Družina Freeman

4. julij, 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

Elektronski peer-to-peer denarni sistem

SKLADIŠČENJE VREDNOSTI + MEDIJ IZMENJAVE + OBRAČUNSKA ENOTA

1,7 milijarde odraslih nima dostopa do globalnega finančnega sistema, medtem ko je dodatne 1,3 milijarde še bolj zapostavljenih. Epic Cash odklene človeški potencial s povezovanjem posameznikov na globalni trg. Hitro, navidezno brezplačno za uporabo in odprto za vse.

Verzija 7.1b

Kazalo

I. Povzetek

Epic Cash je končna točka na poti do pravega P2P internetnega denarja, ki je temelj zasebnega finančnega sistema. Valuta Epic želi postati najbolj učinkovita oblika digitalnega denarja za varovanje zasebnosti na svetu. Da bi izpolnila ta cilj, mora ustrezati trem glavnim funkcijam denarja:

1. **Skladiščenje vrednosti** – Se lahko shrani, pridobi, naknadno izmenja in ima predvidljivo vrednost po pridobitvi;
2. **Medij izmenjave** – Sprejme se vse, kar predstavlja standard vrednosti in kar se lahko zamenja za blago ali storitve;
3. **Obračunska enota** – Enota, s katero se vrednost stvari obračuna in primerja.

	$ USD	BTC	EPIC
Skladiščenje vrednosti	✗	✓	✓
Medij izmenjave	✓	✗	✓
Obračunska enota	✓	✗	✓

Leta 2009 se je Bitcoin pojavil kot prva digitalna valuta, osnovana na blockchainu, in skupaj z njim tri določujoče karakteristike s pomočjo katerih so ovrednotene druge kriptovalute:

- **Brez potrebe po zaupanju** – Od nikogar se ne zahteva, da zaupa kakršnikoli centralizirani entiteti ali nasprotni stranki, zato da bi lahko omrežje delovalo;
- **Nespremenljivost** – transakcij ni mogoče razveljaviti;
  a. Ponovno pisanje zgodovine mora biti malo verjetno ali težko;
  b. Prenos sredstev mora biti nemogoč za kogarkoli razen za lastnika zasebnega ključa, s katerim so ta sredstva povezana;
  c. Vse transakcije so zapisane na blockchainu.
- **Decentralizacija** – "Blockchaini so politično decentralizirani (nihče jih ne nadzoruje) in arhitekturno decentralizirani (brez infrastrukturne točke napake)"[1].

Bitcoin je tehnološko ubral nove poti, medtem pa upošteval časovno preizkušene temelje v strukturi svoje denarne politike. Bitcoinov uspeh je močno povezan z njegovo omejeno zalogo, združeno z blockchainom, ki je nespremenljiv, decentraliziran in brez potrebe po zaupanju. Epic Cash posnema Bitcoinovo denarno politiko manjšanja inflacije in omejene zaloge, da zagotovi, da lahko valuta Epic služi kot učinkovito skladiščenje vrednosti.

Kljub Bitcoinovemu uspehu so bile odkrite nekatere pomanjkljivosti od njegovega spočetja pred 10 leti. Drugi projekti so poskušali premagati te pomanjkljivosti in raziskali najboljše od teh za uporabo za naše izhodišče. Odločili smo se za uporabo Grinove kode in odličnega dela več drugih projektov, ki nam bo pomagalo izpopolniti težko izborjene dosežke in odkrite pomanjkljivosti predhodnikov Epic Casha. Epic Cash poseduje ključne značilnosti za idealno valuto:

- **Fungibilnost** – Vrednost dane enote Epica mora biti vedno enaka drugi enoti Epica, tako kot je en jen ali juan vedno enak in nadomestljiv z drugim jenom ali juanom. Dosežek fungibilnosti je v veliki meri odvisen od zasebnosti.
- **Zasebnost** – Epic Cashev blockchain varuje anonimnost imetnikov Epica in uporabnikov s tem, da ščiti podrobnosti transakcij od tretjih oseb in je osnovan, da je neviden za nadzor in da ga je hkrati nemogoče izslediti.
- **Razširljivost** – Epic Cash ohranja prostorno učinkovit blockchain, na katerem se lahko preprosto ustvarijo nova vozlišča brez opreme, ki zahteva veliko virov. Epic Cashev blockchain je sposoben vsaj dvakratne prepustnosti Bitcoina.
- **Hitrost** – Transakcije Epic Casha so nemotene, neprekinjene in izvedene hitreje kot v prejšnjih generacijah blockchain tehnologije. Medtem ko Bitcoin zahteva, da šest 10-minutnih blokov doseže popolno potrditev transakcije, se Epicove transakcije zgodijo znotraj potrditve enega bloka takoj, ko je narudarjen 1-minutni blok.

[1] Buterin, Vitalik, ***The Meaning of Decentralization***, 6. februar, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Zasebnost

Uporaba denarja v današnjem svetu se lahko razume kot kolektivni prenos obračunskih enot med ljudmi in institucijami. Svet denarja se lahko opiše na poljubni točki v času z odgovori na naslednja vprašanja:

1. *Kdo si ga lasti in koliko si ga lastijo?*
2. *Kdo posluje s kom in s kakšno količino?*

Za tradicionalne fiat valute in prav tako za Bitcoin lahko odgovorimo na te vprašanji. Pri tem lahko odkrijemo veliko o življenjih ljudi, kot so vzorci potrošnje, lastništvo in transakcijske nasprotne stranke. Začrtamo lahko dokaj natančne zaključke o interesih in namerah posameznika s sledenjem prenosom vrednosti. Brez zasebnosti so lahko transakcijski podatki v rokah plenilskih tretjih oseb nevarne informacije.

Uporaba kriptovalut prejšnjega desetletja prikazuje kontinuum "zasebnosti" v različnih implementacijah blockchaina. Lestvica zasebnosti, če jo upoštevamo, se razprostira od odprte in razvpite na eni strani do anonimne na drugi. Ko se zasebnost poveča, se drugi bistveni temelj kriptovalute, ki je ta, da je brez potrebe po zaupanju, zmanjša. Kot je razvidno iz uspeha analiznih storitev Bitcoinovega blockchaina je Bitcoin bolj usmerjen k razvpito transparentni strani zasebnega spektra. Uporabniki morajo opraviti vedno več korakov, da zagotovijo, da nehote ne poslujejo z "umazanim" Bitcoinom. Rešitev Epic Casha se zanese na anonimnost in obnovi to bistveno lastnost s tem, da zagotovi, da sta tako zasebnost posameznika kot tudi zasebnost transakcij, zasnovani v sistemu na temeljni ravni.

