**Freeman Family**

4. Srpnja 2019

# EPIC CASH

## EPIC PRIVATNI INTERNET NOVAC

### Peer-to-peer elektronički gotovinski sustav

### SKLADIŠTE VRIJEDNOSTI + SREDSTVO RAZMJENE + OBRAČUNSKA JEDINICA

1,7 milijardi odraslih nema pristup globalnom financijskom sustavu, dok još 1,3 milijarde ima nedovoljno dobar pristup. Epic Cash otključava ljudski potencijal spajajući pojedince na globalno tržište. Brz, gotovo besplatan za upotrebu i otvoren svima.

Version 7.1b Croitian

# Sadržaj

# I. Sažetak

*Epic Cash završna je točka na putu do prave P2P internetske gotovine, kamen temeljac privatnog financijskog sustava. Cilj Epic valute je postati najučinkovitiji oblik digitalnog novca koji štiti privatnost. Da bi ispunio taj cilj, on zadovoljava tri glavne funkcije novca:*

1. **Skladište vrijednosti** – može se spremiti, uzeti i razmijeniti kasnije te ima predvidljivu vrijednosti prilikom preuzimanja;
2. **Sredstvo razmjene** – sve što se prihvaća kao standard vrijednosti te je zamjenjivo za robu ili usluge;
3. **Obračunska jedinica** – jedinica pomoću koje se vrijednost stvari obračunava i uspoređuje.

| | $ USD | BTC | EPIC |
|---|---|---|---|
| **Skladište vrijednosti** | ✗ | ✓ | ✓ |
| **Sredstvo razmjene** | ✓ | ✗ | ✓ |
| **Obračunska jedinica** | ✓ | ✗ | ✓ |

2009. godine Bitcoin se pojavio kao prva digitalna valuta temeljena na blockchainu, s njim su se pojavile i tri karakteristike prema kojima se vrednuju ostale kripto valute:

- **Bez povjerenja** – nitko ne mora vjerovati bilo kojem centraliziranom entitetu ili drugoj ugovornoj strani kako bi mreža funkcionirala;
- **Nepromjenljivost** – transakcije se ne mogu poništiti;
  a. Trebalo bi biti gotovo nemoguće ili teško promijeniti povijest;
  b. Trebalo bi biti nemoguće da netko osim vlasnika privatnog ključa premješta sredstva povezana s tim privatnim ključem;
  c. Sve transakcije se bilježe na blockchain
- **Decentralizacija** – "Blockchain je politički decentraliziran (nitko ih ne kontrolira) i arhitektonski decentraliziran (nema infrastrukturne točke neuspjeha) ... [1].

Bitcoin je tehnološki pokrenuo nove staze pridržavajući se provjerenih osnova u strukturi svoje monetarne politike. Uspjeh Bitcoina snažno je povezan s ograničenom opskrbom u kombinaciji s nepovjerljivim, nepromjenjivim i decentraliziranim blockchainom. Epic Cash oponaša Bitcoinovu monetarnu politiku smanjenja inflacije i ograničene ponude kako bi se osiguralo da Epic valuta može poslužiti kao učinkovito skladište vrijednosti.

Unatoč uspjehu Bitcoina, otkriveni su određeni nedostaci od njegovog osnutka prije 10 godina. Drugi su projekti pokušali prevladati te nedostatke, a mi smo istražili najbolje za našu početnu točku. Odlučili smo se za upotrebu Grin baze podataka i odličnog rada nekoliko drugih projekata kako bi gradili na njihovim hvale vrijednim dostignućima i otklonili nedostatke prethodnika Epic Casha. Epic Cash posjeduje ključne kvalitete idealne valute:

- **Zamjenjivost** – Vrijednost određene jedinice Epica uvijek mora biti jednaka drugoj jedinici Epica, baš kao što je jedan Jen ili Yuan uvijek jednak i zamjenjiv s drugim Jenom ili Yuanom. Postizanje zamjenjivosti u velikoj mjeri ovisi o privatnosti.
- **Skalabilnost** – Epic Cash održava prostorno učinkovit blockchain na kojem se mogu lako uspostaviti novi čvorovi bez opreme koja zahtijeva mnogo resursa. Epic Cash blockchain sposoban je postići najmanje dvostruku propusnost Bitcoina.
- **Privatnost** – Epic Cash blockchain štiti anonimnost vlasnika i korisnika Epic-a zaštitom detalja o transakcijama od trećih strana, a osmišljen je na način da mu se ne može ući u trag te da bude nevidljiv za nadzor.
- **Brzina** – Transakcije Epic Casha su glatke, kontinuirane i izvršavaju se mnogo brže nego u prethodnim generacijama blockchain tehnologije. Dok Bitcoin zahtijeva šest 10-minutnih blokova za potpunu potvrdu transakcije, Epic transakcija je potvrđena čim se izrudari jedan 1-minutni blok.

[1] Buterin, Vitalik, ***The Meaning of Decentralization***, 7. Veljače 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

# II. Privatnost

Suvremeno korištenje novca može se shvatiti kao kolektivno prenošenje obračunskih jedinica između ljudi i institucija. Svojstva novca mogu se mapirati u bilo kojem trenutku odgovaranjem na sljedeća dva pitanja:

1. *Tko ga posjeduje i koliko?*
2. *Tko radi transakcije s kim, i sa koliko novca?*

Za tradicionalne fiat valute, ali i bitcoin, možemo odgovoriti na ta pitanja. Pritom se može otkriti mnogo o životima ljudi, poput obrazaca potrošnje, vlasništva i transakcijskih partnera. Dosta precizni zaključci mogu se iznijeti o interesima i namjerama pojedinca praćenjem prijenosa vrijednosti. Bez privatnosti, podaci o transakcijama mogu biti opasni podaci u rukama zlonamjernih trećih strana.

Upotreba kripto valute u proteklom desetljeću pokazuje kontinuitet "privatnosti" u različitim implementacijama blockchaina. Ako se uzme u obzir skala privatnosti koja se kreće od otvorenog i zloglasnog s jedne strane do potpune anonimnosti na drugom kraju skale. Kako se narušava privatnost, degradira se jedan bitan element kripto valute, izostanak potrebe za povjerenjem. Kao što je dokazano uspjehom servisa za analizu Bitcoin blockchaina, Bitcoin se nalazi više prema ozloglašenom transparentnom kraju spektra privatnosti. Korisnici moraju poduzimati sve više koraka kako bi se osigurali da nenamjerno ne koriste zaraženi Bitcoin. Epic Cash rješenje usmjerava iglu prema anonimnosti osiguravajući da se u temeljnoj razini sustava integrira i privatnost pojedinca i privatnost transakcija unutar sustava.

