokaz radom (PoW) i putem kojeg se rješavaju složene matematičke zagonetke.

4.10 Napadi na Bitcoin, blockchain mreže i novčanike

Iako se tehnologija ulančanih blokova zbog svoje decentralizirane prirode, nepromjenjivosti, uspostavljenog povjerenja i verificiranih tvrdnji smatra izuzetno sigurnom, nije otporna na napade, posebno zbog napada nove ere koji su vrlo sofisticirani i mogu prouzrokovati nepopravljive štete.

Napadi nove ere na sigurnost tehnologije ulančanih blokova dijele se u četiri kategorije:

1. Napadi na P2P mrežu
2. Napadi na konsenzus i ledger
3. Napadi na pametne ugovore
4. Napadi na novčanike

Najpoznatije vrste napada su Sybil napad, napad od 51%, napad dvostrukog trošenja i nedostatak konsenzusa, koji će, uz ostale napade, u nastavku biti ukratko opisani.

4.10.1 Sybil napad (*eng. Sybil attack*)

Sybil napad je napad koji je usmjeren na cijelu mrežu te spada u kategoriju napada na P2P mrežu (*eng. Peer-to-Peer Network-based Attacks*). U ovom napadu, napadač za cilj ima preplaviti mrežu velikim brojem čvorova, odnosno stvara veliki broj lažnih identiteta na mreži s ciljem stjecanja što većeg utjecaja. Jedna osoba ili entitet dakle stvara više računa kojima napada cijelu mrežu. S tim velikim brojem identiteta napadač stječe povjerenje i kredibilitet unutar mreže što posljedično može dovesti do centralizacije mreže te se može koristiti za manipuliranje ishodom transakcija. Stjecanjem kontrole nad većinom mreže moguće je izvoditi druge napade, stoga Sybil napadi predstavljaju prijetnju sigurnosti i integritetu mreža.

S ciljem sprječavanja Sybil napada, velik broj mreža koristi mehanizme konsenzusa poput PoW ili PoS (*eng. Proof-of-Stake*), kojim se od korisnika zahtijeva određena količina računalne snage ili kriptovalute za sudjelovanje u mreži, čime je otežano stvaranje velikog broja lažnih identiteta od strane napadača.

Zanimljiva činjenica: Naziv Sybil napad, zbog karakterističnog stvaranja velikog broja lažnih identiteta, potječe od žene imenom Sybil Dorsett, liječene od disocijativnog poremećaja identiteta (poremećaj višestruke osobnosti, *eng. Multiple Personality Disorder*).

4.10.2 Napad većine ili 51% napad (*eng. 51% attack, Majority attack*)

Napad koji je moguć ako rudar ili grupa rudara (čvorova) u lancu blokova kontrolira 51% ili više ukupne rudarske snage mreže. Mogućnost ovog napada veća je u malim mrežama. U slučaju da se dogodi da grupa ima većinsku kontrolu, postoji mogućnost za manipulacijom blokova, što dovodi do izvođenja niza zlonamjernih aktivnosti, uključujući poništavanje ili izmjenu postojećih transakcija, sprječavanje dodavanja novih transakcija, kao i mogućnosti dvostrukog trošenja kriptovaluta. Ključ u sprječavanju ovakvog napada je osiguravanje

dovoljno decentralizirane mreže rudara (čvorova), kako ne bi moglo doći do stvaranja grupe koja bi preuzela kontrolu nad više od 51% ukupne rudarske snage mreže. Takav napad može dovesti do smanjenja sigurnosti i integriteta mreže, čime dolazi do gubitka povjerenja u mrežu, ali i potencijalnog smajnenja vrijednosti kriptovalute.

4.10.3 Napad dvostrukog trošenja (*eng. Double spending attack*)

Vrsta napada u lancu blokova u kojoj zlonamjerna treća strana pokušava potrošiti već potrošenu kriptovalutu, u više transakcija. S ciljem sprječavanja ovakvog napada, većina tehnologija ulančanih blokova služi se oblikom mehanizma konsenzusa, što osigurava potvrdu važeće transakcije, koja nije prethodno potrošena. Bitcoin u tu svrhu koristi PoW – dokaz o radu, koji grupira transakcije u blokove te ih dodaje procesom rudarenja u lanac blokova.