Zasebnost identitete

Zasebnost transakcije

Zasebnost identitete

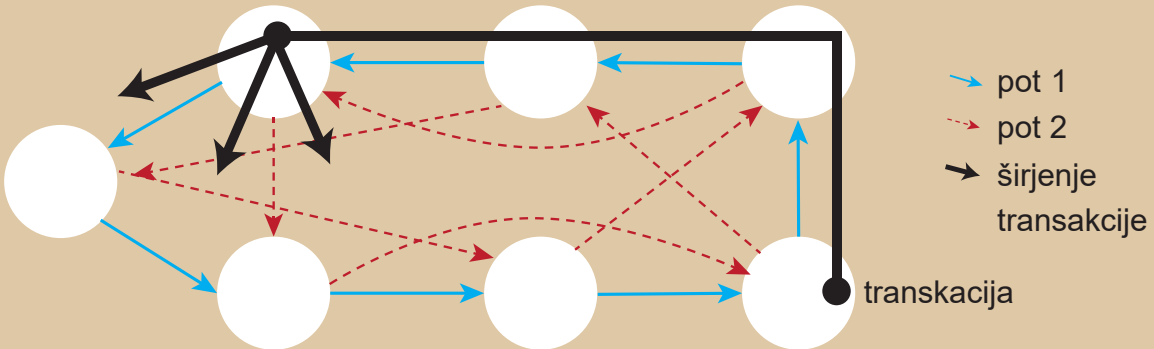
Večina kriptovalut kot naprimer Bitcoin je shranjenih v denarnicah, katerih naslovi se nanašajo na javne ključe, ki so izpeljani iz zasebnih ključev denarnice. Te naslove lahko obravnavamo kot lokatorje zasebnega sefa v digitalnem svetu. Epic Cashev blockchain popolnoma odstrani naslove in namesto tega uporabi en velik multipodpis, iz katerega so generirani vsi javni in zasebni ključi na osnovi enkratne uporabe.

Ker so Bitcoinovi naslovi denarnice lokatorji sefa v digitalnem svetu, se lahko to denarnico izsledi do IP-naslova (Internet Protocol) lastnika, ki ga zasidra na računalniku na edinstveni lokaciji v dani točki v času. Preprosto povedano: ko se zgodi Bitcoin transakcija, se ta odda iz komunikacijskega središča, ki se imenuje "vozlišče" in se nato razširi do ostalih vozlišč, ki se imenujejo "soležniki". Ta informacija se potem hitro razširi do vsakega od teh soležnih vozlišč zaporedno po vsem omrežju. Temu postopku rečemo "protokol obrekovanja". Preprosto ima vsak Bitcoin vidno pozicijo na spletu in fizično lokacijo, kjer ga lahko najdemo ali bolje rečeno, njegovega lastnika. Na to je opozorila tudi novinarka Grace Caffyn, ki je dejala: "Bitcoin ni večja skrivnost kot iskanje preko Googlea s pomočjo domače internetne povezave."[2]

Poleg odstranjevanja naslovov denarnic pa Epic Cashev blockchain tudi zaščiti zasebnost identitete s tem, da zagotovi, da IP-naslovom ni mogoče slediti. To naredi s pomočjo integracije ***protokola Dandelion++***. ***Protokol Dandelion++*** je izboljšan izvirni ***protokol Dandelion*** in je rezultat nenehnega dela sedmih raziskovalcev za boj proti napadom deanonimizacije na blockchainu. Skozi ***Dandelion++*** so transakcije prenesene k naključnim prepletenim potem ali "kablom" in nato nenadoma razpršene po velikem omrežju vozlišč kot stroki regrata, ki jih odpihne iz stebla (slika 1). Tako je transakcijam skoraj nemogoče slediti nazaj k njihovemu izvoru in s tem njihovemu izvirnemu IP-naslovu.

Slika 1: Anonimizacija transakcij s *protokolom Dandelion++.*

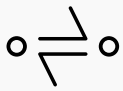
Dandelion++ posreduje sporočila eni od dveh prepletenih poti na 4-regularnemu grafu in jih nato odda z uporabo razpršitve. Na sliki se transakcija širi po modri neprekinjeni poti[3]. Ta postopek omogoči izjemno težko sledenje transakcijam nazaj k njihovemu izvoru, s tem pa se ohranja zasebnost.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network***, 14. marec, 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.***, 2. knj., članek 29, str. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

Zasebnost transakcije



Epic Cashev blockchain zagotavlja zasebnost transakcij s prikrivanjem zneskov in razmerja med pošiljateljem in prejemnikom v transakciji. To se doseže z uporabo znanih idej iz metod ***Confidential Transactions (CT)***[4] in ***CoinJoin***[5], ki so bile v veliki meri razvite s strani Gregoryja Maxwella (Bitcoin Core razvijalec, soustanovitelj in glavni tehnološki uradnik pri Blockstreamu).

CT, ki je bil prvotno ustvarjen s strani Adama Backa in kasneje dodelan s strani Maxwella, deluje tako, da razbije transakcije v manjše delčke s pomočjo homomorfskega šifriranja, kjer ta metoda izvaja izračune na šifriranih informacijah brez predhodnega dešfriranja z namenom, da ohrani zasebnost. Ko so te razdeljene, opazovalci ne morejo videti dejanskih zneskov transakcij zaradi slepih dejavnikov, tj. sistema, ki vrže naključne številke v mešanico transakcijskih fragmentov, da zakrije vrednosti le-teh. Na koncu poznajo vrednost izmenjave samo stranke, med katerimi poteka transakcija, medtem ko je transakcija preverjena s strani omrežja s pomočjo potrditve, da je vsota izhodnih vrednosti enaka vsoti vhodnih vrednosti in vsota izhodnih slepih dejavnikov enaka vsoti vhodnih slepih dejavnikov.

Da bi še bolj zakomplicirali nalogo radovednim očem, so vse Epic Casheve transakcije zakrite s ***CT*** in nato zmešane skupaj z namenom skrivanja povezav med strankami v transakciji. To se naredi s pomočjo druge Maxwellove zasnove, ***CoinJoina***.

Da bi poenostavljeno ponazorili ***CoinJoin***, si lahko predstavljate, da A, B in C pošiljajo Epic do X, Y in Z. Ko to pošljemo skozi ***CoinJoin*** medij, je znano samo to, da A, B in C pošiljajo, X, Y in Z pa sprejemajo, medtem ko transakcijski zneski ostanejo nevidni. Sistem ***CoinJoin*** je temelj Epic Casha s pomočjo One-Way Aggregate Signatures (OWAS), ki združi vse transakcije znotraj bloka v eno samo.