## Privatnost Identiteta

## Privatnost Transakcija

# Privatnost Identiteta

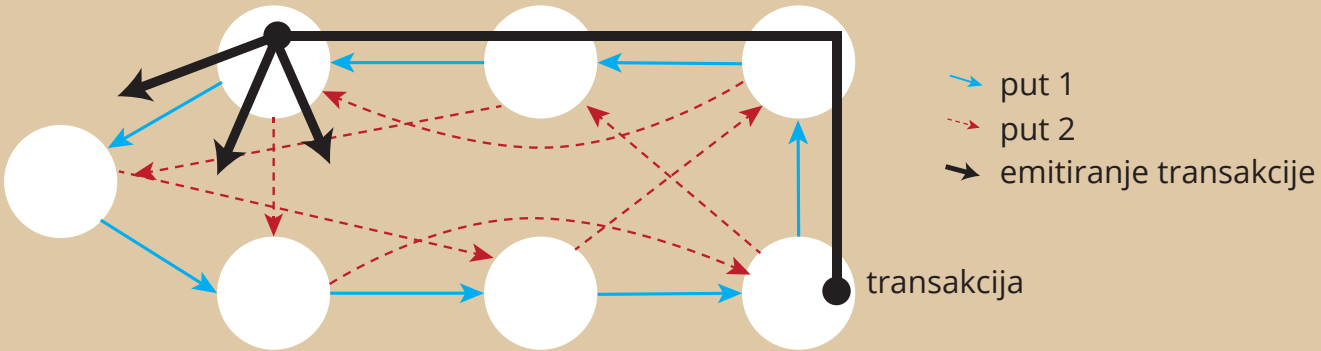
Većina kriptovaluta poput Bitcoina pohranjuje se u novčanike čija se adresa poziva na javni ključ izveden iz privatnog ključa novčanika. Ove se adrese mogu smatrati lokatorima nečijeg privatnog trezora u digitalnom svijetu. Epic Cash blockchain eliminira adrese u cijelosti i umjesto toga primjenjuje jedan veliki višestruki potpis iz kojeg se generiraju svi javni i privatni ključevi za jednokratnu upotrebu.

Budući da su adrese Bitcoin novčanika lokatori trezora u digitalnom svijetu, taj se novčanik može pratiti do vlasnikove adrese internetskog protokola (IP adresa), koja vlasnika povezuje s računalom na jedinstvenom mjestu u određenom trenutku. Jednostavno objašnjeno: kada se dogodi bitcoin transakcija, transakcija se emitira iz komunikacijskog centra nazvanog "čvor" i zatim se širi u druge čvorove nazvane "peers". Te se informacije brzo brzo šire na svaki od tih čvorova uzastopno po cijeloj mreži. Taj se postupak prikladno naziva "protokol tračanja". Jednostavno, svaki Bitcoin ima vidljivu internetsku poziciju i fizičku lokaciju na kojoj ga se, ili bolje rečeno njegovog vlasnika, može pronaći. Kao što je primijetila novinarka Grace Caffyn, Bitcoin nije "ništa više tajan nego Google pretraga s kućne internetske veze".[2]

Uz uklanjanje adresa novčanika, Epic Cash blockchain omogućava privatnost identiteta osiguravajući da se IP adrese ne mogu pratiti. To se postiže integracijom Dandelion ++ protokola. Unaprijeđujući na svom prethodniku, izvornom Dandelion Protokolu, Dandelion ++ Protokol rezultat je istraživanja sedam istraživača na polju borbe protiv napada deanonimizacije na blockchainu. Preko Dandelion ++ protokola transakcije se prosljeđuju slučajnim isprepletenim stazama ili "kablovima", a zatim se naglo raspršuju u veliku mrežu čvorova, poput sjemenja cvijeta maslačka kad ih se otpuhne sa stabljike (slika 1). Zbog toga je gotovo nemoguće pratiti transakcije do njihovog izvora, a samim time i izvornih IP adresa.

## Slika 1: Anonimizacija transakcija pomoću Dandelion ++ protokola.

***Dandelion++*** prosljeđuje poruke preko jedne od dvije isprepletene staze na grafu 4. stupnja, a zatim emitira transakcije koristeći difuziju. Na slici se transakcija širi plavim čvrstim putem broj 3. Ovim postupkom izuzetno je teško pratiti transakcije do njihovog izvora te se time čuva privatnost.




[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 Ožujka, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

# Privatnost Transakcija

Epic Cash blockchain osigurava privatnost transakcije skrivajući iznose i odnos pošiljatelja i primatelja transakcije. To se postiže primjenom ideja poznatih iz Povjerljivih transakcija (CT) 4 i CoinJoin[5], metoda koje je velikim dijelom razvio Gregory Maxwell (Bitcoin Core developer, Suosnivač i CTO Blockstream).

*CT*, izvorno kreiran od strane Adama Backa i kasnije usavršen od strane Maxwella, djeluje razbijanjem transakcija na manje dijelove pomoću homomorfne enkripcije, metode izvođenja izračuna na šifriranim informacijama bez dešifriranja radi očuvanja privatnosti. Jednom podijeljene, promatrači ne mogu vidjeti stvarne iznose transakcija zbog zasljepljujućih faktora, sustava koji baca slučajne brojeve u kombinaciju fragmenata transakcija kako bi prikrio vrijednosti tih fragmenata. U konačnici, samo ugovorne strane znaju vrijednost razmjene, dok mreža transakciju verificira potvrdom da je zbroj izlaznih vrijednosti jednak zbroju ulaznih vrijednosti, a zbroj izlaznih faktora zasljepljivanja jednak je zbroju ulaznih faktora zasljepljivanja.

Kako bi dodatno zakomplicirali posao znatiželjnih očiju, sve transakcije Epic Cash-a prekrivaju se CT-om, a zatim se pomiješaju kako bi se sakrile veze između transakcijskih strana. To se provodi kroz Maxwell-ov drugi koncept, CoinJoin.

Da bi pojednostavljeno ilustrirali CoinJoin , zamislite da A, B i C šalju Epic na X, Y i Z. Nakon slanja kroz CoinJoin medij, sve što se zna jest da A, B i C šalju i X, Y i Z primaju, dok iznosi transakcije ostaju nevidljivi. CoinJoin sustav je važan za Epic Cash zbog Jednosmjernih agregatnih potpisa (One-Way Aggregate Signatures - (OWAS), koji kombiniraju sve transakcije unutar bloka u jednu transakciju.