4.10.4 Nedostatak konsenzusa (*fork*)

Vrsta napada u kojem skupina napadača stvara nevažeće transakcije ili blokove u mreži te sprječava mrežu u postizanju konsenzusa o ispravnom stanju tehnologije ulančanih blokova. Ovakav napad može dovesti do podjele (*eng. Fork*) tehnologije ulančanih blokova, što za posljedicu ima značajne poremećaje u mreži i gubitak povjerenja u sigurnost tehnologije. S ciljem sprječavanja ovog napada, mreža ima snažne mehanizme konsenzusa.

4.10.5 Napad sebičnog rudarenja (*eng. Selfish mining attack*)

Napad koji se sastoji od mogućnosti da „sebični“ rudar pokuša nastaviti graditi blokove potajno na postojećem lancu, a u trenutku kada stvori prednost od dva ili više blokova u odnosu na trenutni lanac u mreži, može objaviti svoj privatni razvodnik koji će biti prihvaćen kao istinit, jer će biti najduži lanac. Također može izvršavati transakcije u javnoj mreži neposredno prije objavljivanja svog duljeg lanca, s ciljem poništavanja transakcije koju je upravo obavio. Ovo efikasno pruža kratkotrajnu priliku napadaču da izvrši dvostruko trošenje temeljeno na sposobnosti izgradnje tajnog lanca, stvaranjem dovoljno prednosti u blokovima (Finney napad).

4.10.6 Napad vremenskog presretanja (*eng. Timejack attack*)

Prije objašnjenja napada, važno je znati kako čvorovi u određenim blockchain mrežama ovise o internom vremenskom sustavu koji proizlazi iz vremena koje prijavljuju njegovi peer čvorovi. U slučaju izvršenja ovog napada na ciljani čvor, tada taj isti čvor neće prihvatiti blokove iz stvarne mreže, jer vremenske oznake blokova neće biti u skladu s vremenskom oznakom tog čvora. Opisano pruža priliku napadaču za dvostruko trošenje ili obavljanje transakcija s ciljanim čvorom, jer se te transakcije ne mogu predati stvarnoj blockchain mreži.

4.10.7 Finney napad (*eng. Finney attack*)

Napad koji se može dogoditi ukoliko osoba prihvati nepotvrđenu transakciju na mreži. Ukratko objašnjeno, rudar je u mogućnosti generirati blok u koji će uključiti transakciju kriptovalute s adrese A na adresu B, pri čemu obje navedene adrese pripadaju jednoj osobi. Nakon ovoga, rudar – napadač će izvršiti još jednu uplatu istim valutama, šaljući je s adrese A na adresu C, koja pripada drugom korisniku. Ukoliko korisnik C prihvati transakciju bez potvrde s mreže, napadač može objaviti blok koji sadržava njegovu početnu transakciju. Navedeno poništava transakciju koja je izvršena trgovcu, a omogućuje napadaču dvostruko trošenje sredstava.

4.10.8 Napad utrke (*engl. Race attack*)

Ova vrsta napada predstavlja manju varijaciju Finney napada, a razlika je u tome što napadač ne mora unaprijed izrudariti blok s transakcijom koju namjerava dvostruko potrošiti. Tijekom ovog napada, napadač predaje nepotvrđenu transakciju trgovcu, odnosno žrtvi, te istovremeno izvršava drugu transakciju koju šalje u mrežu. Za napadača je lakše izvesti ovu vrstu napada ako je direktno povezan s čvorom trgovca.

4.10.9 Napadi na Pametne ugovore (*engl Smart Contract-based Attacks*)

Pametni ugovori (*eng. Smart contracts*), opisani u drugom poglavlju, su u potpunosti automatizirani ugovori koji izvršavaju dogovorenu transakciju između sudionika, sa stvarnim unosima, a bez potrebe za posrednikom. Kada je pametni ugovor jednom pokrenut, ne može biti zaustavljen, a transakcija kada je jednom završena i zapisana u lanac, postaje nepromjenjivom. Ovo daje jamstvo sudionicima o povratu temeljenom na njihovoj izvedbi, kako je dogovoreno pri ulasku u ugovor. Ukoliko pametni ugovor ima greške, može doći do ozbiljnih posljedica jer su milijuni dolara u pitanju i ne postoji mogućnost promijene ugovora. U nastavku će biti prikazan primjer napada na pametni ugovor – DAO napad.