Zasebnost: Povzetek

Epic Cashev blockchain ščiti zasebnost posameznikov in njihovih transakcij z:

- **Odstranjevanjem naslovov denarnic** – identifikatorji lokacij do digitalnih sefov znotraj blockchaina ne obstajajo. Transakcije so zgrajene neposredno med osebama na osnovi od denarnice do denarnice;
- *Zaupnimi transakcijami* - transakcije se razdelijo v več delov in v zbirko le-teh se vpeljejo slepi dejavniki, tako da so vrednosti delov in ostalih transakcijskih parametrov neznani;
- *Protokolom Dandelion++* – zakrije digitalne poti transakcije od IP-naslova pošiljatelja;
- *CoinJoin* – združi transakcije v snope, da zakrinka razmerja med strankami v transakciji.

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

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

III. Fungibilnost

Charlie Lee, ustvarjalec Litecoina, je dejal, da je fungibilnost edina lastnost zdravega denarja (ang. sound money), ki pri Bitcoinu in Litecoinu manjka in tako priznal, da sta zasebnost in fungibilnost naslednje bojišče za ta dva kovanca[6]. Andreas Antonopoulos, ki je eden največjih strokovnjakov za blokchain na svetu, je dejal: "...umazani kovanci so škodljivi. Če odpravite fungibilnost in zasebnost, uničite valuto."[7]

Fungibilnost je lastnost množice blaga ali sredstev, ki zagotavlja, da imajo posamezne enote te množice enake vrednosti in so zamenljive. To loči zgodnje oblike valut od njihovih predhodnih sistemov trgovanja. Brez zaupanja v fungibilnost denarja ta hitro izgubi svojo uporabnost. Kot bo prikazano spodaj, je fungibilnost večine kriptovalut negotova, medtem ko Epic Casheva arhitektura zasebnosti zagotavlja, da je odporna za enake grožnje.

Večini kriptovalut, ki je podobnih Bitcoinu in po naravi obstajajo na transparentnih blockchainih, je možno preverljivo slediti skozi vsako denarnico, v kateri so bile shranjene. Tako zasebne tretje osebe kot tudi vlade nadzorujejo Bitcoinov blockchain na vse bolj prefinjene načine, da bi hitro odkrili kovance, ki so se uporabljali v prejšnjih dejavnostih. To seveda vodi do skrbi, da bi lahko umazani kovanci nekega dne bili prepovedani za transakcije, kar bi njihovim poznejšim dobrovernim imetnikom povzročilo izgubo.

U.S. Office of Foreign Asset Control (OFAC) je 19. marca 2018 oznanil, da je premišljeval o tem, da bi vključil naslove digitalnih valut na seznam z imenom Specially Designated Nationals (SDN-ji), ki so entitete, s katerimi je osebam ali podjetjem iz ZDA prepovedano poslovati. Še bolj skrb vzbujajoče je to, da OFAC ni izključila možnosti vključitve naslovov, ki trenutno držijo umazane kovance, na seznam SDN, kar bi dejansko uvrstilo nedolžne imetnike umazanih kriptovalut na kriminlno črno listo zaradi povezave z imetjem umazanih kovancev. To je vodilo do tega, da je profesor prava iz Univerze v New Yorku zbadljivo dejal: "poslovite se od fungibilnosti", in še nato dejal, da naj javnost pričakuje "premijo na sveže skovane kovance ali izsledene čiste kovance..."[8].

S tem razvojem v mislih si ni težko predstavljati preobrata na kripto trgu in trpljenje ali celo izumrtje veliko dobro uveljavljenih kriptovalut. Vendar pa je Epic ena od redkih kriptovalut, ki se popolnoma izognejo temu problemu zaradi močnih funkcij zasebnosti, ki so bile prej že predstavljene v tej knjigi. Z odstranitvijo povezave med identiteto in lastništvom in razmerja med strankami v transakciji, Epic nikoli ne more biti povezan z osebo ali dejavnostjo. Kot taka, ostane vrednost Epica neodvisna od svojih uporabnikov in zagotavlja visoko stopnjo zasebnosti in varnosti, s katerima zlonamerni akterji ne morejo preprosto manipulirati na kriminalnem, finančnem ali političnem prizorišču.

> **“...UMAZANI KOVANCI SO ŠKODLJIVI. ČE ODPRAVITE FUNGIBILNOST IN ZASEBNOST, UNIČITE VALUTO.”**
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29. januar, 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. april, 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. marec, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Razširljivost

Epic Cash je MimbleWimble implementacija blockchaina, ki izkorišča napredek v razširljivosti kot rezultat prostorsko učinkovitega dizajna, ki se znebi odvečnih transakcijskih podatkov. Funkcionalnost "cut-through", ki je odgovorna za to, zagotovi, da blockchain sčasoma postane bolj prostorsko učinkovit za razliko od ostalih kriptovalut, kot je Bitcoin, in da so lahko nova vozlišča ustvarjena z minimalnimi investicijami v pomnilnik in računalniško zmogljivost. S tem da ostaja prostorsko učinkovit, je zmožen imeti široko razpršeno omrežje in spodbujati decentralizacijo. Poleg tega so vozlišča Epic Casha zmožna prispevati k varnosti omrežja, ki je osnovana na majhni podmnožici blokov, medtem ko mora vsako Bitcoinovo vozlišče hraniti celotno verigo.

Večina kriptovalut zahteva neomejeno shranjevanje vseh transakcijskih podatkov na svojih blockchainih. Bitcoinova veriga trenutno pridobi 0,1353 GB spomina na dan, medtem ko se Ethereumova veriga celo hitreje veča, in sicer z 0,2719 GB na dan. Če bo Bitcoinova veriga nadaljevala rast s trenutno hitrostjo, bo do trenutka, ko bo narudarjen zadnji nagradni blok v letu 2140, sčasoma dosegla velikost, ki znaša približno 6 TB. Ethereum bo presegel 10 TB do tega datuma[9]. V večini blockchainih brez MimbleWimble, morajo biti transakcije preverjene s strani vozlišč po celem svetu. Ko se podatki večajo, se veča tudi breme na vsakem vozlišču. Tudi pri samo 200 GB (približna velikost trenutne Bitcoinove verige) zahteva sinhronizacija podatkov stabilno omrežje in disk z zmožnostjo branja in pisanja z veliko hitrostjo.