## Privatnost: Sažetak

Epic Cash blockchain štiti privatnost pojedinaca i njihove transakcije:

- **Eliminacije adresa novčanika – U blockchainu nema identifikatora lokacije za digitalne trezora. Transakcije se izrađuju izravno od osobe do osobe između njihovih novčanika;**
- ***Privatnih Transakcija* – podijeli transakcije na više dijelova i uvodi zasljepljujuće faktore u kolekciju tih dijelova, tako da se vrijednosti pojedinih dijelova i drugi parametri transakcija ne mogu znati;**
- ***Dandelion++ Protokola* – zamagljuje digitalne puteve transakcije s IP adrese pošiljatelja transakcije;**
- ***CoinJoin* – kombinira transakcije u snopove kako bi prikrio odnose između ugovornih strana.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 Kolovoza, 2013, post na Bitcoin Forumu, https://bitcointalk.org/index.php?topic=279249.0

# III. Zamjenivost

Charlie Lee , tvorac Litecoin-a, izjavio je da je zamjenjivost jedino svojstvo pravog novca koji nedostaje Bitcoin-u i Litecoin-u, priznajući da su privatnost i fleksibilnost sljedeće bitke za te valute.[6] Andreas Antonopoulos , jedan od vodećih svjetskih stručnjaka za blockchain, tvrdio je da su "... okaljani novčići destruktivni. Ako slomite zamjenjivost i privatnost, slomili ste i valutu."[7]

Zamjenjivost je svojstvo skupa dobara ili imovine koje osigurava da su pojedine jedinice tog skupa jednake vrijednosti i međusobno zamjenjive. To je ono što razlikuje najranije oblike valute od njihovih barterskih prethodnih sustava. Bez pouzdanja u zamjenjivost novca, taj novac brzo gubi svoju korisnost. Kao što će biti prikazano u daljnjem tekstu, zamjenjivost većine kripto valuta je neizvjesna, dok arhitektura privatnosti Epic Cash-a osigurava da ne postoji takva prijetnja.

Većina kriptovaluta sličnih Bitcoinu, po prirodi transparentnih blokova na kojima postoje, može se provjeriti kroz svaki novčanik u kojem su se čuvale. Privatne treće strane i vlade podjednako prate Bitcoin blockchain sa sve sofisticiranijim sredstvima kako bi brzo identificirali novčiće korištene u prethodnim aktivnostima. To, naravno, vodi do zabrinutosti da bi okaljani novčići jednog dana mogli biti zabranjeni u transakcijama, na štetu njihovih trenutnih dobronamjernih vlasnika.

19. ožujka 2018. američki Ured za kontrolu devizne imovine (OFAC) objavio je da razmišlja o uključivanju adresa digitalnih valuta na popis posebno imenovanih državljana (SDN), koji su entiteti s kojima američkim osobama ili tvrtkama zabranjuje ugovor. Još više zabrinjavajuće, OFAC nije isključio uključivanje adresa koje trenutno posjeduju okaljane kovanice na SDN listu, čime bi nedužni vlasnici okaljanih kriptovaluta bili na crnoj listi zbog povezanosti s okaljanim novčićima u vlasništvu. To je natjeralo profesora pravnog fakulteta sa Sveučilišta New York, Andrewa Hinkesa, da se "oprosti od zamjenjivosti", a javnost bi trebala očekivati „premiju na tek izrudarene novčiće ili dokazano neokaljane novčiće“ ...[8].

Imajući u vidu ovaj razvoj događaja, nije teško zamisliti preokret na tržištu kriptovaluta i patnje ili čak izumiranje mnogih dobro utvrđenih kripto valuta. Međutim, Epic je jedna od rijetkih kripto valuta koja ovaj problem u potpunosti izbjegava zbog snažnih značajki privatnosti prethodno opisanih u ovom radu. Uklanjanjem veze između identiteta i vlasništva i odnosa između transakcijskih strana, Epic se nikada ne može povezati s osobom ili nekom aktivnošću. Kao takva, vrijednost Epica i dalje je neovisna o svojim korisnicima i pruža visoki stupanj privatnosti i sigurnosti kojom zlonamjerni akteri na kriminalnim, financijskim ili političkim arenama ne mogu lako manipulirati.

> “...OKALJANI NOVČIĆI SU DESTRUKTIVNI. AKO SLOMITE ZAMJENJIVOST I PRIVATNOST, SLOMILI STE I VALUTU.”
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 Siječnja 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-For-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 Travnja, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 Ožujka 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

# IV. Skalabilnost

Epic Cash je MimbleWimble blockchain implementacija koja donosi napredak skalabilnosti kao rezultat učinkovitog upravljanja prostorom koje odbacuje suvišne podatke o transakcijama. Cut-Through funkcionalnost odgovorna za to osigurava da blockchain s vremenom postaje sve više prostorno učinkovit, za razliku od većine kripto valuta, uključujući Bitcoin, i da se mogu stvoriti novi čvorovi uz minimalna ulaganja u memoriju i računalnu snagu. Ostajući prostorno učinkovit, on promovira široko raspršenu mrežu i potiče decentralizaciju. Nadalje, dok svaki Bitcoin čvor mora pohraniti cijeli lanac, Epic Cash čvorovi mogu pridonijeti sigurnosti mreže na temelju male podskupine blokova.

Većina kriptovaluta zahtijeva neograničeno pohranjivanje svih podataka o transakcijama na svojim blockchainima. Bitcoin blockchain trenutno dobija 0,1353 GB svaki dan, dok se Ethereum blockcahain povećava još većom brzinom od 0,2719 GB dnevno. Ako lanac Bitcoina i dalje nastavi rasti po svojoj sadašnjoj stopi, na kraju će dostići približno 6 TB u trenutku kada se izrudari posljednji blok nagrada u 2140. godini. Ethereum će do tog datuma nadmašiti 10 TB[9]. U većini blockchaina bez MimbleWimblea transakcije moraju biti ovjerene čvorovima širom svijeta. Kako se podaci povećavaju, povećava se i opterećenje za svaki čvor. Čak i na samo 200 GB (približna veličina trenutnog Bitcoin blockchaina), sinkronizacija podataka zahtijeva stabilnu mrežu i mogućnost čitanja i pisanja po disku disku velikom brzinom.

Posljedično, rudarstvo postaje sve više centralizirano među velikim bazenima koji koriste skupe računalne resurse. **Ako bi se cijela povijest Bitcoin blockchaina pohranjivala na Epic Cash blockchain, on bi zauzimao gotovo 90% manje prostora.** Manje je brže jer svaka transakcija zahtijeva manje vremena za prijenos i sigurnost.

MimbleWimble rješava ovu dilemu za pohranu inovativnom metodom obrezivanja blokova, koja se naziva "Cut-Through". Da biste shvatili kako Cut-Through funkcionira, najbolje je prvo pogledati kako se transakcije i blokovi sastavljaju u unutar MinbleWimble blockchaina.