Prije objašnjavanja primjera, nužno je naglasiti kako se ovdje radi o pametnom ugovoru na Ethereum mreži. Primjer će biti objašnjen jer je BTC nedavno implementirao pametne ugovore, kako bi se uvidjele potencijalne opasnosti.

DAO (*eng. Decentralized Autonomous Organizations*) je ustvari decentralizirana autonomna organizacija koja predstavlja virtualni entitet, važnu značajku Etheruma. Napad na DAO odvio se kada je tvrtka „Slock“ pokrenula skupno financiranje (*eng. crowdfunding*) za projekt nazvan „The DAO“. Skupnim financiranjem prikupljeno je 12,7 milijuna Ethera, u tom periodu vrijednih 150 milijuna dolara. Napadač je uspješno identificirao ranjivost u kodu gdje se rekurzivna funkcija povlačenja mogla izvršiti bez provjere rješavanja trenutne transakcije – napadač je započeo napad na način da je doprinio malu količinu, a tražio je povlačenje rekurzivnom funkcijom. Navedeno je napadaču omogućilo izvlačenje gotovo 70 milijuna dolara prikupljenih skupnim financiranjem. „Ethereum Foundation“ je potom prijetila napadaču da zaustavi napad i zamrzne račun, na što je napadač odgovorio kako djeluje prema dogovorenom ugovoru i da će intervencija putem mekanog ili tvrdog *forka* biti kršenje ugovora, što za posljedicu ima odlazak cijelog slučaja na sud. Iako je napadač s vremenom obustavio opisani napad, ovaj događaj je izazvao veliku zabrinutost oko autonomije pametnih ugovora i mnoge kontroverze.



Peti dio



5. Bitcoin i energija

Kada je 4. prosinca 1921., New York Tribune objavio članak u kojem je opisao Fordovu viziju zamjene zlata valutom koja se zasniva na energiji, za koju je vjerovao da bi mogla prekinuti monopol bankarskih elita nad globalnim bogatstvom i stati na kraj ratovima, nitko nije mogao predvidjeti bitcoin. Ford je to kanio učiniti izgradnjom "najveće elektrane na svijetu" i stvaranjem novog valutnog sustava temeljenog na "jedinicama snage".

Ford, koji je osnovao Ford Motor Company 1903., rekao je tada: "U sustavu energetske valute standard bi bio određena količina energije uložena tijekom jednog sata koja bi bila jednaka jednom dolaru. To je jednostavno slučaj razmišljanja i kalkuliranja u uvjetima drugačijim od onih koje nam je postavila međunarodna bankarska grupa na koju smo se toliko navikli da mislimo da ne postoji drugi poželjan standard."

Pojedinosti oko reprezentacije vrijednosti valute zasnivana na energiji "bit će razrađene kada Kongres bude želio čuti o tome", rekao je tada Ford.

Iako Ford nikada nije uspio realizirati svoju viziju valute, bitcoin je naizgled opravdao tu ideju stoljeće kasnije. Od 2009. više od 18,8 milijuna BTC-a stvoreno je kroz energetski intenzivan proces rudarenja koji zahtijeva računala za rješavanje sve složenijih matematičkih problema. Ovo rudarenje s dokazom rada izazvalo je teške kritike zbog svog navodnog utjecaja na okoliš - kratkovidna tvrdnja koja zanemaruje sposobnost bitcoin kriptovalute da ubrza prelazak na obnovljivu energiju čineći je financijski prihvatljivijom.

Da bi shvatili odakle Fordu ideja i valuti koja počiva na energiji, potrebno je vratiti se u eru drevnih sustava razmjene u kojima je nepostojanje standardizirane fiat valute dovelo do razmjene dobara i usluga kroz uzajamno podudaranje u datom trenutku. Ovaj sustav, iako funkcionalan, bio je prožet neučinkovitošću. Na primjer, ako bi lovac želio zamijeniti svoje meso za sol kako bi sačuvao svoj ulov, zauzvrat bi prihvatio samo sol, a ne primjerice vunu. Posljedično, svatko tko želi doći do mesa od lovca trebao bi posjedovati točno ono što lovac želi, u ovom slučaju sol. Ovo oslanjanje na uzajamnu podudarnost želja stvorilo je iskrivljeno razumijevanje principa ponude i potražnje.