Posledično postaja rudarjenje zmeraj bolj centralizirano med velikimi bazeni (ang. pools), kar zahteva drage računalniške vire. **Če bi shranili celotno zgodovino Bitcoinovega blockchaina na Epic Cashevem blockchainu, bi ustrezal skoraj 90% manj prostora.** Manjše je hitrejše zaradi tega, ker vsaka transakcija zahteva manj časa za prenos in varovanje.

MimbleWimble reši dilemo shranjevanja z inovativno metodo obrezovanja blokov, ki ga s tujko imenujemo "cut-through". Da bi razumeli, kako ta deluje, je najbolje najprej pogledati, kako so sestavljene transakcije in bloki znotraj MimbleWimble blockchaina.

Vhodi:

Reference na stare izhode;

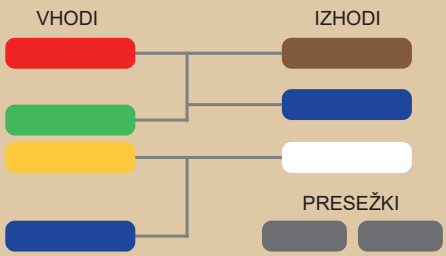
Izhodi:

Izhodi *zaupnih transakcij (Confidential Transactions)* in **rangeproof-i**;

Presežek:

Razlika med izhodi in vhodi skupaj s **podpisi** (za avtentikacijo in dokaz, da ni inflacije).

Slika 2:
Deli transakcije MimbleWimble.



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

Vsi Epic Cashevi bloki vsebujejo:

Merklova drevesa transakcijskih vhodov;

Merklova drevesa transakcijskih izhodov in rangeproof-e;

Seznam presežnih vrednosti in podpise.

Na sliki 2 in 3 iz predstavitve Andrewa Poelstre lahko vidimo nove narudarjene Epice, ki jih predstavljajo bele vhodne celice. Enako obarvane celice predstavljajo izhode s pripadajočimi porabljenimi vhodi. S postopkom "cut-through" so vhodi in ustrezni porabljeni izhodi odstranjeni, da sprostijo prostor znotraj bloka, kar zmanjša količino podatkov, ki mora biti shranjena na blockchainu. Medtem ko so transakcije izpuščene iz glavne knjige, se v ostala presežna jedra (zgolj 100 bajtov) trajno zapiše, da so se transakcije zgodile.

Ko se bloki ustvarjajo, uporabi MimbleWimle "cut-through" po blokih, tako da na dolgi rok ostanejo samo glave blokov (približno 250 bajtov), neporabljene transakcije in transakcijska jedra (približno 100 bajtov). Grin, ki je druga zagnana implementacija MimbleWimble, je pokazal, da bi imela veriga MimbleWimble s podobnim številom transakcij kot pri Bitcoinovi verigi skoraj 10% velikosti Bitcoinove verige. Poleg tega bo velikost vozlišča "nekaj GB za verigo z velikostjo Bitcoina in potencialno optimizirana na nekaj sto megabajtov".[12]

To nasprotuje Bitcoinu, kjer mora biti celoten blockchain shranjen na vsakem vozlišču. Ko se bo ščasoma prostorska učinkovitost Epic Cashevega blockchaina povečala glede na Bitcoinov blockchain, se bodo tudi stroškovne učinkovitosti glede na sodelovanje vozlišč v omrežju Epic Cash. Nižje ovire za sodelovanje pomagajo zagotavljati ključno odpornost na sloju vozlišč dizajna omrežja.

S pomočjo implementacije MimbleWimble in uporabe obrezovanja verige s "cut-through" postopkom ponuja Epic Cashev blockchain razširljivost na način, ki je pogosto spregledan s strani skupnosti za kriptovalute. To je tisti, ki zajame bistvo Bitcoina in podobnih projektov: decentralizacija. Ne glede na to, koliko transakcij na sekundo je kovanec zmožen predelati se je treba vprašati, zakaj je to dobro, če ne more biti vzdrževano s strani širokega in raznolikega omrežja? Če so spominske zahteve takšne, da validacija na koncu gravitira proti močnim konglomeratom rudarjenja, so potem vsi napori skupnosti za kriptovalute za ustvarjanje decentraliziranega ekosistema zaman. Za zagotavljanje dodatne prepustnosti je načrtovana implementacija v Lightning slogu za 2. sloj kot kratkoročni cilj v načrtu dela Epic Cashevega razvoja.

Slika 3: MimbleWimble transakcije pred in po "cut-through".

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

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

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

V. Denarna politika

Denarni politiki Epic Casha in Bitcoina sta zelo podobni. Epic Casheva zaloga v obtoku se najprej hitro razširi in nato sinhronizira z zalogo Bitcoina v obtoku leta 2028. Zatem se povečuje z upadajočo hitrostjo, dokler ne doseže maksimalne zaloge 21 milijonov Epicov v letu 2140. Epic Cash ima značilnosti, da postane varna shramba dolgoročne vrednosti, ker je zaloga v obtoku znana na vsaki točki skupaj s svojim življenjskim ciklom emisij in ker doseže višek v fiksni maksimalni zalogi. Za denarno politiko Epic Casha so značilne naslednje štiri funkcije:

- Hitra emisija v prvih devetih letih življenjske dobe, v katerih bo ustvarjenih 20,343,750 Epicov (96,875% skupne zaloge). Točne hitrosti emisij so prikazane v poglavju urnika emisij v tej knjigi;
- Leta 2140 bo dosežena maksimalna zaloga 21 milijonov Epicov, in sicer v približno istem obdobju, ko bo Bitcoin dosegel maksimalno zalogo 21 milijonov enot;
- Zaloga v obtoku Epicov in hitrost emisij se sinhronizirata s tistimi od Bitcoina v Epic Singularity, okoli 24. maja 2028. Po singularnosti se bo hitrost emisij zmeraj bolj povečevala, zaloga v obtoku pa zmeraj bolj zmanjševala;
- Epic ima strukturo deljivosti z 8 decimalkami, tako da je 1 Epic enak 100,000,000 freemanom (kot je 1 Bitcoin enak 100,000,000 satoshijem).

Epic Casheva denarna politika je povzeta po Bitcoinovi zaradi naslednjih razlogov:

- Strinjanje z ekonomskimi temelji Bitcoina, in sicer s tem, da pomanjkanje in predvidljivost zaloge v obtoku tvorita osnovo za njegove močne lastnosti shranjevanja vrednosti;
- Javnost je že seznanjena z modelom Bitcoina in njegovimi dokazanimi rezultati v zadnjih desetih letih od njegovega nastanka. S tem da se približno sinhronizira z zalogo v obtoku Bitcoina in posnema maksimalno zalogo Bitcoina ter strukturo deljivosti, gre Epic po poti s čim manj odpora proti množičnemu sprejetju.