**Ulazi:**

Reference na stare izlaze;

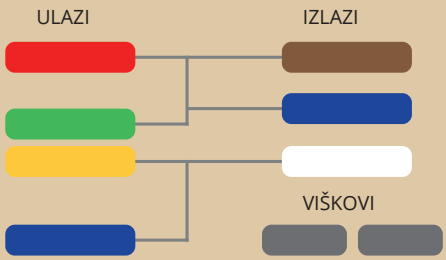
**Izlazi:**

*Povjerljivi Transakcijski Izlazi i* **rangeproofs**;

**Viškovi:**

Razlike između ulaza i izlaza, plus **potpisi** (za autentifikaciju i dokazivanje neinflacije).).

**Slika 2:**
**MimbleWimble djelovi transakcija.**




[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 Siječnja 2019, https://www.longhash.com/news/blockchains-big-data-problem

Svi Epic Cash blokovi sadrže:

**Merkle Stabla transakcijskih ulaza;**

**Merkle Stabla transakcijskih izlaza i rangeproofs;**

**Listu nepotrebnih vrijednosti i potpisa.**

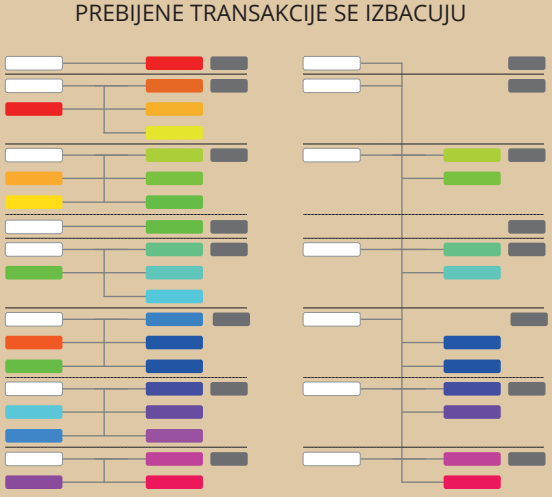
Na slikama 2 i 3, prilagođene iz prezentacija Andrewa Poelstre[10], možemo vidjeti tek izrudareni Epic koji je predstavljen kao bijele ulazne ćelije. Jednako obojene ćelije predstavljaju izlaze s odgovarajućim porošenim ulazima. Cut-Trough procesom uklanjaju se ulazi i usklađeni potrošeni izlazi kako bi se oslobodio prostor unutar bloka, što smanjuje količinu podataka koju je potrebno pohraniti u blokckchain. Iako su transakcije izostavljene iz glavne knjige, preostale jezgre (samo 100 bajtova) trajno dokumentiraju da su se transakcije održale.

Kako se blokovi i dalje kontinuirano stvaraju, MimbleWimble primjenjuje Cut-Trough kroz sve blokove, tako da dugoročno gledano sve što ostaje su zaglavlja blokova (otprilike 250 bajtova), neiskorištene transakcije i jezgre transakcija (otprilike 100 bajtova). Grin, druga implementacija MimbleWimblea koja je pokrenuta, pokazao je da će lanac MimbleWimble s sličnim brojem transakcija kao i Bitcoin lanci biti gotovo 10% veličine Bitcoin lanca.[11] Nadalje, veličina čvora bit će "veličine nekoliko GB za Bitcoin lanac, što je potencijalno moguće optimizirati na nekoliko stotina megabajta."[12]

To je u kontrastu s Bitcoinom, gdje svaki čvor mora pohraniti cjelokupni blockchain. S vremenom, kako prostorna učinkovitost Epic Cash bloka raste s obzirom na Bitcoin blockchain, tako će se povećati i troškovna učinkovitost u odnosu na sudjelovanje čvorova u Epic Cash mreži. Manje prepreke za sudjelovanje pomažu u osiguravanju ključne otpornosti na čvornom sloju mrežnog dizajna.

Kroz implementaciju MimbleWimblea i primjenu Cut-Trough procesa obrezivanja, Epic Cash blockchain nudi skalabilnost na način na koji kriptovalutna zajednica često previdi. To je sama srž Bitcoina i sličnih projekata: decentralizacija. Bez obzira na to koliko transakcija u sekundi novčić može obraditi, što to vrijedi ako ga ne može održavati široka i raznolika mreža? Ako su zahtjevi za memorijom takvi da validacija u konačnici gravitira jakim rudarskim konglomeratima, tada se zaobilaze svi napori zajednice kriptovaluta u stvaranju decentraliziranog ekosustava. Kako bi se osigurala dodatna propusnost, planirana je implementacija Lightning drugog sloja kao kratkoročni cilj u planu razvoja Epic Cash-a.

**Slika 3: MimbleWimble transakcije prije prije i poslije reza.**




[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 Studenog, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, ***Grin Blockchain Size,*** Prosinca 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, ***Introduction to Mimblewimble and Grin,*** 28 Ožujka 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

# V. Monetarna Poltika

Monetarne politike Epic Casha i Bitcoina vrlo su slične. Trenutačna količina Epic Casha u opticaju najprije se brzo povećava, a zatim se sinkronizira s cirkulirajućom opskrbom Bitcoina 2028. godine. Nakon toga se povećava smanjenom brzinom do dostizanja maximalne količine 21 milijuna Epica 2140. Epic Cash ima kvalitete postati sigurno spremište vrijednosti na duže vrijeme zato jer cirkulirajuća količina Epica poznata u bilo kojem trenutku duž njezinog životnog ciklusa emisije i dovodi do fiksne maksimalne opskrbe. Monetarnu politiku Epic Casha karakteriziraju sljedeće četiri značajke:

- Brza emisija tijekom prvih devet godina njezina životnog vijeka, tijekom kojih je potrebno izrudariti 20.343.750 Epica (96.875% ukupne opskrbe). Točne stope emisija prikazane su u odjeljku Raspored Emisija u ovom radu;
- Cirkulirajuća količina Epica i emisija usklađuje se s onima Bitcoina u Epic Singularity događaju oko 24. svibnja 2028. Nakon singularnosti, stopa emisije smanjuje se sve brže i brže, dok cirkulirajuća količina raste s opadajućim faktorom brzine;
- Maksimalna količina od 21 milijuna Epica bit će postignuta 2140. godine, otprilike u isto vrijeme kada Bitcoin dosegne maksimalnu količinu od 21 milijuna jedinica;
- Epic ima strukturu dijeljenja do 8 decimala, tako da: 1 Epic je jednak 100.000.000 freemana (jednako kao što je 1 Bitcoin jednak 100.000.000 satoshija).

Monetarna politika Epic Casha modelirana je prema Bitcoinu iz sljedećih razloga:

- Slažemo se s ekonomskim osnovama Bitcoina, naime da su oskudnost i predvidivost cirkulirajuće količine novca baza da bi roba postala snažna pohrana vrijednosti;
- Javnosti je već poznat i dokazan model Bitcoina u posljednjih deset godina od njegovog osnutka. Otprilike sinkronizirajući se s Bitcoinovom cirkulirajućom količinom i zrcalivši maksimalnu količinu i strukturu djeljenja Bitcoina, Epic je krenuo putem najmanjeg otpora prema masovnom usvajanju.