Izazov utvrđivanja pravedne razmjene za jedinstvene, nezamjenjive stavke postaje očit u

takvim scenarijima. Kako možemo osigurati da obje uključene strane dobiju odgovarajuću naknadu za vrijeme, trud i energiju koje su uložile u proizvodnju robe ili usluga koje prodaju?

Koncept "životne energije" obuhvaća ograničeni vremenski raspon, trud i kreativnu energiju koju pojedinci posvećuju svom poslu, što rezultira opipljivim i produktivnim rezultatima.

Međutim, u sustavu razmjene, pojam životne energije nije prikladno uračunat. Umjesto toga, vanjski čimbenici snažno utječu na vrijednost proizvoda ili usluge, često zanemarujući životnu energiju uloženu u njihovu proizvodnju. U idealnom slučaju, potreban nam je sustav koji omogućuje akumulaciju i skladištenje ovog utroška energije, koji se može nazvati "viškom energije", zajedno s povezanom vrijednošću.

Dobrobiti proizašle iz ovog principa ulaganja životne energije daleko nadilaze pojedinca koji je uložio takav napor. Figurativna snaga svake ekonomije leži u pojmu "viška energije". Ako je protok energije (novca?) otežan ili opstruiran, rezultat će biti slabije i stagnirajuće gospodarstvo. Međutim, ako se resursi učinkovito iskoriste i tok vrijednosti ostane fluidan, gospodarstvo ima potencijal rasta, poticanja inovacija i provođenja mjera koje će koristiti društvu u cjelini. Akumulacija energije u prvim društvima kroz prikupljeno žito, drvo za ogrijev ili neku drugu vrstu skladišta robe dovele su do razvoja civilizacije.

Bez implementacije preciznih mehanizama, a što provodi politika, prikupljanje i očuvanje viška energije ili vrijednosti gotovo je nedostižno. Stoga postaje ključno mjeriti ovu izlaznu energiju na najučinkovitiji i najjednostavniji mogući način, čime se osigurava da pojedinci dobiju pravičnu naknadu za svoj trud i imaju priliku iskoristiti energiju koju su potrošili. U tom smislu, značajna prekretnica u napredovanju civilizacije bio je prijelaz s razmjene na korištenje robnog novca, što je na kraju evoluiralo u korištenje prijenosnih, zamjenjivih i standardiziranih metalnih kovanica.

Rimsko je Carstvo uspjelo uspostaviti ekonomsku učinkovitost minimizirajući trenje prijenosa vrijednosti korištenjem valute denara. Ova je valuta napravljena od ograničene količine plemenitih metala, što joj je omogućilo da služi kao pohrana vrijednosti. Denar je također bio prenosiv, što je olakšavalo transport i trgovinu diljem carstva, a što je rezultiralo ekonomskim cirkulacijskim sustavom koji je bio preplavljen energijom, budući da je trenje unutar razmjene dobara i usluga svedeno na minimum. To je omogućilo formiranje novih specijaliziranih tržišta rada, što je povećalo produktivnost i inovativnost.

Denar je bio robna valuta koja je olakšavala gospodarsku ekspanziju, jer je bio standardiziran, prenosiv i ograničen. Učinkovito je iskoristio rimsku energiju u produktivnost i gospodarski rast. Međutim, sve se to promijenilo kada je svaki rimski car želio potrošiti više energije nego što je valuta dopuštala. Počeli su erodirati zalihi vrijednosti denarija, što je uzrokovalo njegovu slabu sposobnost da točno prikazuje izlaze životne energije ljudi. Udio srebra u svakom denaru postajao je sve manji, što je nagrizzalo sposobnost valute da održi vrijednost i kupovnu moć. Danas shvaćamo da je to bila inflacija kod koje sa svakim ciklusom pada vrijednosti valute, a ljudi gube povjerenje u obećanje da je njihova životna energija pravilno izmjerena.