VI. Urnik emisij

Epic Cash ima skupno 33 obdobij rudarjenja, vsaka pa je definirana z zmanjševanjem nagrad blokov glede na predhodno obdobje. Epic Genesis, datum na katerega je bil narudarjen 1. blok, se je zgodil avgusta 2019. V eni minuti se narudari en blok. Prvih pet obdobij pridela skoraj 97% maksimalne zaloge Epica, kar ustreza 20 letom emisij Bitcoina v približno devetih letih. To je mogoče obravnavati kot priložnost, da "zavrtimo čas nazaj" za tiste, ki so zamudili spektakularno rast Bitcoina.

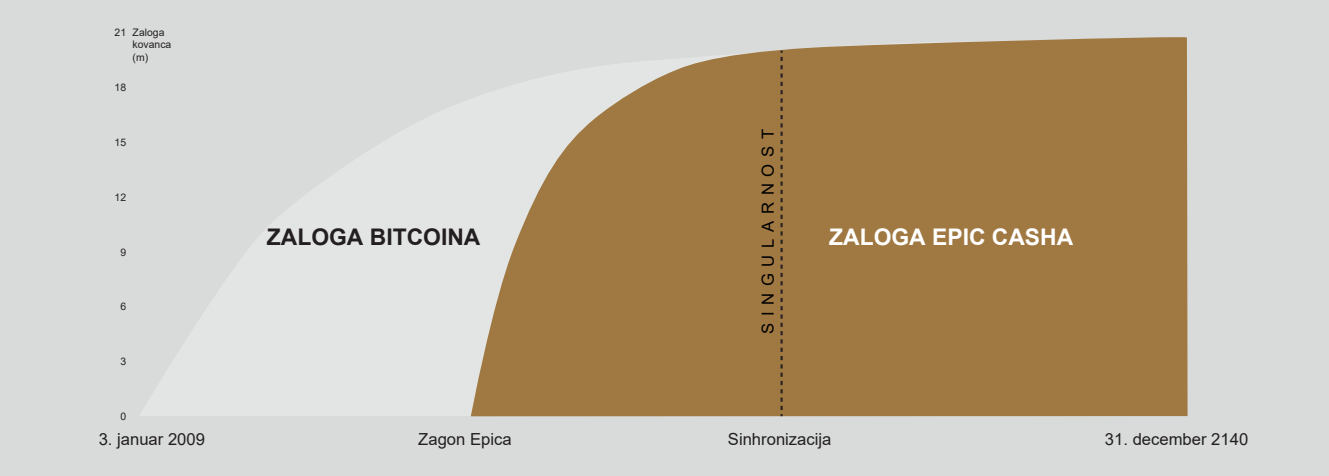
Urnik emisij v tabeli 1 prikazuje začetne in končne datume prvih sedem obdobij rudarjenja, njihove ustrezne nagrade blokov in zaloge v obtoku za vsako obdobje. Obdobij od 8 do 33 ni vključenih v tabeli zaradi jedrnatosti. Za ta obdobja je zadostno razumeti, da bo imelo vsako poznejše obdobje nagrado bloka, ki bo enaka polovici količine nagrade predhodnega obdobja, kot je to pri Bitcoinu. Količina izpuščenega Epica med vsakim od teh obdobij bo vsota nagrad blokov znotraj 4-letnega obdobja (približno 1460 dni).

V Epic Singularity (2028) se Epicova zaloga v obtoku sreča z zalogo v obtoku Bitcoina in na tej točki Epic Cash prevzame Bitcoinov vzorec nagrad blokov in prepolovitve, kjer se nagrade blokov zmanjšajo za polovico na vsake štiri leta. Edina izjema je ta, da se rudarjenje Epicovih blokov nadaljuje s hitrostjo enega bloka na minuto v kontrastu z Bitcoinovo hitrostjo enega bloka na vsakih deset minut. S tem bo zaloga v obtoku Epica ohranila približno pariteto z zalogo v obtoku Bitcoina za preostanek njunega obstoja.

Tabela 1: Urnik emisij za prvih sedem obdobij rudarjenja. Datumi so približki.

Obdobje	1	2	3	4	5	SINGULARNOST	6	7
Nagrada bloka	16	8	4	2	1		0,15625	0,078125
Začetni datum	1. avgust 2019	29. junij 2020	11. oktober 2021	3. junij 2023	10. avgust 2025		24. maj 2028	22. maj 2032
Končni datum	29. junij 2020	11. oktober 2021	3. junij 2023	10. avgust 2025	24. maj 2028		22. maj 2032	20. maj 2036
Dolžina (v dnevih)	334	470	601	800	1019		1460	1460
Začetna zaloga	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Končna zaloga	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% maksimalne zaloge	36,6%	62,4%	78.,%	89,9%	96,9%		98,4%	99,2%

Slika 4: Urnik emisij Epica in Bitcoina



VII. Rudarjenje

Epic Cashev blockchain sledi decentralizaciji s tem, da sprejema široko paleto računalniške strojne opreme. Rudarjenje Epica je prvotno na voljo procesorjem, grafičnim karticam in ASIC-om z uporabo treh algoritmov zgoščevanja, in sicer RandomX, ProgPow, and CuckAToo31+. Algoritme se lahko hitro trivialno zamenja brez ogrožanja integritete verige.

1 RandomX in procesorji

RandomX je "Proof-of-Work" (PoW) algoritem, ki je optimiziran za splošno-namenske procesorje. Uporablja naključne izvršitve programa z več tehnikami "memory-hard" za doseganje naslednjih ciljev:

- Preprečitev razvoja ASIC-ev z enim čipom;
- Minimizacija prednosti učinkovitosti specializirane strojne opreme pred splošno-namenskimi procesorji.

Rudarjenje Epica s procesorji zahteva povezano alokacijo 2 GB fizičnega pomnilnika (RAM), 16 KB predpomnilnika L1, 256 KB predpomnilnika L2 in 2 MB predpomnilnika L3 na nit za rudarjenje. Naprave z Windows 10 zahtevajo 8 GB pomnilnika ali več. Ni neverjetno, da bi nekega dne v ne tako oddaljeni prihodnosti mobilni telefoni postali uspešno delujoča vozlišča za rudarjenje. Zgodnja integracija procesorjev v Epic Cashevemu omrežju rudarjenja je odlična priložnost za veliko ljudi, ki posedujejo le skromne računalniške vire, da zaslužijo nagrade blokov in pomagajo varovati omrežje Epic Casha.