# VI. Raspored Emisije

Epic Cash ima ukupno 33 rudarske ere, od kojih je svaka definirana smanjenjem nagrada u bloku, u odnosu na njihovo prethodno razdoblje. Epic Genesis, datum na kojem se rudari Epic blok # 1, biti će kolovoza 2019. Blokovi se rudare jedan svake minute. Prvih pet razdoblja će proizvesti gotovo 97% maksimalne količine Epica, što odgovara 20 godina Bitcoin emisije u otprilike devet godina. Ovo se može smatrati šansom za "vraćanje sata" za one koji su propustili spektakularni uspon Bitcoina.

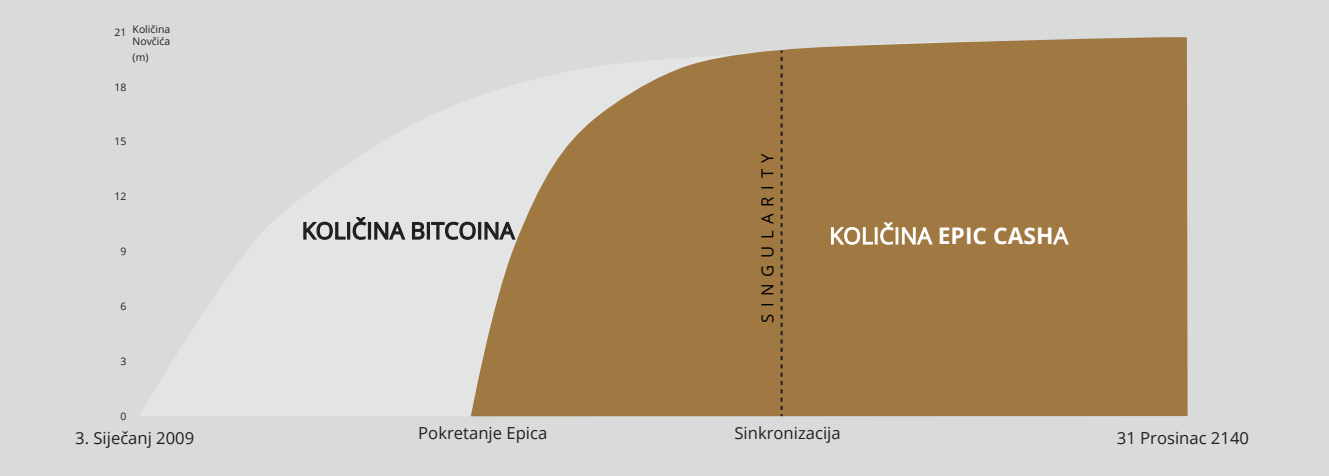
Raspored emisija u tablici 1 prikazuje datum početka i završetka prvih sedam rudarskih razdoblja, odgovarajuće nagrade za blok i posljedičnu cirkulirajuću količinu Epica za svako razdoblje. Razdoblja od 8 do 33 nisu uvrštena u tablicu radi sažetosti. Za ta razdoblja dovoljno je razumjeti da će svako sljedeće razdoblje imati blok nagradu koja je upola manja od nagrade iz prethodnog razdoblja, točno kao u Bitcoinu. Količina Epica emitirane tijekom svakog razdoblja biti će zbroj nagrada u bloku unutar četverogodišnjeg razdoblja (otprilike 1460 dana).

U Epic Singularity (2028) događaju, cirkulirajuća količina Epica presijeca količinu Bitcoina, u tom trenutku Epic Cash prihvaća obrazac nagrađivanja i prepolovljenja Bitcoin bloka, koji uvjetuje da se nagrade na bloku smanjuju za polovicu svake četiri godine. Jedina iznimka je da se blokovi Epica i dalje rudare brzinom od jedne minute, nasuprot brzini Bitcoina od jednog bloka svakih deset minuta. Na taj način, cirkulirajuća količina Epica održava približni paritet s cirkulirajućom količinom Bitcoina do kraja njihovog postojanja.

**Tablica 1: Raspored emisija za prvih sedam rudarskih razdoblja. Datumi su aproksimativni.**

| Razdoblje | 1 | 2 | 3 | 4 | 5 | SINGULARITY | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Blok Nagrada | 16 | 8 | 4 | 2 | 1 | | 0.15625 | 0.078125 |
| Početak | Aug 1, 2019 | Jun 29, 2020 | Oct 11, 2021 | Jun 3, 2023 | Aug 10, 2025 | | May 24, 2028 | May 22, 2032 |
| Kraj | Jun 29, 2020 | Oct 11, 2021 | Jun 3, 2023 | Aug 10, 2025 | May 24, 2028 | | May 22, 2032 | May 20, 2036 |
| Trajanje (dana) | 334 | 470 | 601 | 800 | 1019 | | 1460 | 1460 |
| Početna Količina | 0 | 7,695,360 | 13,109,760 | 16,571,520 | 18,875,520 | | 20,342,880 | 20,671,380 |
| Završna Količina | 7,695,360 | 13,109,760 | 16,571,520 | 18,875,520 | 20,342,880 | | 20,671,380 | 20,835,630 |
| % od ukupne Količine | 36.6% | 62.4% | 78.9% | 89.9% | 96.9% | | 98.4% | 99.2% |

**Slika 4: Raspored emisija Epica i Bitcoina.**



# VII. Rudarenje

Epic Cash blockchain provodi decentralizaciju pružajući širok izbor računalnog hardvera. Rudarenje Epica izvorno je dostupno za CPU, GPU, i ASIC, koristeći tri odgovarajuća hashing algoritma: RandomX, ProgPow, i CuckAToo31+. Algoritmi se mogu trenutno i trivijalno zamjenjivati bez ugrožavanja integriteta lanca.

## 1 RandomX i CPU

RandomX je Proof-of-Work (PoW) algoritam optimiziran za CPU opće namjene. On koristi nasumično izvršavanje programa s nekoliko vrlo teških tehnika za postizanje sljedećih ciljeva:

- Sprječavanje razvoja ASIC-a s jednim čipom;
- Smanjivanje prednosti učinkovitosti specijaliziranog hardvera nad procesorima opće namjene.