Za točno mjerenje životne energije, bitno je imati zamjenjivi i standardizirani mjerac koji omogućuje izračun vrijednosti nezamjenjivih dobara i usluga. Osim toga, ovaj bi mjerac trebao imati sposobnost pohranjivanja vrijednosti i biti prenosiv. Ovi temeljni elementi daju pojedincima alat za učinkovito pretvaranje njihovog ograničenog vremena i energije u produktivne i dobro kompenzirane druge oblike pohrane vrijednosti. Međutim,

bitno je da se taj integritet ne oslanja na medijatore i jamstvenike koji imaju mogućnost promjene mjerila.

Ideja Satoshija Nakamota o bitcoinu predstavlja revolucionarni koncept uniformne reprezentacije vrijednosti zasnovana na jedinici za energiju Joule - J. Nakamoto je predložio sustav koji eliminira potrebu za povjerenjem u centralizirane entitete koji kontroliraju monetarne sustave i umjesto toga predložio sustav u kojem se povjerenje uspostavlja kroz kriptografski dokaz do kojeg se dolazi radom. Bitcoin kao elektronički sustav plaćanja omogućuje pojedincima da kapitaliziraju svoju utrošenu energiju kroz reprezentaciju rada.

Pitanje koje se postavlja je kako osigurati sigurnost ove nove komponente povjerenja. U prošlosti su intelektualci predlagali da se novac podupre jedinicama energije. Na primjer, John Maynard Keynes je u svojim predavanjima od 1912. do 1913. predstavio ideju mjerenja novca u jedinicama električne energije. Ovaj pristup pruža okvir za uspostavljanje sigurnijeg i pouzdanijeg monetarnog sustava.

U konačnici, razmjena sredstava između poslodavaca i zaposlenika predstavlja razmjenu energije. Međutim, niti poslodavci niti zaposlenici nemaju kontrolu nad kretanjem te kompenzacijske energije, već je to kretanje omogućeno kroz neku nacionalnu valutu, kojom u potpunosti upravljaju središnje banke i politika.

Stoga su središnje banke te koje posjeduju isključivu ovlast da tijekom vremena mijenjaju tijek te energije, što podsjeća na praksu starih rimskih careva.

Raspored ponude i izdavanja valute ima najznačajniji utjecaj na njezinu vrijednost kao zalihe bogatstva. I središnje banke i rimski carevi pokazali su tendenciju da drastično mijenjaju raspoloživu ponudu, što je rezultiralo negativnim utjecajem na to osnovno svojstvo bilo čega što predstavlja vrijednost.

Posljedično, to negativno utječe na sposobnost svakog pojedinaca i smanjuje mu mogućnost iskorištavanja energije koju je uložio u koristan rad.

No, bitcoin možda nudi odgovore na suvremene izazove kao sustav prijenosa vrijednosti nastao na mjerljivoj energiji i zaštićen energijom.

Bitcoin je digitalna valuta koja je digitalno prenosiva, što je čini savršenom za naše digitalno doba. Njegova oskudica definirana je na energetske agnostičan način, koji se razlikuje od Fordove valute koja se ipak temelji na električnoj energiji. Fordova valuta bila je centralizirana i ranjiva na napade, dok bitcoin koristi energiju iz bilo kojeg dostupnog izvora, što ga čini decentraliziranim i otpornim.

Decentralizirana priroda računalne snage stvara robustan i siguran sustav koji je otporan na napade. Bitcoin mreža osigurava novu komponentu povjerenja, koja je kriptografski dokaz, kroz energiju koju koristi. Michael Saylor vjeruje da je bitcoin rješenje problema skladištenja energije, a time i vrijednosti, u vremenu i prostoru.

Unatoč brojnim prednostima, ostaje pitanje trajnosti bitcoina u odnosu na vanjske čimbenike i postoje li legitimne prijetnje njegovoj sigurnosti. Međutim, činjenica da je bitcoin energetske agnostičan i decentraliziran čini ga sigurnijom i otpornijom valutom od tradicionalnih centraliziranih valuta.

Nepromjenjiva priroda blockchain zapisa omogućuje razinu verifikacije koja će s napretkom umjetne inteligencije postati sve potrebija kako bi se jamčila vjerodostojnost podataka. Međutim, ono što je još značajnije je kako bitcoin entuzijasti doživljavaju bitcoin kao nešto više od špekulativne imovine, već kao način života. Ova nepokolebljiva podrška sve većeg dijela društva pridonijet će otpornosti bitcoina na nadolazeće inovacije, političke promjene ili bilo koje druge potencijalne prijetnje u budućnosti.