2 ProgPow in grafične kartice

Programmatic Proof-of-Work (ProgPow) je algoritem, ki je odvisen od pasovne širine pomnilnika in izračunov jedra za naključna matematična zaporedja, ki izkoristi prednosti računskih lastnosti veliko grafičnih kartic in s tem učinkovito zajame skupen strošek energije strojne opreme. Ker je ProgPow specifično osnovan za izkoriščanje prednosti proizvodnih grafičnih kratic, je hkrati težko in drago doseči znatno večje učinkovitosti skozi specializirano strojno opremo. Tako algoritem ProgPow ublaži spodbudo za večje ASIC bazene za izpodrivanje grafičnih kartic, kot je to pogosto pri veliko drugih PoW algoritmih, naprimer pri Bitcoinovemu SHA-256. Grafične kartice, ki sicer niso tako prevladujoče kot procesorji, so še vedno brez težav na voljo. S tehnološkim razvojem, ki ga vodita gonilni sili Nvidia in AMD, so grafične kartice sposobne vzporedne obdelave veliko več rešitev pri rudarjenju na enoto za razliko od procesorjev. To je zaradi kombinacije vsenavzočnosti in visoke procesorske moči, ki ju bodo grafične kartice zagotovile kot hrbtenico za večino rudarske dejavnosti med začetnimi obdobji, kot je to prikazano v tabeli 2.

3 CuckAToo+31 in ASIC-i

CuckAToo31+ je ASIC-u prijazna permutacija algoritma Cuckoo Cycle, ki je bila razvita s strani nizozemskega računalničarja, Johna Trompa. CuckAToo31+, ki je soroden na ASIC odpornemu CuckARoo29, generira naključne bipartitne grafe in rudarjem predstavi nalogo iskanja zanke z dano dolžino "N", ko se sprehajajo skozi točke tega grafa.

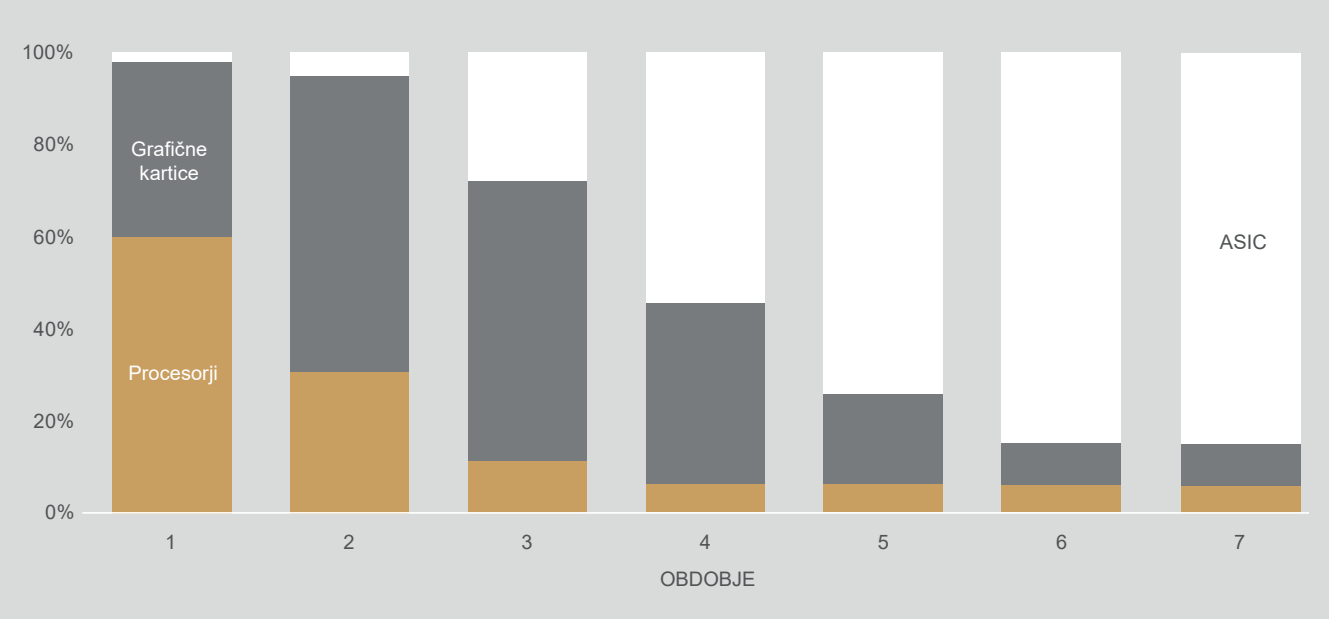
[13] Tevador, ***RandomX***, 28. marec 2019, https://github.com/tevador/RandomX

To je opravilo, ki je vezano na pomnilnik, kar pomeni, da je čas rešitve vezan na pasovno širino pomnilnika namesto na surovo hitrost procesorja ali grafične kartice. Kot rezultat proizvede algoritem Cuckoo Cycle manj toplote in potroši precej manj energije kot tradicionalni PoW algoritmi. ASIC-u prijazen CuckAtoo31+ omogoča izboljšanje učinkovitosti glede na grafične kartice z uporabo na stotine megabajtov pomnilnika SRAM, medtem ko ostane pod blokado pomnilnika I/O[14]. Na koncu ponujajo ASIC-i najboljše potencialne ekonomije obsega treh možnosti rudarjenja. V interesu vključenosti pa kljub temu da jim je od samega začetka dodeljen majhen del nagrad rudarjenja glede na procesorje in grafične kartice, ASIC-i prevzamejo večinski delež narudarjenih nagrad blokov ob predpostavki, da bo obstajal konkurenčni ekosistem proizvajalcev naprav za CuckATOo31+.

Tabela 2: Dodelitve nagrad rudarjenja. Predmet za revizijo. Dodelitve bodo usmerjenje k doseganju maksimalne decentralizacije in konsistence z dolgoročnimi interesi omrežja.

Obdobje	1	2	3	4	5	6	7
Dnevi	334	470	601	800	1019	1460	1460
Procesorji	60%	30%	10%	5%	5%	5%	5%
Grafične kartice	38%	65%	62%	40%	20%	10%	10%
ASIC-i	2%	5%	28%	55%	75%	85%	85%

Slika 5: Dodelitve nagrad rudarjenja za vsako obdobje glede na tabelo 2. Predmet za revizijo.



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

4 Prispevki za rudarjenje

Z začetkom pri Epic Genesis (2019) in koncem pri Epic Singularity (2028) je med postopkom rudarjenja alokacija Epica usmerjena proti EPIC Blockchain Foundation, tako kot so prispevki za rudarjenje.