Rudarenje Epica koristeći CPU zahtijeva neprekidnu raspodjelu 2 GB2 fizičke RAM memorije, 16 KB L1 cache, 256 KB L2 cache, i 2 MB L3 cache po rudarskoj jezgri[13]. Uređajima koji koriste Windows 10 sustav potrebno je 8 GB ili više RAM-a. Nije nezamislivo da bi jedan dan u ne tako dalekoj budućnosti mobiteli mogli postati održivi rudarski čvorovi. Rana integracija procesora u rudarsku mrežu Epic Cash izvrsna je prilika za mnoge koji imaju samo skromna računalna sredstva da zarade na blok nagradama pomažući u osiguranju mreže Epic Cash.

## 2 ProgPow i GPU

Programmatic Proof-of-Work (ProgPow) je algoritam koji ovisi o propusnosti memorije i izračunavanju randomiziranih matematičkih nizova unutar jezgre, koji koristi mnoge računalne značajke GPU-a i na taj način učinkovito koristi ukupni trošak energije hardvera. Kako je ProgPow posebno dizajniran kako bi u potpunosti iskoristio javno dostupne GPU kartice, teško je i skupo postići značajno veće učinkovitosti pomoću specijaliziranog hardvera. Kao takav, algoritam ProgPow ublažava poticaje za velike ASIC bazene da nadmaše GPU-ove, kao što se često vidi kod mnogih drugih PoW algoritama, kao što je Bitcoinov SHA-256. GPU, iako nisu toliko rasprostranjeni kao CPU, i dalje su obično dostupni. Tehnološkim razvojem koje pokreću, Nvidia i AMD, GPU je u mogućnosti paralelno obraditi više redova rudarskih rješenja u usporedbi s CPU jedinicom. Zbog ove kombinacije sveprisutnosti i velike snage obrade GPU će pružiti okosnicu većine rudarskih aktivnosti tijekom početnih razdoblja, kako je naznačeno u tablici 2.

## 3 CuckAToo+31 i ASIC

CuckAToo31 + je ASIC prijateljska permutacija Cuckoo Cycle algoritma koju je razvio nizozemski informatičar John Tromp. Rođak na ASIC otpornog CuckARoo29 , CuckAToo31+ generira nasumične bipartitne grafove te predstavlja rudarima zadatak da pronađu petlju određene duljine 'N' koja prolazi kroz vrhove tog grafa.

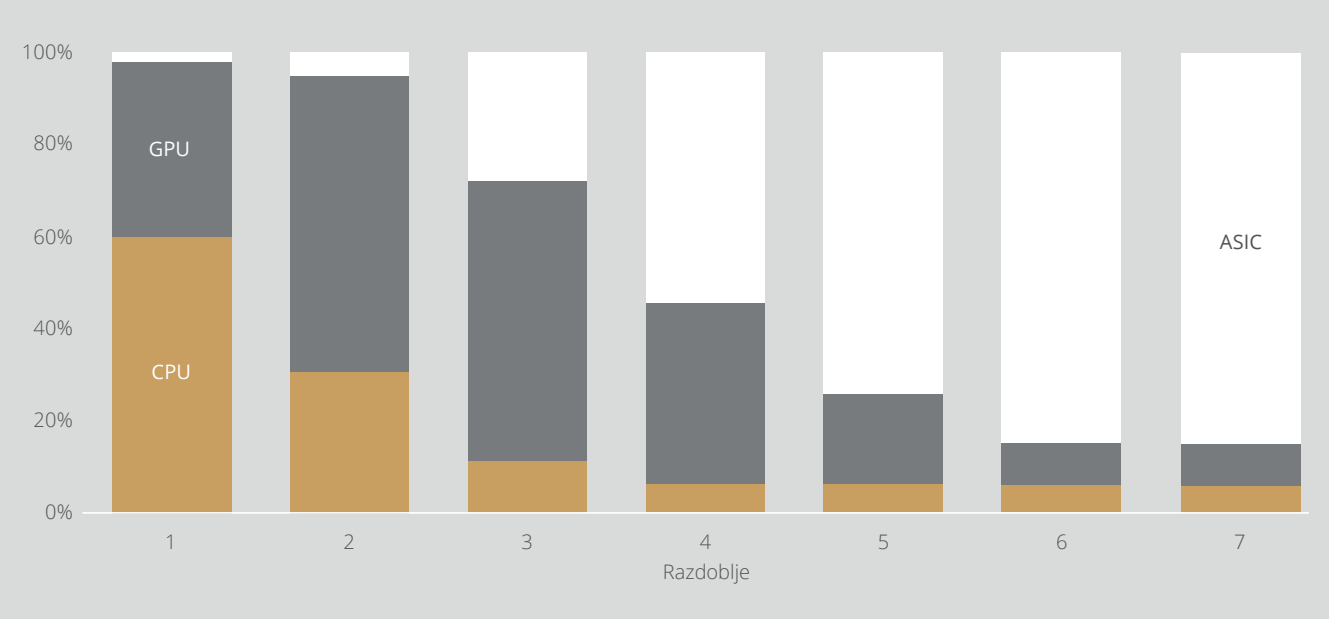
[13] Tevador, ***RandomX***, 28 Ožujka 2019, https://github.com/tevador/RandomX

Ovo je zadatak vezan za memoriju, što znači da vrijeme rješenja ovisi o propusnosti memorije, a ne brzini procesora ili GPU-a. Kao rezultat toga, algoritmi Cuckoo Cycle proizvode manje topline i troše znatno manje energije od tradicionalnih PoW algoritama. CuckATоo31 +, prijateljski nastrojen prema ASIC-u, omogućava poboljšanje učinkovitosti u odnosu na GPU koristeći stotine MB SRAM memorije dok je usko grlo memorijski I/O[14]. U konačnici, ASIC nudi najveću potencijalnu ekonomisku dobit od tri mogućnosti rudarenja. Međutim, u korist inkluzivnosti, iako im je rano dodijeljen mali dio nagrada za rudarstvo u odnosu na CPU i GPU, ASIC preuzima većinski udio u rudarskim nagradama blokova, pod pretpostavkom da će postojati konkurentan ekosustav proizvođača uređaja za CuckATоo31 +.

**Tablica 2: Dodjeljivanje nagrada za rudarstvo. Podložno reviziji. Raspodjela će biti usmjerena na postizanje maksimalne decentralizacije i u skladu s dugoročnim interesima mreže.**

| Razdoblje | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Dana | 334 | 470 | 601 | 800 | 1019 | 1460 | 1460 |
| CPU | 60% | 30% | 10% | 5% | 5% | 5% | 5% |
| GPU | 38% | 65% | 62% | 40% | 20% | 10% | 10% |
| ASIC | 2% | 5% | 28% | 55% | 75% | 85% | 85% |

**Slika 5: Isplate nagrada za svako razdoblje prema Tablici 2. Podložno reviziji.**




[14] Le Sceller, Quentin, ***An Introduction to Grin Proof-of-Work,*** 16 Studenog, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

# 4 Doprinosi Rudarenja

Počevši sa stvaranjem Epic Genesis bloka (2019) i završavajući sa zadnjim Epic Singularity blokom (2028), tijekom procesa rudarstva dolazi do raspodjele Epica koja se preusmjerava kao doprinos za rudarstvo prema EPIC Blockchain fondaciji.

EPIC Blockchain Foundation posvećena je tehničkom razvoju i promicanju svijesti i korisnosti projekta Epic Cash tijekom prvih godina njegovog osnutka stvaranjem marketinških aktivnosti i razvijanjem partnerstva u industriji financijske tehnologije.

Nakon Singularity događaja, EPIC Foundation ulogu preuzeti će EPIC Distributed Autonomous Corporation (EDAC), koju će razviti fondacija prije primopredaje.

EPIC Blockchain Foundation financira se postotkom rudarske nagrade oduzete od nagrada u bloku, prema sljedećim godišnjim stopama:

**Tablica 3: Godišnje stope za doprinose rudarstva Fondaciji kao postotak nagrada za rudarstvo.**

| Godina | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 |
|---|---|---|---|---|---|---|---|---|---|---|
| % Nagrada Rudarenja | 8.88 % | 7.77 % | 6.66 % | 5.55 % | 4.44 % | 3.33 % | 2.22 % | 1.11 % | 1.11 % | 0 % |

# VIII. Zaključak

Epic želi biti poznat kao "decentralizirano digitalno srebro", medij razmjene koji odgovara Bitcoinovoj prepoznatoj poziciji decentraliziranog digitalnog zlata. Ponovnim uvođenjem izgubljene zamjenjivosti na znatno energetski učinkovitiju i ekološki prihvatljiviju hardversku okosnicu, Epic Cash vraća ravnotežu snage na stranu pojedinačnih korisnika, u velikoj suprotnosti s nedavnim trendovima centralizacije. Kombinacija Bitcoin ekonomije, teorije igara i dokazane formule dokaza o radu s najboljim suvremenim blockchain tehnologijama rezultira nepovjerljivom, nepromjenjivom i decentraliziranom valutom (Epic) koja je skalabilna, zamjenjiva i štiti privatnost svojih korisnika. Epic Cash blockchain je otvorenog koda, javan, bez granica i otporan na cenzuru. Čuva privatnost i bogatstvo svojih korisnika i nagrađuje one koji svoj hardver koriste za podršku mreže rudarenjem. Svaki je Epic izrudaren u postojanje dokazom o radu. Dostupna količina počinje na nuli te se mreža smatra fer pokrenutim, s funkcionalnim testnetom koji trenutno radi.

**Epic Cash Ključne Činjenice::**

- **Rudarenje počinje Kolovoza 2019.**
- **Epic Cash blockchain je baziran na MimbleWimble protokolu.**

  Najvažnije značajke protokola su:

  1. **Cut-Through** – uklanjanje suvišnih informacija iz blockchaina za promociju prostorne učinkovitosti, poticanje širokog sudjelovanja u validaciji mreže i decentralizacija upravljanja;
  2. ***CoinJoin*** – kombiniranje transakcija unutar bloka u snop kako bi se osigurala zamjenjivost kriptovalute Epic;
  3. ***Dandelion++ Protokol*** – širenje transakcija komunikacijom preko isprepletenih kanala i difuziranjem kroz široku mrežu čvorova, prekidajući veze između transakcija i njihova podrijetla;
  4. **Bez Adrese Novčanika** – upotreba velikeog višestrukog potpisa za generiranje privatnih ključeva za jednokratnu upotrebu korisnika, eliminirajući u potpunosti potrebu za adresama novčanika.

---

- **Epic Cash monetarna politika** dizajnirana je tako da sinkronizira cirkulirajuću opskrbu Epica i Bitcoina u otprilike devet godina i dosegne istu maksimalnu opskrbu od 21 milijuna jedinica istovremeno s Bitcoinom, u 2140. godini. Ova opadajuća inflatorna politika jamči transparentnost, predvidljivost opskrbe i nedostatak, potičući sigurnost dugoročne pohrane vrijednosti.

---

- **Rudarenje** koje uključuje CPU, GPU i ASIC putem odgovarajućih algoritama RandomX, ProgPow i CuckATo31 + kako bi se olakšalo masovno usvajanje i mrežna učinkovitost.

---

# IX. Tehnička Specifikacija

**Ime Projekta:** Epic Cash
**Ime Valute:** Epic
**Vrijeme Bloka:** 60 sekundi
**Veličina Bloka:** 1 MB
**Početna Količina:** 0
**Maksimalna količina:** 21,000,000
**Prvi Blok (Genesis):** Kolovoza 2019
**Konsenzus:** RandomX (CPUs), ProgPow (GPUs) i CuckATOO31+ (ASICs)

**Poveznice:**

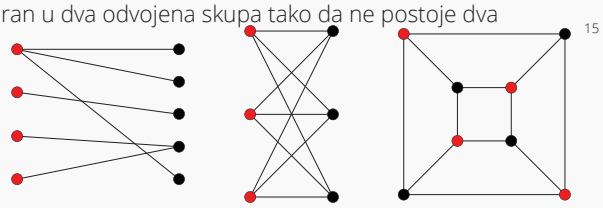
www.epic.tech

t.me/EpicCash – Telegram

# X. Rječnik

**ASIC** Integrirani krugovi specifični za aplikaciju; čip koji je osmišljen za jedinstvenu svrhu

**Bipartitni graf** skup točaka grafikona dekomponiran u dva odvojena skupa tako da ne postoje dva čvorišta grafa unutar istog skupa.




**Faktor Zasljepljenja** slučajni element uveden u digitalnu poruku radi olakšavanja šifriranja; zajednička tajna između dviju strana koja šifrira ulaze i izlaze u toj konkretnoj transakciji, kao i javne i privatne ključeve transakcijskih strana.[16]

**Blok Nagrada** novi Epic koji distribuira mreža kao nagradu za izvršene operacije računanja potrebnih za provjeru transakcija unutar novog bloka.

**Cache** hardverska ili softverska komponenta koja pohranjuje podatke kako bi se budući zahtjevi za te podatke mogli brže uručiti.

**Trenutna Opskrba** količina Epica koji postoji u određenom trenutku.

**CPU** Centralna procesna jedinica: računalna komponenta odgovorna za interpretaciju i izvršavanje većine naredbi iz drugog hardvera i softvera.

**Cut-Through** MimbleWimble blockchain proces kojim se uklanjaju ulazi i usklađeni potrošeni izlazi kako bi se oslobodio prostor unutar bloka, smanjujući količinu podataka potrebnih za pohranjivanje u blockchain.

**Decentralizacija** stanje raspršenosti rada i upravljanja mrežom.

**Emisija** stvaranje novog Epica koji su rudari zaradili u blok nagradama. Epic se kreira svakih 60 sekundi nakon što se transakcije potvrde u blockchain.