Unatoč tome, još uvijek postoji nedostatak odgovarajućeg okvira u vezi s potrošnjom energije bitcoina.

Prema Sveučilištu Cambridge, Judge Business School, Centre for Alternative Finance - CCAF, potrošnja električne energije u sustavima rudarenja bitcoina u trenutku pisanja ovog teksta iznosi 164 TWh godišnje, što je ekvivalentno potrošnji energije u zemljama poput Argentine, Ujedinjenih Arapskih Emirata ili Švedske, a šest puta više od Novog Zelanda. Utjecaj rudarenja bitcoina na okoliš tema je rasprava među zakonodavcima u SAD-u i Europi, a rudarenjem PoW - dokaz radom, potrošnjom energije, metodom koju koristi mreža bitcoin, zabranjeno je u državi New York i skoro je bila zabranjena u Europskoj uniji.

Ipak, države poput Texasa podržavaju rudarenje bitcoina zbog činjenice da rudari mogu lako prilagoditi svoju potrošnju energije u roku od nekoliko minuta što omogućuje iskorištavanje bilo kojih viškova neupravljive proizvodnje iz obnovljivih izvora električne energije, a to može pomoći u stabilizaciji mreže i smanjenju gubitaka u prijenosu. Međutim, postoji zabrinutost da ova prednost otežava drugim industrijama da održe korak, što u konačnici usporava energetska tranziciju potrebnu u drugim sektorima kao što su velika proizvodnja baterija i elektrifikacija prometa. Činjenica jest da se rudari bore za iste jedinice energije kao i ostale industrije, no isto tako istina je da jedni imaju koristi od drugih i obrnuto.

Obnovljivi izvori energije suočavaju se s velikim izazovom koji se često zanemaruje: upravljivost. Zbog fluktuirajuće prirode solarne energije i energije vjetra, opskrba električnom energijom nije stalna. Međutim, mreža je dizajnirana za stabilnu opskrbu koja se može prilagoditi kako bi zadovoljila potrošnju. Kao rezultat toga, značajna količina električne energije proizvedene iz obnovljivih izvora gubi se kada je potrošnja niska, a proizvođači su prisiljeni isključiti se iz mreže dok se potrošnja ne poveća.

Ova nemogućnost upravljanja fluktuirajućom prirodom primarnog energenta, kao i nemogućnost upravljanja potrošnjom sprječava mnoge lokalitete obnovljive energije da svojim viškom kapaciteta doprinesu mreži, što rezultira gubitkom prihoda, privremenim gašenjima, pa čak i velikim gubicima. Dodatno, bitcoin rudari imaju prednost jer se mogu locirati u udaljenim područjima gdje se obično nalaze projekti obnovljivih izvora energije, što im omogućuje pristup izvoru energije prije nego što se ona prenese na velike udaljenosti.

Kao što je već rečeno, Teksas je dobra ilustracija sinergijskih napora između operatera mreže, ERCOT, i rudara kriptovalute bitcoin u olakšavanju besprijekorne integracije obnovljivih izvora energije u električnu mrežu. U zamjenu za njihovu predanost uključivanju u programe upravljanja potrošnjom, bitcoin rudarima se nudi povoljna cijena, čime se pomaže u stabilizaciji varijabilne proizvodnje energije povezane sa solarnim izvorima i vjetroelektranama. Nadalje, ERCOT aktivno promiče preseljenje bitcoin rudara u zapadni Teksas, gdje postoji višak kapaciteta zahvaljujući inicijativama za solarnu energiju i korištenje vjetra. Ovaj dodatni prihod koji se generira za proizvođače energije ne samo da doprinosi smanjenju troškova, već također podržava stabilnost mreže, a u konačnici olakšava priključenje projekata obnovljivih izvora energije na mrežu i nižu cijenu energije za krajnje kupce.

Prednosti suradnje između rudarenja bitcoina i obnovljivih izvora energije nisu ograničene samo na Teksas. Korištenjem viška energije, bitcoin rudari igraju ključnu ulogu u stabilizaciji električne mreže, čime se olakšava prelazak na ekološki prihvatljiviji i održiviji

energetski sustav. U medijima se tvrdi kako prisutnost bitcoin rudara, koji učinkovito iskorištavaju višak kapaciteta iz obnovljivih izvora energije, stvara izazovno okruženje za druge industrije i promiče natjecanje, no i čini se da koči napredak energetske tranzicije u različitim sektorima i klasičnim inicijativama kao što su veliki baterijski sustavi i elektrifikacija prijevoza. Međutim, razvoj projekata baterija nije ugrožen, dapače, može biti poticajno ubrzan integracijom bitcoin rudarenja u zajedničko alternativno rješenje za učinkovito upravljanje promjenjivom proizvodnjom solarnih elektrana i vjetroelektrana. Dodatni prihod koji generiraju bitcoin rudari može podržati mrežne operatere u financiranju potrebnih nadogradnji za učinkovitiju prilagodbu projektima obnovljivih izvora energije.

Važno je i uzeti u obzir pozitivan utjecaj koji rudarenje bitcoina može imati na okoliš, posebno u smislu integracije obnovljivih izvora energije u elektroenergetsku mrežu. Partnerstvom s proizvođačima obnovljivih izvora energije rudarenje bitcoina može odigrati ključnu ulogu u prijelazu prema čišćoj i održivijoj budućnosti. Jedna od ključnih prednosti rudarenja bitcoina je njegova sposobnost da djeluje kao odgovor na strani potrošnje na promjenjivu i nekontroliranu prirodu opskrbe obnovljivim izvorima energije. Dodatno, bitcoin rudari mogu se locirati u udaljenim područjima blizu projekata obnovljivih izvora energije, podržavajući lokalne zajednice i učinkovitije iskorištavajući inače izgubljen energiju. U područjima s prekomjernom opskrbom iz obnovljivih izvora energije, rudarenje bitcoina može pretvoriti izgubljen energiju u profit, dok u područjima s ograničenim kapacitetom mreže može učiniti održivima projekte obnovljivih izvora energije. Nadalje, korištenje obnovljivih izvora energije može biti ekonomski korisno za rudare i privući institucionalne ulagače, smanjujući njihov trošak kapitala. Općenito, rudarenje bitcoina može proizvođačima energije i mrežnim operaterima pružiti dodatni izvor prihoda za ulaganje u prijenosne kapacitete, fleksibilna opterećenja i projekte skladištenja energije. Rudarenje bitcoina predstavlja alternativno tržište za stvaranje prihoda u energetskom sektoru.

Budući da rudarenje kriptovaluta nije energetski regulirana djelatnost i da su neki sustavi nadzora i praćenja iz kojih izvora se rudari kriptovaluta bitcoin tek u povojima, analizu udjela pojedinih izvora energije u ukupnom rudarenju je moguće obaviti samo pouzdajući se u podatke koje pruža sveučilište Cambridge.

Cambridge Bitcoin Electricity Consumption Index (CBECI) uspostavljen je u srpnju 2019. kako bi se zadovoljila sve veća potražnja za pouzdanim podacima o potrošnji električne energije u Bitcoin eko sustavu. Kao odgovor na rastući javni interes za ovu temu, naponi CCAF-a prirodno su evoluirali kako bi se postupno proširio opseg njihova Indeksa, s konačnim ciljem ponuditi sveobuhvatnije razumijevanje utjecaja Bitcoin mreže na okoliš. Kako bi se premostio jaz u znanju, alat za indeksiranje poboljšao je u svibnju 2020. integracijom nove značajke pod nazivom Mining Map. Navedeni alat vizualno prikazuje geografsku distribuciju računalne snage (*hashrate*) tijekom određenog vremenskog razdoblja. Formiranjem longitudinalnog skupa podataka dobivenog kroz ekskluzivno partnerstvo s istaknutim zadrugama (*pool*) za rudarenje bitcoina, ova karta rudarenja pruža dragocjene uvide u fizičke lokacije rudarskih operacija. Najnovije ažuriranje, pokrenuto u rujnu 2022., služi kao ključna komponenta za procjenu utjecaja Bitcoin mreže na okoliš i kombinira nalaze iz prethodnih studija s regionalnim podacima o izvorima električne energije koji se koriste na određenim područjima. Takva baza je od vitalnog značaja jer uzima u obzir varijacije u specifičnim profilima mješavine električne energije u regijama u kojima se odvija rudarenje bitcoina.

Prema posljednjim dostupnim podacima, onima za siječanj 2022. godine, ugljen služi kao primarni energent s udjelom od 36,6%, dok je hidroenergija najveći obnovljivi izvor energije s udjelom od 14,9%. Rezultati pokazuju da fosilna goriva čine gotovo 62,4% ukupne mješavine električne energije prilikom rudarenja bitcoina, dok obnovljivi izvori energije čine 37,6%, uključujući i 11,3% koliko čini nuklearna energija. Ovi nalazi su u suprotnosti s procjenama Bitcoin Mining Council-a, vodeće zajednice ove industrije, koja sugerira da obnovljivi izvori energije čine 59,5% električne energije u Bitcoin mreži.

Sektor rudarenja bitcoina u stalnom je stanju promjena i važno ih je sve pratiti kako bi se mogle napraviti što točnije procjene u budućnosti. Podaci će se zasigurno nastaviti usavršavati tijekom vremena i po pitanju kvalitete i po pitanju kvantitete, a izgledan je i postupni prelazak metodologije iz apstraktnog u stvarni, mjerljivi, svijet. Danas već postoje neki fascinantni razvojni putevi u svijetu rudarenja bitcoina, kao što je korištenje povrata otpadne topline za proizvodnju hrane ili korištenje otpadnih plinova u naftnim bušotinama koji bi se inače spalili na baklji kao energetna za rudarenje bitcoina. Porast cijene bitcoina sigurno će pomoći u smanjenju ograničenja obnovljivih izvora energije i potaknuti će infrastrukturne elektroenergetske projekte. Vrijeme će pokazati hoće li se te ideje pokazati uspješnim ili ne.



Bibliografija

- [1] Don Tapscott and Alex Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio, 2016.
- [2] Duca Domenico. Novac i školjke. *Numizmatičke Vijesti*, 54(65):15–20, 2012.
- [3] David Kovač. Prvi kovani novac. *Numizmatičke Vijesti*, 62(73):5–13, 2020.
- [4] LLC CNG. Classical numismatic group. <https://www.cngcoins.com/Default.aspx> [Pristupljeno: (03.11.2023.)].
- [5] Calgary Coin & Antique Gallery. Chinese cast coins. <https://www.calgarycoin.com/reference/china/china8.htm> [Pristupljeno: (03.11.2023.)].
- [6] Ognjen Arandjelovic and Marios Zachariou. Images of roman imperial denarii: A curated data set for the evaluation of computer vision algorithms applied to ancient numismatics, and an overview of challenges in the field. *Sci*, 2:91, 12 2020.
- [7] Jiaozi (currency). [https://hmn.wiki/nm/Jiaozi_\(currency\)](https://hmn.wiki/nm/Jiaozi_(currency)) [Pristupljeno: (05.11.2023.)].
- [8] M. Polo and H. Murray. *The Travels of Marco Polo*. Edinburgh cabinet library. Harper & brothers, 1845.
- [9] 1661 - first banknotes in europe. <https://www.riksbank.se/en-gb/about-the-riksbank/history/historical-timeline/1600-1699/first-banknotes-in-europe/> [Pristupljeno: (09.11.2023.)].
- [10] G. Davies and Julian Hodge Bank. *A History of Money: From Ancient Times to the Present Day*. CYMRU-Contemporary German Writers Series. University of Wales Press, 2002.

-
- [11] Credit cards: Helping people go into debt since 1946, 2019. <https://www.moneypeach.com/history-of-credit-cards-timeline/>[Pristupljeno: (09.11.2023)].
- [12] What is sha-256?, 2022. <https://www.moneypeach.com/history-of-credit-cards-timeline/>[Pristupljeno: (05.11.2023)].
- [13] Bitcoin block reward halving countdown. <https://www.bitcoinblockhalf.com/>[Pristupljeno: (11.11.2023)].

Regionalni centar kompetentnosti Elektrotehničke i prometne škole Osijek

Istarska 3, 31000 Osijek

031/289-829;031/289-830

ured@ss-elektrotehnicka-prometna-os.skole.hr

www.elpros.net

www.rck.elpros.net

Više informacija o EU fondovima na

www.strukturnifondovi.hr