EPIC Blockchain Foundation se posveča tehničnemu razvoju in promociji ozaveščenosti ter uporabnosti projekta Epic Cash v zgodnjih letih njegovega začetka z ustvarjanjem tržnih dejavnosti in razvijanjem partnerstev znotraj finančne tehnološke industrije.

Po singularnosti bo vlogo EPIC Foundation prevzela EPIC Distributed Autonomous Corporation (EDAC), ki bo razvita s strani fundacije pred predajo.

EPIC Blockchain Foundation financira odstotek nagrad rudarjenja, ki so odštete od nagrad blokov glede na naslednje letne stopnje:

Tabela 3: Letne stopnje za prispevke za rudarjenje fundacije kot odstotek nagrad rudarjenja.

Leto	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% nagrad rudarjenja	8,88 %	7,77 %	6,66 %	5,55 %	4,44 %	3,33 %	2,22 %	1,11 %	1,11 %	0 %

VIII. Zaključek

Epic namerava biti priznan kot "decentralizirano digitalno srebro", torej podoben medij izmenjave pri priznanem položaju Bitcoina kot decentraliziranega digitalnega zlata. S ponovnim uvajanjem izgubljene fungibilnosti na veliko bolj energijsko učinkoviti in ekološko prijazni hrbtenici strojne opreme, prevesi Epic Cash tehtnico moči nazaj do posameznih uporabnikov, kar je v velikem nasprotju z nedavnim trendom centralizacije. To je kombinacija ekonomije Bitcoina, teorije iger in dokazane "proof-of-work" formule z najboljšimi rezultati moderne blockchain tehnologije v nespremenljivi in decentralizirani valuti (Epic) brez potrebe po zaupanju, ki je razširljiva in fungibilna ter ščiti zasebnost svojih uporabnikov. Epic Cashev blockchain je odprt, javen, brez meja in odporen proti cenzuri. Ohranja zasebnost in premoženje svojih uporabnikov in nagrajuje tiste, ki posodijo svojo strojno opremo za podporo omrežju s pomočjo rudarjenja. Vsak Epic je narudarjen v obstoj skozi "proof-of-work". Zaloga se začne pri ničli, za omrežje pa velja, da ima pošten zagon s funkcionalnim testnet-om, ki trenutno teče.

Ključna dejstva Epic Casha:

- **Rudarjenje se je začelo avgusta 2019.**
- **Epic Cashev blockchain je osnovan na**

  MimbleWimble. Bistvene značilnosti protokola so:

  1. **Cut-through** – odstranitev odvečnih informacij iz blockchaina za promocijo prostorske učinkovitosti, spodbujanje sodelovanja širokega obsega, validacije omrežja in decentralizacije stevarda;
  2. ***CoinJoin*** – združevanje transakcij znotraj bloka za zagotavljanje fungibilnosti kriptovalute Epic;
  3. ***Protokol Dandelion++*** – širjenje transakcij s pomočjo komunikacije med prepletenimi kanali in razprševanja po širokem omrežju vozlišč, kar pretrga povezave med transakcijami in njihovimi izvori;
  4. **Brez naslovov denarnic** – uporaba velikega multipodpisa za generiranje zasebnih ključev za enkratno uporabo za stranke v transakciji, kar popolnoma odstrani potrebo po naslovih denarnic.

- **Epic Casheva denarna politika** je zasnovana tako, da sinhronizira zalogo v obtoku Epica z Bitcoinovo zalogo v obtoku v približno devetih letih in doseže enako maksimalno zalogo 21 milijonov enot v istem času kot Bitcoin, in sicer v letu 2140. Ta padajoča inflacijska politika jamči transparentnost, predvidljivost zaloge in pomanjkanje, kar goji varnost dolgoročnega skladiščenja vrednosti.

- **Rudarjenje**, ki vključuje procesorje, grafične kartice in ASIC-e z ustreznimi algoritmi RandomX, ProgPow in CuckAToo31 za lajšanje množičnega sprejetja in efikasnosti omrežja.

IX. Tehnične specifikacije

Ime projekta: Epic Cash
Ime valute: Epic
Čas bloka: 60 sekund
Velikost bloka: 1 MB
Začetna zaloga: 0
Končna zaloga: 21,000,000
Blok geneze: avgust 2019
Konsenz: RandomX (procesorji), ProgPow (grafične kartice) in CuckAToo31+ (ASIC-i)

Povezave:

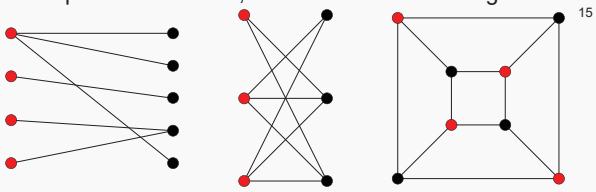
www.epic.tech

t.me/EpicCash – Telegram

X. Slovarček

ASIC Application Specific Integrated Circuits so vezja, ki so oblikovana za en sam namen.

Bipartitni graf množica točk grafov, ki razpade v dve nepovezani množici, tako da si niti dve točki grafa znotraj iste množice nista sosedni.



Slepi dejavnik naključni element, ki je vpeljan v digitalno sporočilo za lajšanje šifriranja; deljena skrivnost med dvema strankama, ki šifrira vhode in izhode v tej specifični transakciji in prav tako javne in zasebne ključe strank v transakciji[16].

Nagrada bloka novi Epici, ki so distribuirani s strani omrežja kot nagrade za opravljene izračune za preverjanje transakcij znotraj novega bloka.

Predpomnilnik komponenta strojne ali programske opreme, ki hrani podatke, da so lahko prihodne zahteve za te podatke hitreje na voljo.

Zaloga v obtoku količina Epica v obstoju na dani točki v času.

Procesor (CPU) Central Processing Unit: računalniška komponenta, ki je odgovorna za interpretacijo in izvrševanje večine ukazov iz strojne ali programske opreme računalnika.

Cut-through postopek **MimbleWimble** blockchaina, kjer so vhodi in ustrezni porabljeni izhodi odstranjeni za sproščanje prostora znotraj bloka, kar zmanjša količino podatkov, ki jih je potrebno shraniti na blockchainu.

Decentralizacija stanje disperzije operacij in upravljanja omrežja.

Emisija ustvarjanje novih Epicov, zasluženih s strani rudarjev v nagradah blokov. Epic je ustvarjen na vsakih 60 sekund, ko so transakcije potrjene na blockchainu.