**Epic Singularity** točka u kojoj se cirkulirajuća opskrba Epica sinkronizira s cirkulirajućom opskrbom Bitcoina (svibanj 2028).

**Višak (MimbleWimble)** razlika između izlaza i ulaza, plus potpisa (za autentifikaciju i dokazivanje neinflacije).

**Zamjenjivost** svojstvo dobra ili robe kojom su pojedine jedinice u osnovi međusobno zamjenjive, a svaki je njegov dio nerazlučiv od drugog dijela.

**Genesis (Događaj)** rudarenje prvog bloka Epica i službeno pokretanje blockchaina.

**GPU** Jedinica za obradu grafike: jedinica koja sadrži programibilni logički čip (procesor) specijalizirana za funkcije prikaza. Potrošački GPU-ovi mogu biti vrlo pogodni za rudarenje kriptovaluta.

**Prepolovljenje (za Bitcoin)** javlja se svake 4 godine. Stopa opskrbe smanjuje se za 50% nakon svakog događaja prepolovljenja.

**Hash** vrijednost izračunata iz osnovnog ulaza pomoću hashing funkcije.

**Hashing Algoritam (funkcija)** matematički algoritam koji preslikava podatke proizvoljne veličine u hash fiksne veličine koji se koristi za generiranje i provjeru digitalnih potpisa, kodova za provjeru autentičnosti poruka (MAC) i drugih oblika provjere autentičnosti.

**Homomorfna enkripcija** metoda izvođenja izračuna na šifriranim informacijama, a da se prethodno ne dešifrira.

**Nepromjenjivost** stanje u kojem se objekt ne može mijenjati nakon njegovog stvaranja.

**Ulaz (MimbleWimble)** komponenta MimbleWimble transakcije koja predstavlja stranu koja šalje ugovor; stvorena iz izlaza prethodnih transakcija.

**I/O** ulaz/izlaz; komunikacija između sustava za obradu informacija, poput računala, i vanjskog svijeta, možda ljudskog ili drugog sustava za obradu informacija.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 Listopada 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

| | |
|---|---|
| **Maksimalna Količina** | količina Epica koju treba postići, nakon tog trenutka cirkulacijska opskrba se neće više povećavati (21 000 000 Epic). |
| **Memorijski Zahtjevan** | korištenje puno RAM-a da se spriječe pokušaji pokretanja paralelnih konekcija. Memorijski zahtjevne funkcije su algoritmi za koje je vrijeme računanja prvenstveno odlučeno raspoloživom memorijom za čuvanje podataka. Poznate su i kao memorijske funkcije. |
| **Merkle Stablo** | struktura podataka koja se koristi u računalnim aplikacijama. Kod blockchaina, Merkle stabla omogućuju učinkovitu i sigurnu provjeru sadržaja u velikim strukturama podataka. |
| **MimbleWimble** | protokol pušten u javnost od nepoznatog suradnika pod pseudonimom Tom Elvis Jedusor, u chat kanalu za Bitcoin razvojne programere |
| **Višestruki Potpis** | shema digitalnog potpisa koja grupi korisnika omogućuje potpisivanje jednog dokumenta. Algoritam obično stvara zajednički potpis koji je kompaktniji od zbirke različitih potpisa svih korisnika[17]. |
| **Čvor** | računalo koje se povezuje na blockchain mrežu i grana se se na druge čvorove unutar mreže za distribuciju informacija o transakcijama i blokovima, koristeći peer-to-peer komunikaciju. |
| **One Way Aggregate Signature (OWAS)** | transakcijski potpis sastavljen od mnogih potpisa koji su šifrirani na način da je vrlo teško dohvatiti pojedinačne potpise koji su dio tog agregata. |
| **Izlaz (MimbleWimble)** | komponenta MimbleWimble transakcije koja predstavlja potvrdu transakcije; koristi se kao ulaz za naknadne transakcije. |
| **Pedersen Commitment Scheme** | kriptografski primitiv koji omogućuje dokazivaču da se opredijeli za odabranu vrijednost bez otkrivanja bilo kakvih podataka o njoj i bez mogućnosti da dokazivač poništi opredjeljenje na tu vrijednost. |
| **Privatni Ključ** | privatni ključ je maleni djelić koda koji je uparen s javnim ključem za pokretanje algoritama za šifriranje i dešifriranje teksta. Nastao je kao dio kriptografije javnog ključa tijekom šifriranja asimetričnih ključeva i koristi se za dešifriranje i pretvaranje poruke u čitljiv format. |
| **Dokaz o Radu (PoW)** | dio podataka koji je teško (skupo i dugotrajno) proizvesti, ali je lako provjeriti i koji udovoljava određenim zahtjevima. Dokazi o radu često se koriste u stvaranju blokova kriptovaluta. |
| **Javni Ključ** | javni se ključ stvara u kriptografiji javnog ključa koja koristi algoritme za enkripciju asimetričnih ključeva. Javni ključevi koriste se kako bi se pretvarilo poruku u nečitljiv format. |
| **RAM (Random Access Memory)** | čipovi za brzi pristup podacima u računalnom uređaju u kojem se čuvaju operativni sustav (OS), aplikativni programi i podaci u trenutačnoj uporabi kako bi ih procesor uređaja mogao brzo doseći. |
| **Rangeproof** | potvrda obveze koja provjerava da je zbroj ulaznih transakcija veći od zbroja izlaznih transakcija i da su sve vrijednosti transakcije pozitivne. Raspon zaštite osigurava da monetarna ponuda nije bila ugrožena. |
| **(Digitalni) Potpis** | standardni dio blockchain protokola, koji se uglavnom koristi za osiguranje transakcija i blokova transakcija, prijenos informacija, upravljanje ugovorima i bilo koje druge slučajeve u kojima je važno otkrivanje i sprječavanje bilo kakvog vanjskog zlostavljanja. Oni nude tri prednosti pohrane i prijenosa informacija na blockchain:<br>• Otkrivaju jesu li podaci koji su poslani bili promjenjeni;<br>• Ovjerava sudjelovanje određene stranke u transakciji;<br>• Može biti pravno obvezujuć. |
| **SRAM (Static Random Access Memory)** | RAM (Random Access Memory) memorija koja zadržava podatkovne bitove u svojoj memoriji sve dok napajanje nije prekinuto. |
| **Propusnost** | mjera koliko transakcija u sekundi može obaviti određeni protokol kriptovaluta. |
| **Trustlessness** | mogućnost kriptovalutne mreže da se pridržava pravila protokola bez provođenja/uplitanja od strane središnjeg autoriteta. |

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

# EPIC CASH

EPIC PRIVATNI INTERNET NOVAC