Epic singularity ali singularnost točka v času, ko se Epicova zaloga v obtoku sinhronizira z Bitcoinovo zalogo v obtoku (maj 2028).

Presežek (MimbleWimble) razlika med izhodi in vhodi skupaj s podpisi (za avtentikacijo in dokazovanje, da inflacija ne obstaja).

Fungibilnost lastnost blaga ali surovine, kjer so posamezne enote pravzaprav zamenljive in je vsak od delov različen od drugih delov.

Genesis ali geneza (dogodek) rudarjenje prvega Epic bloka in uradno spočetje blockchaina.

Grafična kartica (GPU) Graphics Processing Unit: enota, ki vsebuje programabilni logični čip (procesor), specializiran za funkcijo prikazovanja. Potrošniške grafične kartice so lahko zelo primerne za rudarjenje kriptovalut.

Prepolovitev (za Bitcoin) se zgodi na vsake 4 leta. Hitrost zaloge se zmanjša za 50% po vsakem dogodku prepolovitve.

Hash vrednost, ki je izračunana iz osnovne vhodne številke z uporabo funkcije zgoščevanja.

Algoritem zgoščevanja (funkcija) matematični algoritem, ki določa podatke poljubne velikosti hash-u fiksne velikosti, ki se uporablja za generiranje in preverjanje digitalnih podpisov, kod za avtentikacijo sporočil (MAC-i) in ostalih oblik avtentikacije.

Homomorfsko šifriranje metoda, s katero se izvajajo izračuni na šifriranih informacijah brez predhodnega dešifriranja. (v programerstvu) stanje, v katerem objekt ne more biti spremenjen po svoji stvaritvi.

Nespremenljivost

Vhod (MimbleWimble) komponenta MimbleWimle transakcije, ki predstavlja pošiljajočo stranko transakcije; ustvarjena iz izhodov prejšnjih transakcij.

I/O input/output ali vhod/izhod; komunikacija med informacijskim procesnim sistemom, kot je računalnik, in zunanjim svetom, po možnosti človekom ali drugim informacijskim procesnim sistemom.

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

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

Maksimalna zaloga	količina Epica, ki bo dosežena in na tej točki se zaloga v obtoku ne bo več povečevala (21,000,000 Epicov).
Memory-hard	velika poraba pomnilnika (RAM) za onemogočanje poskusov vzporednega izvajanja hkratnih povezav. "Memory-hard" funkcije so algoritmi, ki imajo čase računanja primarno jasne s strani razpoložljivega pomnilnika za držanje podatkov. Poznane tudi kot "memory-bound" funkcije.
Merklovo drevo	podatkovna struktura, ki se uporablja v računalniških aplikacijah. Merklova drevesa v blockchainu omogočajo učinkovito in varno preverjanje vsebine velikih podatkovnih struktur.
MimbleWimble	protokol, ki ga je zasnoval prispevatelj pod psevdonimom, znan le pod imenom Tom Elvis Jedusor v Bitcoinovi klepetalnici za razvijalce.
Multipodpis	digitalna shema podpisov, ki omogoča skupini uporabnikov, da podpišejo en sam dokument. Ponavadi proizvede algoritem multipodpisa skupen podpis, ki je bolj zgoščen kot zbirka različnih podpisov od vseh uporabnikov[17].
Vozlišče	računalnik, ki se poveže na blockchain omrežje in se razveji do ostalih vozlišč znotraj omrežja za distribucijo informacij o transakcijah in blokih, in sicer na način, ki ga imenujemo "peer-to-peer".
One Way Aggregate Signature (OWAS)	enosmerni agregatni podpis je podpis transakcije, ki je sestavljen iz veliko podpisov, ki so šifrirani na način, da je zelo težko izračunati posamezne podpise, ki so del celote.
Izhod (MimbleWimble)	komponenta MimbleWimble transakcije, ki predstavlja recept transakcije; uporaba za vhode za naslednje transakcije.
Pedersenova shema za zapriseganje	primitivna kriptografija, ki omogoča dokazovalniku (ang. prover), da se zaveže izbrani vrednosti brez odkrivanja kakršnekoli informacije o njej in brez tega, da bi bil zmožen to zaprisego razveljaviti.
Zasebni ključ	zasebni ključ je majhen delček kode v paru z javnim ključem, ki pripravi algoritme za šifriranje in dešifriranje besedila. Ustvarjen je kot del kriptografije javnega ključa med šifriranjem asimetričnega ključa in uporabljen za dešifriranje in preoblikovanje sporočila v obliko za branje.
Proof-of-Work (PoW)	dokaz o delu je del podatkov, ki ga je težko (drago in časovno potratno) proizvesti, vendar preprosto preveriti s strani drugih in ki zadošča določenim zahtevam. Dokazi o delu so pogosto uporabljeni pri generiranju blokov kriptovalut.
Javni ključ	javni ključ je ustvarjen v kriptografiji šifriranja javnega ključa, ki uporablja algoritme šifriranja asimetričnega ključa. Javni ključi so uporabljeni za predelavo sporočila v neberljivo obliko.
RAM (Random Access Memory)	čip za hitri dostop do shranjenih podatkov v računalniški napravi, ki vsebuje operacijski sistem (OS), aplikacijske programe in trenutne podatke v uporabi, da do njih lahko procesor naprave hitro dostopa.
Rangeproof	validacija za zapriseganje, ki preveri, da so vhodi transakcije večji kot vsota izhodov transakcije in da so vse vrednosti transakcij pozitivne. Rangeproof-i zagotovijo, da denarna zaloga ni bila zlorabljena.
(Digitalni) podpis	standarden del protokola blockchain, ki se v glavnem uporablja za zaščito transakcij in blokov transakcij, prenašanje informacij, upravljanje s pogodbami in ostale primere, kjer je pomembno odkrivanje in preprečevanje kakršnekoli zunanje zlorabe. Zagotavljajo tri prednosti shranjevanja in prenašanja informacij na blockchainu: • odkrijejo zlorabljene podatke, ki se pošiljajo; • preverijo sodelovanje določene stranke v transakciji; • so lahko pravno zavezujoči.
SRAM (Static Random Access Memory)	Random Access Memory (RAM), ki hrani delčke podatkov v svojem pomnilniku, dokler ga napajamo.
Prepustnost	merjenje transakcij na sekundo, ki jih lahko opravi dani protokol kriptovalute.
Brez potrebe po zaupanju	kakovost omrežja kriptovalute za upoštevanje pravil protokola brez izvrševanja centralne stranke.

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA,*** Zapiski iz predavanj iz računalništva, knj. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH