Pamilya ni Freeman

Hulyo 4, 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

Isang Peer-to-Peer Electronic Cash na System

PAGIIMBAK NG HALAGA + KAGAMITAN SA PAGPAPALITAN + BATAYAN NG BILANG

1.7 na bilyong katao ang hindi na kakagamit ng pandaigdigang pampinansyal na sistema, habang ang ibang 1.3 na bilyon ay hindi naseserbisyohan. Ang potensyal ng tao dito ay binuksan ng Epic Cash sa pamamagitan ng pagkonekta ng mga indibiwal sa pandaigdigang merkado. Mabilis, libreng magagamit, at bukas para sa lahat.

Version 7.1b

Mga Nilalaman

I. Abstrak	4
II. Pagkapribado	5
III. Fungibility	8
IV. Nasusukat	9
V. Patakarang Pang-salapi	11
VI. Takdang Paglabas	12
VII. Pagmimina	13
VIII. Konklusyon	16
IX. Teknikal na mga Detalye	17
X. Talahulunganan	18

I. Abstrak

Ang Epic Cash ay ang hulihang bahagi sa paglalakbay patungo sa totoong P2P internet cash, ang pundasyon ng isang pribadong pampinansyal na sistema. Nilalayon ng Epic Cash na maging pinaka-epektibong paraan ng pagprotekta sa pagkapribado ng mundo sa digital na pera. Upang maipatupad ang layuning iyon, dapat na magawa nito ang tatlong pangunahing mga pagpapa-andar sa pera:

1. **Pagiimbak ng Halaga** – maaaring mai-salba, maibabalik, at mapalitan sa kahit anong oras, at ng mahuhulaan ang halaga kapag naibalik;
2. **Kagamitan sa Palitan** – anumang bagay na natanggap na kumakatawan sa isang pamantayan ng halaga at napapalitan para sa mga kalakal o serbisyo;
3. **Batayan ng Bilang** – ang bilang na kung saan ang halaga ng isang bagay ay isinasaalang-alang at inihambing.

	$ USD	BTC	EPIC
Pagiimbak ng Halaga	✗	✓	✓
Kagamitan sa Palitan	✓	✗	✓
Batayan ng Bilang	✓	✗	✓

Noong 2009 lumabas ang Bitcoin bilang unang blockchain na nakabase sa digital na pananalapi, at kasama nito ang tatlong mga katangian kontra sa pagsuri sa ibang cryptocurrencies:

- **Mapagkakatiwalaan** – walang sinuman ang kinakailangan na magtiwala sa anumang sentralisadong entidad o katapat na pagkilos upang gumana ang network;
- **Hindi Nababago** – ang mga transaksyon ay hindi naibabalik
  a. Ito ay dapat na lubos na hindi maisasagawa o mahirap na muling isulat ang kasaysayan;
  b. Imposible sa kunsinuman na malipat ang pondo maliban sa may-ari ng private key;
  c. Ang lahat ng transakyon ay nakatala sa blockchain
- **Desentralisasyon** – "Ang Blockchain ay desentralisado (walang kumokontrol sa kanila) at arkitektura na desentralisado (walang punto ng imprastruktura na pagkabigo)..."[1].

Sinimulan ng Bitcoin ang mga bagong daang teknolohikal habang sinusunod ang mga nasusukat na pundasyon sa oras sa istraktura ng patakaran sa pananalapi nito. Ang tagumpay ng Bitcoin ay mahigpit na nauugnay sa limitadong supply nito na sinamahan ng mapagkakatiwalaan, hindi mababago, at desentralisadong blockchain. Sinusuportahan ng Epic Cash ang patakaran sa pananalapi ng Bitcoin ng pagbawas ng inflation at limitadong supply upang matiyak na ang pananalapi ng Epic ay maaaring magsilbing isang epektibong pagiimbak ng halaga.

Sa kabila ng tagumpay ng Bitcoin, ang ilang mga pagkukulang ay ipinahayag mula nang ito ay nag-umpisa 10 taon na ang nakakaraan. Sinubukan ng iba pang mga proyekto na malampasan ang mga pagkukulang na ito at sinisiyasat namin ang pinakamahusay sa mga ito upang magamit bilang panimulang punto. Napagpasyahan namin na magamit ang Grin codebase at ang mahusay na gawain ng iba pang mga proyekto upang matulungan kami na lubos na mapagtagumpayang magawa at matuklasan ang mga pagkakamali ng mga nauna sa Epic Cash. Ang Epic Cash ay nagtataglay ng mga pangunahing katangian upang maging isang mainam na pananalapi:

- **Fungibility** – Ang halaga ng isang bilang ng Epic ay dapat na palaging pantay-pantay sa ibang bilang ng Epic, tulad ng isang Yen o Yuan ay palaging magkatumbas at maaaring mapalitan sa ibang Yen o Yuan. Ang pagkamit sa pagpapalitan ay malaking bahagi sa pagpapagalaw ng pagkapribado.
- **Nasusukat** – Pinapanatili ng Epic Cash ang isang mahusay na blockchain, kung saan ang mga bagong node ay madaling naitatatag na hindi gumagamit ng kagamitan. Ang Epic Cash blockchain ay hindi bababa sa dalawang beses sa kapasidad ng Bitcoin.
- **Pagkapribado** – Ang blockchain ng Epic Cash ay pinoprotektahan ang pagkapribado sa mga may hawak ng Epic at mga gumagamit sa pamamagitan ng pagprotekta sa mga detalye ng mga transaksyon mula sa mga ikatlong partido at idinisenyo upang maging hindi matatahak at hindi nakikita sa pagsubaybay.
- **Mabilis** – Ang mga transaksyon ng Epic Cash ay swabe, tuluy-tuloy at isinasagawa nang mas mabilis kaysa sa mga nakaraang henerasyon ng teknolohiya ng blockchain. Habang ang Bitcoin ay nangangailangan ng anim na 10-minutong mga blocks upang makamit ang kumpletong kumpirmasyon sa transaksyon, ang mga transaksyon sa Epic ay magaganap sa loob ng isang kumpirmadong block sa sandaling ang isang 1 minutong block ay namina.

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

II. Pagkapribado

Ang mordernong paggamit ng pananalapi ay mauunawaan tulad ng kolektibong pagsasalin ng mga bilang ng account sa pagitan ng mga tao at mga institusyon. Ang lugar ng pananalapi sa anumang naibigay na oras ay maaaring mai-map sa pamamagitan ng pagsagot sa mga sumusunod na katanungan:

1. *Sino ang may hawak nito, at ilang ang hawak nila?*
2. *Kanino siya nakikipagtransaksyon, at magkano ito?*

Para sa mga tradisyunal na pananalapi, at sa katotohanan din ng Bitcoin, masasagot natin ang mga katanungang iyon. Sa paggawa nito, marami ang mabubunyag tungkol sa pamumuhay ng mga tao, tulad ng mga pagkonsumo, pagmamay-ari, at mga transakyon ng katapat. Ang makatarungang na mga konklusyon ay maaaring makuha tungkol sa mga interes at hangarin ng isang indibidwal sa pamamagitan ng pagsubaybay sa mga halaga na inililipat. Kung walang pagkapribado, ang datos ng transaksyon ay maaaring manganib ang impormasyon sa mga kamay ng mga mapanganib na third parties.

Ang nakaraang dekada ng paggamit ng cryptocurrency ay nagpapakita ng pagpapatuloy ng "pagkapribado" sa iba't ibang mga pagpapatupad ng blockchain. Ang sukat ng pagkapribado, dapat isaalang-alang, nasasaklaw mula sa bukas at kilala tungo sa isang dulo hanggang sa hindi ito nakikilala. Habang tumatagal ang pagkapribado, isang mahalagang pundasyon ng cryptocurrency, walang pinagkakatiwalaan, pinanghihinalaan. Tulad ng napatunayan ng tagumpay ng mga serbisyo ng pagsusuri sa blockchain ng Bitcoin, Ang Bitcoin ay matatag ang pagkakakilanlan sa pagtatapos ng spectrum ng pagkapribado. Ang mga gumagamit ay dapat na patuloy na gumawa ng mga hakbang upang matiyak na hindi nila sinasadyang gumagawa ng transakyon sa masungit na halaga ng Bitcoin. Ang solusyon ng Epic Cash ay nakatuon patungo sa pagka-anonimo at ibalik ang mahahalagang ari-arian sa pamamagitan ng pagtiyak ng pagkapribado ng indibidwal at pagkapribado ng mga transaksyon ay isinasaayos sa system sa napakahalagang antas.

Pagkapribado ng Pagkakakilanlan

Pagkapribado ng Transaksyon

Pagkapribado ng Pagkakakilanlan

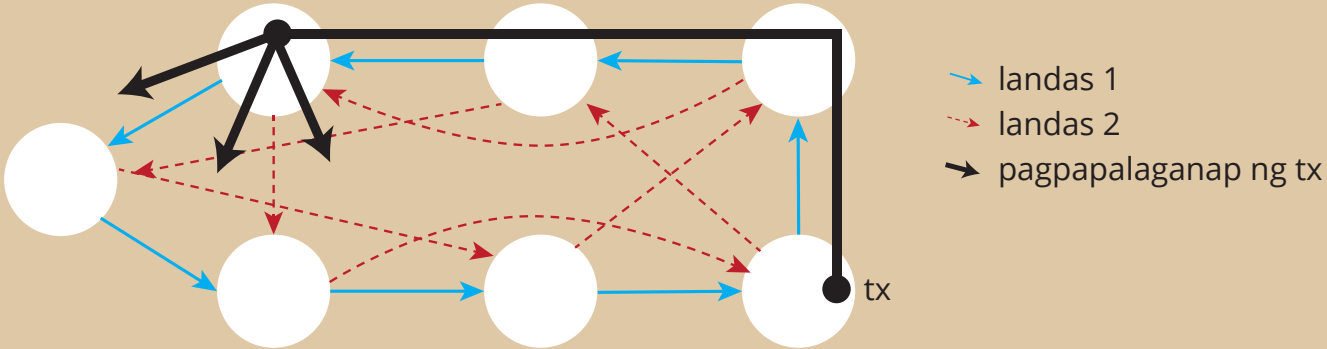
Karamihan sa mga cryptocurrencies tulad ng Bitcoin ay naka-imbak sa mga pitaka na ang mga address ay tumutukoy sa mga public key na nagmula sa mga private key ng isang pitaka. Ang mga address na ito ay maaaring isipin bilang mga tagahanap ng private vault ng digital na mundo. Ang blockchain ng Epic Cash ay tinatanggal ang mga address nang lubusan at sa halip ay inilalapat ang isang grand multi-signature na kung saan ang lahat ng public at private key ay nabuo sa isahangpaggamit.

Dahil ang mga address ng Bitcoin wallet ay tagahanap ng isang vault sa digital na mundo, ang pitaka na iyon ay maaaring masubaybayan sa isang address ng Internet Protocol (IP) ng isang may-ari, na kung saan naka-angkla ang may-ari sa isang computer sa isang natatanging lokasyon sa isang takdang oras. Ipinaliwanag lamang: kapag naganap ang isang transaksiyon sa Bitcoin, ang transaksyon ay naipahayag mula sa isang hub ng komunikasyon na tinatawag na isang 'node' at pagkatapos ay ipinapalaganap sa iba pang mga node na tinatawag na 'peers'. Mabilis na kumakalat ang impormasyong iyon sa bawat isa sa mga kapantay na mga node nang sunud-sunod sa buong network. Ang prosesong ito ay angkop na pinangalanang "Gossip Protocol". Sa madaming salita, ang bawat Bitcoin ay may nakikitang posisyon sa online at isang pisikal na lokasyon kung nasaan ito, o sa halip ang may-ari ng Bitcoin, ay matatagpuan. Tulad ng nabanggit ng mamamahayag na si Grace Caffyn, ang Bitcoin ay "walang lihim kaysa sa Google search mula sa isang koneksyon sa internet sa bahay."[2]

Bilang karagdagan sa pagtatanggal ng mga wallet address, ang blockchain ng Epic Cash ay tinitiyak na ang pagkapribado ng pagkakakilanlan sa pamamagitan ng pagtiyak ay hindi masusubaybayan sa pamamagitan ng IP address. Gagawin ito sa pamamagitan ng pagsasama ng **Dandelion ++ Protocol**. Ang pagpapabuti sa nauna rito, ang orihinal na **Dandelion Protocol**, ang **Dandelion ++ Protocol** ay resulta ng pitong patuloy na gawain ng mga mananaliksik upang labanan ang mga pag-atake ng deanonymization sa blockchain. Sa pamamagitan ng **Dandelion ++**, ang mga transaksyon ay ipinasa sa mga random na intertwined path, o 'mga kable', at pagkatapos ay biglang nagkalat sa isang malaking network ng node, tulad ng mga pods ng isang bulaklak ng Dandelion kapag pinutok mula sa kanilang tangkay (Larawan 1). Gagawin nitong halos imposible na masubaybayan ang mga transaksyon pabalik sa kanilang pinagmulan, at sa gayon din ang pinagmulan ng mga IP address.

Larawan 1: Pag-aanomino ng Transaksyon gamit ang *Dandelion++ Protocol.*

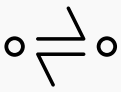
Ang Dandelion ++ ay naghahatid ng mga mensahe sa isa sa dalawang magkakaugnay na mga landas sa isang 4-regular na graph pagkatapos ay naipahayag ang gamit pagkalat. Sa larawan, ang transaksyon ay nagpapalaganap sa asul na solidong landas[3]. Napakahirap ng prosesong ito na masubaybayan ang mga transaksyon pabalik sa kanilang mapagkukunan, sa gayon pinapanatili ang pagkapribado.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 Marso, 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

Pagkapribado ng Transaksyon



Ang blockchain ng Epic Cash ay tinitiyak na ang pagkapribado ng transaksyon sa pamamagitan ng pagkubli ng halaga at ang relasyon ng nagpadala-tatanggap ng isang transaksyon. Ito ay nakamit sa pamamagitan ng aplikasyon ng mga ideya na pamilyar mula sa Confidential Transaction[4] (CT) at CoinJoin[5], mga pamamaraan sa malaking bahagi na binuo ni Gregory Maxwell (developer ng Bitcoin Core, Co-Founder, at CTO ng Blockstream).

Ang CT, na orihinal na nilikha ni Adam Back at kalaunan ay pinino ng Maxwell, ay gumagana sa pamamagitan ng pagsira sa mga transaksyon sa mas maliit na bahagi sa pamamagitan ng homomorphic encryption, isang paraan ng pagsasagawa ng mga kalkulasyon sa naka-encrypt na impormasyon nang hindi nai-decrypt muna upang mapanatili ang pagkapribado. Kapag nahati ito, hindi nakikita ng mga tagamasid ang aktwal na halaga ng mga transaksyon dahil sa mga blinding factors, isang sistema na nagtatapon ng mga random na numero sa halo ng mga fragment ng transaksyon upang maitago ang mga halaga ng mga fragment. Sa huli, ang mga transacting party lamang ang nakakaalam ng halaga ng isang palitan, habang ang transaksyon ay naberipika ng network sa pamamagitan ng kumpirmasyon na ang kabuuan ng mga halaga ng output ay katumbas ng kabuuan ng mga halaga ng pag-input, at ang kabuuan ng mga output ng blinding factors ay katumbas ng kabuuan ng mga input ng blinding factors.

Upang maging higit pang kumplikado ang gawain ng mapagmasid na mata, ang lahat ng mga transaksyon sa Epic Cash ay tinatago sa CT at pagkatapos ay pinagsama-sama upang itago ang mga koneksyon sa pagitan ng mga magkatransaksyon partido. Ito ay gagawin sa pamamagitan ng pangalawang konsepto ni Maxwell, ***CoinJoin***.

Ang simpleng paglalarawan sa ***CoinJoin***, isipin na ang A, B, at C ay nagpapadala ng Epic sa X, Y, at Z, ayon sa pagkakabanggit. Ipinadala sa pamamagitan ng CoinJoin medium, ang lahat ng kilala ay ang A, B, at C ay nagpapadala at ang X, Y, at Z ay tumatanggap, habang ang mga halaga ng transaksyon ay mananatiling hindi nakikita. Ang sistema ng CoinJoin ay pangunahing sa Epic Cash sa pamamagitan ng One-Way Aggregate Signature (OWAS), na pinagsasama ang lahat ng mga transaksyon sa loob ng isang block sa pamamagitan ng isang transaksyon.

Pagkapribado: Buod

Ang blockchain ng Epic Cash ay pinoprotektahan ang pagkapribado ng mga indibidwal at ang kanilang mga transaksyon sa pamamagitan ng:

- **Pag-aalis ng mga wallet address – Twalang lokasyon dito na malalaman sa digital vaults sa loob ng blockchain. Ang mga transaksyon ay ginawa direkta sa tao-sa-tao sa wallet-sa-wallet na batayan.**
- ***Con idential Transactions* – ang mga transaksyon ay hinahati sa maramihang piraso at ipinapakilala ang blinding factors sa koleksyon ng mga pirasong iyon, kaya ang mga halaga ng mga piraso at ang ibang parametro ng transaksyon ay hindi malalaman;**
- ***Dandelion++ Protocol* – tinatakpan ang mga digital na landas ng transaksyon galing sa IP address ng nagpapadala;**
- ***CoinJoin* – pinagsasama-sama ang mga transaksyon sa loob ng mga bundles upang itago ang relasyon sa pagitan ng magkatransaksyon partido.**

[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 Agosto, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. Fungibility

Si Charlie Lee, ang lumikha ng Litecoin, ay naghayag na ang fungibility ay ang tanging katangian ng pananalapi na nawawala mula sa Bitcoin at Litecoin, na inamin na ang pagkapribado at fungibility ay ang susunod na lugar na digmaan para sa mga barya[6]. Si Andreas Antonopoulos, isa sa dalubhasa sa mundo ng blockchain, ay nagsabing ang "... ang mga barya ay nasisira. Kung sinisira mo ang fungibility at pagkapribado, sinisira mo ang pera. "[7]

Ang Fungibility ay ang katangian ng pangkat ng kagamitan o ari-arian na kung saan sinisiguro ang indibidwal na bilang ng pangkat ay katulad na halaga at ito ay napapalitan. Ito ang pagkakaiba sa maagang anyo ng pananalapi galing sa kanilang pinagmulang sistema ng palitan. Kapag walang pagtitiwala sa fungibility ng pera, ang perang iyon ay mabilisang mawawalan ng paggagamitan. Na inilarawan sa ibaba, ang fungibility ng karamihan sa cryptocurrencies ay hindi tiyak, kung saan ang pribadong artkitektura ng Epic Cash ay sinisuguro na hindi tinatablan katulad ng mga panganib na iyon.

Karamihan sa mga cryptocurrencies ay katulad sa Bitcoin, na mayroon na transparent na mga blockchains, na makukumpirma sa pamamagitan ng wallet na tinatago nila. Ang pribadong third parties at gobyerno ay gustong matyagan ang blockchain ng Bitcoin na may mas sopistikadong paraan upang mabilis na makilala ang mga barya na ginamit sa mga nakaraang aktibidad. Ito ay natural na humahantong sa mga alalahanin sa masungit na mga barya ay maaaring balang-araw na ipinagbawal mula sa mga transaksyon, na iniiwan ang sa pagkalagas ag mga mabubuti at mga nagtitiwalang mga tagahawak.

Noong Marso 19, 2018, nag-anunsyo ang U.S. Office of Foreign Asset Control (OFAC) na kinokunsidera bilang nag digital currency addresses sa listahan ng mga Specially Designated Nationals (SDNs), kung saan ang mga tao sa U.S. ay pinagbabawalang magkipagtransaksyon. Mas nakakagambala, ang OFAC ay hindi pinamunuan ang pagsasama ng mga address na kasalukuyang may hawak na mga barya sa listahan ng SDN, na madaling mailalagay ang mga inosente na may-ari ng nabubulok na cryptocurrency sa listahan ng mga kriminal dahil sa pagkakaugnay sa nabubulok na cryptocurrency. Pinangunahan nito ang legal na propesor ng New York University na si Andrew Hinkes, "halikan ang paalam ng fungibility," at dapat asahan ng publiko na "isang premium sa mga bagong barya na naka-print, o sinubaybayan ang mga malinis na mga barya ..."[8]

Sa pagpapaunland ng kaisipan, hindi mahirap isipin ang isang kaguluhan sa merkado ng crypto at ang pagdurusa, o kahit na pagkalipol, ng maraming mahusay na itinatag na mga cryptocurrencies. Gayunpaman, ang Epic ay isa sa ilang mga cryptocurrencies na umiiwas sa problemang ito dahil sa malakas na mga tampok sa pagkapribado na dati nang inilarawan sa papel na ito. Sa pamamagitan ng pag-alis ng link sa pagitan ng pagkakakilanlan at pagmamay-ari, at ang ugnayan sa pagitan ng mga transaksyon na partido, ang Epic ay hindi kailanman maaaring maging kaakibat sa isang tao o isang aktibidad. Dahil dito, ang halaga ng Epic ay nananatiling malaya sa mga gumagamit nito at nagbibigay ng mataas na antas ng pagkapribado at seguridad na hindi madaling baguhin ng mga aktor sa kriminal, pinansiyal, o pampulitikang arena.

> **"...ANG MGA NABUBULOK NA BARYA AY NAKAKASIRA. KUNG SINISIRA MO ANG FUNGIBILITY AT PAGKAPRIBADO, SINISIRA MO ANG PANANALAPI"**
>
> **ANDREAS ANTONOPOULOS**

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

IV. Nasusukat

Pinapatulad ng blockchain ng MimbleWimble ang Epic Cash na nagdudulot ng pagsulong sa pagsusukat bilang isang resulta ng isang disenyo na nagbabawas ng labis na data ng transaksyon. Ang paggawa ng Cut-through na responsable para sa paniniguro na ang blockchain ay lumalaki ng mas mahusay sa paglipas ng panahon hindi katulad ng karamihan sa mga cryptocurrencies, kabilang ang Bitcoin, at ang mga bagong node ay maaaring malikha nang may kaunting pamumuhunan sa memorya at kapangyarihan ng pagbibilang. Sa natitirang mahusay sa espasyo, mahusay na pinapalawak ng pagkakalat ng network at pagpapaunlad ng desentralisasyon. At saka, habang ang Bitcoin node ay naiimbak sa look ng chain, ang mga ng Epic Cash ay maaaring nag-ambag sa seguridad ng network base sa maliit na subset ng mga block.

Karamihan sa mga cryptocurrencies ay kailangan ng walang takdang pag-iimbak ng lahat ng data ng transaksyon sa kanilang mga blockchain. Ang chain ng Bitcoin ay kasalukuyang nakakakuha ng 0.1353 GB ng memorya kada araw, habang ang chain ng Ethereum ay tumataas sa mas mabilis na rate na 0.2719 GB sa isang araw. Kung ang chain ng Bitcoin ay patuloy na lumalaki sa kasalukuyang rate nito, sa bandang huli ay maaabot nito ang laki ng 6 na TB sa oras na ang huling reward block na ito ay namina sa taon ng 2140. Ang Ethereum ay lalampas sa 10 TB sa petsang iyon[9]. Sa karamihan ng mga blockchain na walang MimbleWimble, ang mga transaksyon ay dapat mabiripika ng mga node sa buong mundo. Habang nagdaragdag ang data, gayon din ang pasanin sa bawat node. Kahit na sa 200 GB lamang (ang tinatayang laki ng kasalukuyang chain ng Bitcoin), ang pag-synchronize ng data ay nangangailangan ng isang matatag na network at ang bilis na disk na kayang mag basa at mag sulat.

Sa kadahilanang ito, ang pagmimina ay lalong naging sentralisado sa mga malalaking pool na gumagamit ng mga mapagkukunan ng magastos sa pagbibilang. **Sa halip, kung ang buong kasaysayan ng blockchain ng Bitcoin ay maiimbak sa Epic Cash blockchain, magkakasya ito sa halos 90% na mas kaunting espasyo**. Mas maliit ang mas mabilis dahil ang bawat transaksyon ay nangangailangan ng mas kaunting oras upang maipadala at masigurado.

Malulutas ng MimbleWimble ang dilemma ng imbakan na ito na may isang makabagong pamamaraan ng pag-pruning ng block, na tinukoy bilang 'Cut-through'. Upang maunawaan kung paano gumagana ang Cut-through, pinakamahusay na tingnan muna kung paano binubuo ang mga transaksyon at block sa loob ng isang blockchain MimbleWimble.

Inputs:

Sanggunian sa lumang mga outputs;

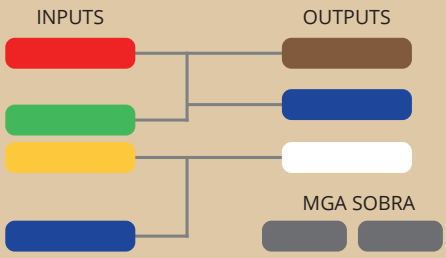
Outputs:

Kompidensyal na Transaksyon outputs at **rangeproofs**;

Sobra:

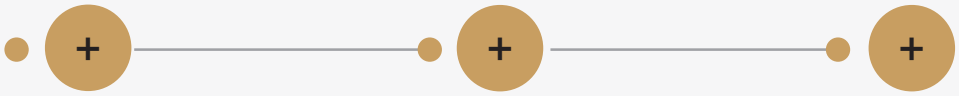
ng pagkakaiba sa pagitan ng outputs at inputs, karagdagan ang mga **signatures** (para sa pagpapatunay at upang mapatunayan ang non-inflation).

Larawan 2:
Mga Parte ng transaksyon ng MimbleWimble



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

All Epic Cash blocks contain:



Merkle Trees ng transaksyon na inputs; | **Merkle Trees ng transaksyon na outputs at rangeproofs;** | **Listahan ng mga halaga at signature**

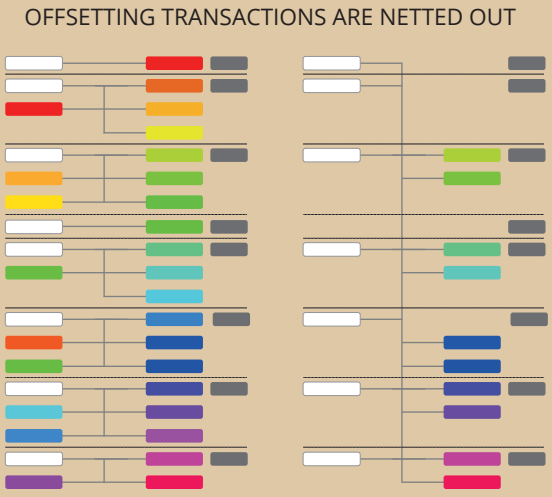
Sa Mga larawan 2 at 3, na inangkop mula sa mga presentasyon ni Andrew Poelstra10, makikita natin ang mga bagong naminang Epic na kinakatawan bilang ang mga puting input cells. Ang mga magkatulad na kulay na cell ay kumakatawan sa mga output na may kaukulang ginugol na mga input. Sa proseso ng Cut-Through, ang mga input at pagtutugma ng ginugol na mga output ay tinanggal upang malaya ang puwang sa loob ng block, na binabawasan ang dami ng data na kailangang maimbak sa blockchain. Habang ang mga transaksyon ay tinanggal mula sa ledger, ang natitirang labis na kernels (100 na bytes) ay permanenteng dokumento na naganap.

Ang mga block ay patuloy na nililikha, ang MimbleWimble ay nalalapat ang Cut-through sa mga block, kaya sa katagalan ay ang lahat ng natitira ay ang mga block header (humigit-kumulang na 250 bytes), mga hindi nakitang mga transaksyon, at mga kernels sa transaksyon (humigit-kumulang na 100 bytes). Si Grin, ang pangalawang pagpapatupad ng MimbleWimble na inilunsad, ay nagpakita na ang isang chain ng MimbleWimble na may katulad na bilang ng mga transaksyon sa chain ng Bitcoin ay halos 10% ng laki ng chain ng Bitcoin[11]. Bukod dito, ang sukat ng isang node ay magiging "sa pagkakasunud-sunod ng ilang GB para sa sukat ng Bitcoin chain, at potensyal na ma-optimize sa ilang daang megabytes.""[12]

Ito ay nakamarka na kaibahan sa Bitcoin, kung saan ang buong blockchain ay dapat na nakaimbak ng bawat node. Sa paglipas ng panahon, habang ang kahusayan ng espasyo ng Epic Cash blockchain ay lumalaki na nauugnay sa Bitcoin blockchain, gayon din ang mga kahusayan sa gastos na nauugnay sa paglahok ng mga node sa Epic Cash network. Ang mas mababang mga hadlang upang makilahok ay tumutulong na matiyak ang mahalagang kahusayan sa node layer ng disenyo ng network.

Sa pamamagitan ng pagpapatupad ng MimbleWimble at aplikasyon ng pagputol ng chain na may proseso ng Cut-through, ang Epic Cash blockchain ay nag-aalok ng nasusukat sa isang paraan na madalas na hindi napapansin ng pamayanang cryptocurrency. Ito ay isa na nakukuha ang kakanyahan ng mga proyekto ng Bitcoin at tulad ng pag-iisip: desentralisasyon. Hindi alintana kung gaano karaming mga transaksyon sa bawat segundo ang maaaring maiproseso ng barya, ano ang mabuti kung hindi ito mapapanatili ng isang malawak at magkakaibang network? Kung ang mga kinakailangan sa memorya ay tulad na ang pagpapatunay sa huli ay pumapasok sa malakas na kalipunan ng pagmimina, kung gayon ang lahat ng mga pagsisikap ng pamayanan ng cryptocurrency na lumikha ng isang desentralisado na ekosistema ay nahuhulog. Upang magbigay para sa karagdagang pagdaan, ang isang pagpapatupad ng istilo ng Layer 2 na Lightning ay pinlano bilang isang panandaliang layunin sa roadmap ng pagbuo ng Epic Cash.

Larawan 3:
Mga MimbleWimble na transaksyan bago at pagkatapos ng 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 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Patakarang Pang-salapi

Ang patakaran sa pananalapi ng Epic Cash at Bitcoin ay magkatulad. Ang Epic Cash na nagpapalipat-lipat na supply ay unang nagpapalawak ng mabilis at pagkatapos ay nagsi-synchronize sa nagpapalipat-lipat na supply ng Bitcoin noong 2028. Tumataas ito pagkatapos sa isang bumababang rate hanggang sa maabot ang isang maximum na supply ng 21 milyong Epic sa 2140. Ang Epic Cash ay may mga katangian upang maging isang ligtas na tindahan ng pangmatagalan na halaga dahil ang nagpapalipat-lipat na supply ay kilala sa anumang punto kasama ang lifecycle ng paglabas nito at nagtatapos sa isang nakapirming maximum na supply. Ang patakaran sa pananalapi ng Epic Cash ay nailalarawan sa pamamagitan ng sumusunod na apat na tampok:

- Mabilis na paglabas sa unang siyam na taon ng habangbuhay, kung saan 20,343,750 Epic (96.875% ng kabuuang supply) ay dapat na mamina. Ang eksaktong mga bilang ng paglabas ay nakabalangkas sa seksyon ng Emisyon Iskedyul ng papel na ito;
- Ang maximum na supply ng 21 milyong Epic ay maaabot sa taon 2140, sa humigit-kumulang na parehong oras tulad ng kapag ang Bitcoin ay umabot sa isang maximum na supply ng 21 milyong mga bilang;
- Ang Epic na nagpapalipat-lipat ng supply at paglabas ng rate ay naka-synchronize sa mga Bitcoin sa Epic Singularity ng Mayo 24, 2028. Kasunod ng Singularity, ang rate ng paglabas ay bumababa sa isang pagtaas ng rate, habang ang nagpapalipat-lipat na supply ay lumalaki sa isang pagbaba rate;
- Ang Epic ay may 8 decimal divisibility na istraktura, tulad ng: 1 Epic ay katumbas ng 100,000,000 freeman (tulad ng 1 Bitcoin ay katumbas ng 100,000,000 satoshi).

Ang patakaran sa pananalapi ng Epic Cash ay na-modelo pagkatapos ng Bitcoin para sa mga sumusunod na kadahilanan:

- Kasunduan sa pang-ekonomiyang mga pundasyon ng Bitcoin, lalo na ang kakulangan at mahuhulaan ng nagpapalipat-lipat na supply ay nakasalalay sa matibay nitong katangian na pag-iimbak ng halaga;
- Pamilyar na ang publiko sa modelo ng Bitcoin at napatunayan na track record nitong nakaraang sampung taon mula nang ito ay umpisahan. Sa pamamagitan ng humigit-kumulang na pag-synchronise sa supply ng sirkulasyon ng Bitcoin, at pagsalamin sa pinakamataas na istruktura ng paghahatid at paghihiwalay ng Bitcoin, ang Epic ay tumatakbo sa landas ng hindi bababa sa paglaban sa pag-tangkilik ng masa.

VI. Iskedyul ng Paglabas

Mayroong 33 mining eras ang Epic Cash, bawat isa ay tinukoy ng pagbawas sa mga block rewards, na nauugnay sa kanilang nauna. Ang Epic Genesis, ang petsa kung saan ang epic block na # 1 ay namina, naganap sa Agosto 2019. Ang mga block ay namina isang beses bawat minuto. Ang unang limang erya ay gumagawa ng halos 97% ng maximum na suplay ng Epic, na tumutugma sa 20 taon ng mga paglabas ng Bitcoin sa tinatayang siyam na taon. Maaari itong isipin bilang isang pagkakataon upang 'iatras ang orasan' para sa mga hindi nakuha sa kamangha-manghang pagtaas ng Bitcoin.

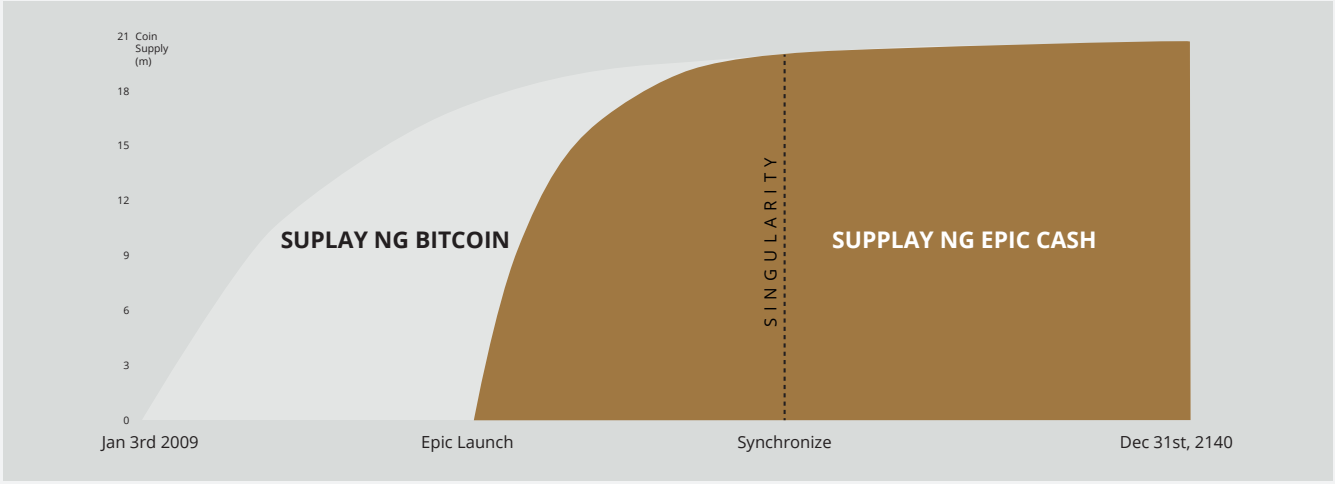
Ang iskedyul ng paglabas sa talahanayan 1 ay nagbabalangkas sa mga simula at pagtatapos ng mga petsa ng unang pitong mining eras, ang kanilang kaukulang mga block rewards, at ang kasunod na nagpapalibot na mga supply para sa bawat panahon. Ang mga eras 8 hanggang 33 ay hindi kasama sa talahanayan para sa kalabisan. Para sa mga panahong iyon, dapat na maunawaan na ang bawat kasunod na panahon ay magkakaroon ng gantimpala sa block na kalahati ng halaga ng gantimpala ng nauna na panahon, tulad ng sa Bitcoin. Ang halaga ng Epic na inilabas sa bawat isa sa mga eras na ito ay ang kabuuan ng mga block rewards sa loob ng 4 na taong panahon (humigit-kumulang 1460 araw).

Sa Epic Singularity (2028), ang Epic na nagpapalipat-lipat ng intersect ang bilang ng nagpapalipat-lipat na supply ng Bitcoin, kung saan tinatanggap ng Epic Cash ang Bitcoin block reward at paghiwa-hiwalay ng pattern, na nakikita ang mga block rewards na bumaba ng kalahati tuwing apat na taon. Ang tanging pagbubukod ay ang mga block ng Epic ay patuloy na namimina sa isang rate ng bawat minuto, kumpara sa rate ng Bitcoin ng isang bloke bawat sampung minuto. Sa pamamagitan nito, pinapanatili ng suplay ng Epic na nagpapalaganap ang tinatayang pagkakapareho sa nagpapalipat na supply ng Bitcoin para sa nalalabi sa kanilang pag-iral.

Talahanayan 1: Iskedyul ng Paglabas para sa unang pitong mining eras. Ang mga petsa ay malapit na tinatantya.

Panahon	1	2	3	4	5	SINGULARITY	6	7
Block Reward	16	8	4	2	1		0.15625	0.078125
Panimulang Petsa	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
Panghuling Petsa	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
Haba (sa mga araw)	334	470	601	800	1019		1460	1460
Panimulang Suplay	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Panghuling Suplay	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% ng Maximum na Suplay	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Larawan 4: Takdang paglabas ng Epic at Bitcoin



VII. Pagmimina

Ang blockchain ng Epic Cash ay ipinagpapatuloy ang desentralisasyon sa pamamagitan ng pagsalubong sa isang iba't ibang mga hardware computation. Ang pagmimina ng Epic ay unang magagamit sa mga CPU, GPU, at ASIC, gamit ang tatlong kani-kanilang mga hashing algorithm: RandomX, ProgPow, at CuckATOO31+. Ang mga algorithm ay maaaring maging walang pakialam na mapalitan na walang pag-kompromiso sa integridad ng chain.

1 RandomX at CPUs

Ang RandomX ay isang Proof-of-Work (PoW) algorithm na na-optimize para sa mga pangkalahatang layunin ng mga CPU. Gumagamit ito ng randomized na pagpapatupad ng programa na may maraming mga pamamaraan sa memory-hard upang makamit ang mga sumusunod na layunin:

- Iniiwasan ang pagbuo ng single-chip ASICs;
- Bawasan ang pagkalamangan ng mga hardware sa mga pangkalahatang layunin na mga CPU.

Ang Pagmimina ng Epic na may mga CPU ay nangangailangan ng isang magkadikit na paglalaan ng 2 GB ng pisikal na RAM, 16 KB ng L1 cache, 256 KB ng L2 cache, at 2 MB ng L3 cache bawat mining thread[13]. Ang mga Windows 10 na kagamitan ay nangangailangan ng 8 GB o higit pang RAM. Hindi ito aakalain na sa isang araw sa hindi masyadong malayong hinaharap na mga mobile phone ay maaaring na rin gamitin sa mining nodes. Ang unang pagsasama ng CPU sa network ng pagmimina ng Epic Cash ay isang mahusay na pagkakataon para sa marami na may lamang katamtaman na computing ay nangangahulugan na kumita ng mga reward block sa pamamagitan ng pagtulong upang ma-secure ang network ng Epic Cash.

2 ProgPow at GPUs

Ang Programmatic Proof-of-Work (ProgPow) ay isang algorithm na nakadepende sa memorya ng bandwidth at pagkalkula ng core ng mga randomized na pagkakasunud-sunod ng matematika, na kung saan ito ay kinalalamangan ng mga tampok ng mga GPU's at sa gayon mahusay na makuha ang kabuuang gastos ng enerhiya sa hardware. Tulad ng ProgPow ay partikular na idinisenyo upang makalamang ang mga GPU sa kalakal, pareho itong mahirap at mahal upang makamit ang makabuluhang mas mataas na kahusayan sa pamamagitan ng mga hardware. Tulad nito, ang algorithm ng ProgPow ay nagpapagaan ng mga insentibo para sa mga malalaking pool ng ASIC na malalampasan ang mga GPU, tulad ng madalas na nakikita sa maraming iba pang mga algorithm ng PoW, tulad ng SHA-256 ng Bitcoin. Ang mga GPU, kahit na hindi karaniwan bilang mga CPU, ay karaniwang magagamit pa rin. Sa pamamagitan ng pag-unlad ng teknolohikal na hinimok ng mga powerhouse, ang Nvidia at AMD, ang mga GPU ay maaaring magkatulad na proseso ng maraming mga multiple ng mga solusyon sa pagmimina sa itaas ng mga CPU sa isang per-unit na batayan. Ito ay dahil sa kumbinasyon ng ubiquity at mataas na lakas ng pagproseso na ibibigay ng mga GPU ang lakas sa karamihan ng aktibidad ng pagmimina sa panahon ng paunang panahon, tulad ng ipinahiwatig sa Talahanayan 2.

3 CuckATOO+31 at ASICs

Ang CuckATOO31+ ay isang ASIC friendly permutation ng Cuckoo Cycle algorithm na binuo ng Dutch computer scientist na si John Tromp. Katulad ito ng ASIC resistant CuckAROO29, CuckATOO31+ ay bumubuo ng mga random na mga bipartite na mga grapiko at nagpepresenta sa mga minero na may gawain ng paghahanap ng isang loop ng naibigay na haba ng 'N' na dumaan sa mga vertice ng grapiko na iyon.

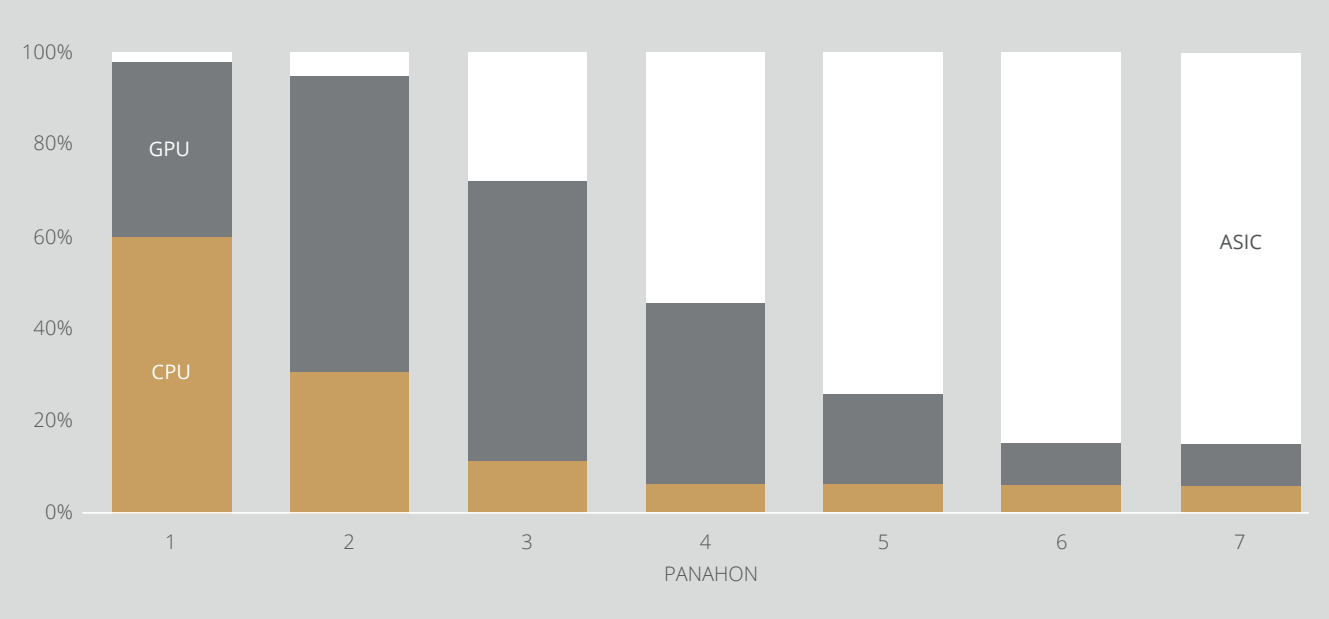
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Ito ay isang memory bound task, na nangangahulugang ang oras ng solusyon ay nakasalalay sa memory bandwith sa halip na raw processor o bilis ng GPU. Bilang isang resulta, ang mga algorithm ng Cuckoo Cycle ay gumagawa ng mas kaunting init at kumonsumo nang mas mababa sa enerhiya kaysa sa tradisyonal na mga algorithm ng PoW. Ang ASIC friendly na CuckAToo31+ ay nagbibigay-daan sa pagpapabuti ng kahusayan sa mga GPU sa pamamagitan ng paggamit ng daan-daang MB ng SRAM habang natitirang bottlenecked ng memorya I/O[14]. Sa huli, ang mga ASIC ay nag-aalok ng pinakamalaking potensyal na mga ekonomiya ng laki ng tatlong mga pagpipilian sa pagmimina. Sa interes ng kawalang-kasiyahan, gayunpaman, kahit na inilalaan nila ang isang maliit na bahagi ng mga reward block na nauugnay sa mga CPU at GPUs nang maaga, sa kalaunan ay ipinapalagay ng mga ASIC ang isang major stake ng mga naminang reward block, sa pag-aakalang magkakaroon ng isang mapagkumpitensya na ekosistema ng mga tagagawa ng kagamitan para sa CuckAToo31+.

Talahanayan 2: Ang mga nilaan na mining reward. Paksa sa pagbabago. Ang mga nilaan ay ituturo upang makamit ang maximum na desentralisasyon at naaayon sa pangmatagalang interes ng network.

Panahon	1	2	3	4	5	6	7
Mga Araw	334	470	601	800	1019	1460	1460
CPUs	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASICs	2%	5%	28%	55%	75%	85%	85%

Larawan 5: Mga nilaan sa mining reward para sa bawat panahon ayon sa Talahanayan 2. Paksa sa pagbabago.



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

4 Mga Kontribusyon sa Pagmimina

Simula sa Epic Genesis (2019) at magtatapos sa Epic Singularity (2028), sa panahon ng proseso ng pagmimina, mayroong isang paglalaan ng Epic na na-redirect, bilang mga kontribusyon sa pagmimina, patungo sa EPIC Blockchain Foundation.

Ang EPIC Blockchain Foundation ay nakatuon sa pagpapa-unlad ng teknikal at nagtataguyod ng kamalayan at kagamitan ng proyekto ng Epic Cash sa mga unang taon ng pagsisimula nito, sa pamamagitan ng paglikha ng mga aktibidad sa marketing at pagbuo ng mga pakikipagsama sa loob ng industriya ng teknolohiya sa pananalapi

Pagkatapos ng Singularity, ang tungkulin ng EPIC Foundation ay kukuha ng EPIC Distributed Autonomous Corporation (EDAC), na bubuo ng pundasyon bago ang pagsauli.

Ang EPIC Blockchain Foundation ay pinondohan ng porsyento ng mga mining reward, na nababawas mula sa mga block rewards, ayon sa sumusunod na taunang rate:

Talahanayan 3: Taunang rate para sa mga pagmimina ng Foundation bilang porsyento ng mga gantimpala mining reward

Taon	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% ng Mining Rewards	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Konklusyon

Ang mga layunin ng Epic na kilalanin bilang 'decentralized digital silver', isang kagamitan ng exchange na kasalungat ng Bitcoin bilang decentralized digital gold. Sa muling paggawa ng nawalang fungibility sa higit na mas mabisa na enerhiya at mabisa na ecologically-friendly na kalakasan, tinalikwas ng Epic Cash ang balanse ng power back sa pabor ng mga indibidwal na gumagamit, sa payak na kaibahan sa kamakailang mga nausong sentalisado. Ang kumbinasyon ng mga ekonomikong Bitcoin, game theory, at napatunayan na proof-of-work formula na may pinakamahusay na kontemporaryong teknolohiyang blockchain ay nagreresulta sa isang walang tiwala, hindi mababago, at desentralisado na pera (Epic) na nasusukat, fungible, at pinoprotektahan ang pagkapribado ng mga gumagamit nito. Ang blockchain ng Epic Cash ay bukas, pampubliko, walang hangganan, at lumalaban sa censorship. Pinapanatili nito ang pagkapribado at kayamanan ng mga gumagamit nito at ginagantimpalaan ang mga nagtatalaga ng kanilang hardware sa suporta ng network sa pamamagitan ng pagmimina. Ang bawat Epic ay namimina sa pamamagitan ng proof-of-work. Nagsisimula ang suplay sa zero at ang network ay itinuturing na patas na inilunsad, na may isang function na testnet na kasalukuyang tumatakbo.

Mga Pangunahin Katotohanan sa Epic Cash:

- **Nagsimula ang Pagmimina noong ika-1 ng Agosto, 2019.**

- **Ang blockchain ng Epic Cash ay naka batay sa MimbleWimble.**

  Ang mga tampok na natukoy sa protocol ay ang mga:

  1. **Cut-Through** – ang pag-tanggal ng kalabisan na impormasyon mula sa blockchain upang maitaguyod ang kahusayan sa espasyo, hinihikayat ang malawak na sukat ng pakikilahok sa network validation, at mapagkakatiwalaang desentralisasyon;
  2. ***CoinJoin*** – ang pag-bundle ng mga transaksyon sa loob ng isang block upang matiyak ang fungibility ng Epic cryptocurrency;
  3. ***Dandelion++ Protocol*** – ang pagpapalaganap ng mga transaksyon sa pamamagitan ng pakikipag-ugnay sa mga magkakaugnay na channel, at nakakalat sa isang malawak na network ng mga node, paghihiwalay ng mga koneksyon sa pagitan ng mga transaksyon at kanilang pinagmulan;
  4. **Walang mga Wallet Address** – ang paggamit ng isang grand multi-signature upang makabuo ng mga private key para sa mga partido na nagtatransaksyon, inaalis ang pangangailangan para sa mga wallet address.

- **Ang Patakaran sa Pananalapi ng Epic Cash** ay idinisenyo upang makasaby ang suplay ng Epic na nagpapalipat-lipat kasama ang nagpapalipat-lipat na suplay ng Bitcoin sa halos siyam na taon at maabot ang parehong maximum na suplay na 21 milyong mga bilang sa parehong oras ng Bitcoin, sa taong 2140. Ang patak na pagbagsak ng inflationary na ito ay ginagarantiyahan ang transparency. mahuhulaan ng suplay, at kakulangan, pinasisigla ang seguridad ng pangmatagalang pag-iimbak ng halaga.

- Ang **Pagmimina** na kung saan kasama ang CPUs, GPUs, at ASICs sa pamamagitan ng RandomX, ProgPow, at CuckATOo31+ algorithms, upang pamahalaan ang mass adoption at pagiging epektibo ng network.

IX. Teknikal na mga Detalye

Pangalan ng Proyekto: Epic Cash
Pangalan ng Pananalapi: Epic
Oras ng Block: 60 na segundo
Sukat ng Block: 1 MB
Panimulang Suplay: 0
Panghuling Suplay: 21,000,000
Genesis Block: Agosto , 2019
Consensus: RandomX (CPUs), ProgPow (GPUs) and CuckAToo31+ (ASICs)

Mga Link:

www.epic.tech

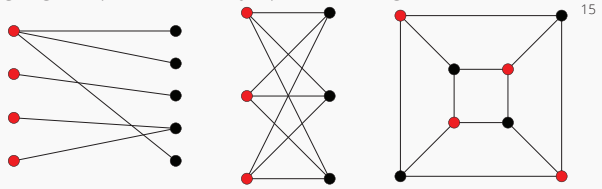
t.me/EpicCash – Telegram

t.me/EpicCashFilipino

X. Talahulunganan

ASIC Application-Specific Integrated Circuits; Ang mga chips na idinisenyo para sa isang

Bipartite Graph layunin ng isang hanay ng mga graph vertices na nahati sa dalawang hindi nagtatakda ng mga set na walang dalawang mga graph vertices sa loob ng katabi ng parehong hanay.



Blinding Factor ang random na element na ipinakilala sa isang digital na mensahe upang mapadali ang pag-encrypt; isang nakabahaging lihim sa pagitan ng dalawang partido na nag-encrypt ng mga input at output sa partikular na transaksyon pati na rin ang public at private key ng magkatransaksyong partido[16].

Block Reward ang bagong Epic na ipinamamahagi ng network bilang mga gantimpala para sa pagkalkula na isinagawa upang mapatunayan ang mga transaksyon sa loob ng isang bagong block.

Cache isang bahagi ng hardware o software na nag-iimbak ng data upang ang mga hinihingi sa hinaharap na data ay maihatid nang mas mabilis.

CPU Central Processing Unit: sangkap ng kompyuter na responsable para sa pagbibigay kahulugan at pagpapatupad ng karamihan sa mga utos mula sa iba pang hardware at software ng computer.

Cut-Through isang proseso ng MimbleWimble blockchain kung saan ang mga input at mga tumutugmang mga output ay tinanggal upang palayain ang espasyo sa loob ng block, binabawasan ang dami ng data na kinakailangan upang maimbak sa blockchain.

Desentralisasyon ang estado ng pagpapakalat ng isang operasyon at pamamahala sa isang network.

Epic Singularity ang punto kung saan ang pag-iikot ng supply ng Epic ay nag-sasabay sa umiikot na supply ng Bitcoin (Mayo 2028).

Fungibility ang katangian ng isang kagamitan o kalakal kung saan ang mga indibidwal na bilang ay mahalagang mapagpapalit, at ang bawat bahagi nito ay hindi mailalarawan mula sa ibang bahagi.

Genesis (Pangyayari) ang pagmimina ng pinakaunang Epic block at ang opisyal na simula ng blockchain.

GPU Graphics Processing Unit: Ang isang yunit na naglalaman ng isang maaaring ma-program na logic chip (processor) na dalubhasa para sa mga pagpapaandar ng pagpapakita. Ang mga GPU ng mamimili ay maaaring maging angkop para sa pagmimina ng cryptocurrency.

Hash isang halaga na nakalkula mula sa isang numero ng input ng paggamit gamit ang isang function ng hashing.

Hashing Algorithm (function) isang algorithm ng matematika na naglalagay ng mga datos ng nakataon sa sukat ng isang hash ng isang nakapirming laki na ginagamit para sa pagbuo at pagpapatunay ng mga signature sa digital, message authentication codes (MAC), at iba pang mga paraan ng pagpapatunay.

Homomorphic Encryption paraan ng paggawa ng kalkulasyon sa naka-encrypt na impormasyon na hindi na naka-decrypt. (sa programming) ang estado kung saan ang isang bagay ay hindi mababago pagkatapos ng paglikha nito.

Immutability

Input (MimbleWimble) ang sangkap ng isang transaksyon ng MimbleWimble na kumakatawan sa pagpapadala ng partido ng transaksyon; nilikha mula sa mga output ng nakaraang mga transaksyon.

I/O input/output; ang komunikasyon sa pagitan ng isang sistema ng pagpoproseso ng impormasyon, tulad ng isang computer, at sa labas ng mundo, marahil isang tao o ibang sistema ng pagproseso ng impormasyon.

Mapagkakatiwalaan ang kalidad ng isang network ng cryptocurrency upang sumunod sa mga patakaran ng isang protocol nang walang pagpapatupad ng isang gitnang partido.

Maximum na Suplay ang halaga ng Epic na maabot sa kung saan ang punto ng nagpapalipat-lipat na supply ay hindi tataas pagkatapos (21,000,000 Epic).

Memory-Hard ang paggamit ng maraming RAM upang maiwasan ang sabay-sabay na mga koneksyon na tumatakbo ng magkakatulad. Ang Memory-hard functions ay mga algorithm na mayroong mga oras ng pagkalkula una na napagpasyahan ng magagamit na memorya upang hawakan ang data. Kilala rin bilang memory-bound functions

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

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

Merkle Tree	isang istraktura ng data na ginamit sa mga aplikasyon ng agham sa computer. Sa mga blockchain, pinapayagan ng mga Merkle tree para sa mahusay at ligtas na pag-verify ng mga nilalaman sa malaking istraktura ng data
MimbleWimble	isang protocol na inilagay ng isang malasagisag na taga-ambag, na ang moniker na si Tom Elvis Jedusor, sa isang chatroom ng mga developer ng Bitcoin.
Multisignature	pamamaraan ng digital na signature na nagbibigay-daan sa isang pangkat ng mga gumagamit na mag-sign isang dokumento. Karaniwan, ang isang multisignature na algorithm ay gumagawa ng isang magkasanib na signature na mas siksik kaysa sa isang koleksyon ng mga natatanging signature mula sa lahat ng mga gumagamit[17].
Node	isang computer na kumokonekta sa isang network ng blockchain at mga sanga sa ibang mga node sa loob ng network upang ipamahagi ang impormasyon tungkol sa mga transaksyon at mga block, sa paraang peer-to-peer.
One Way Aggregate Signature (OWAS)	isang signature sa transaksyon na binubuo ng maraming mga signature na naka-encrypt sa isang paraan upang mahirapan na makalkula ang mga indibidwal na signature na pinagsamang bahagi
Output (MimbleWimble)	ang sangkap ng isang transaksyon ng MimbleWimble na kumakatawan sa pagtanggap ng transaksyon; ginamit bilang mga input para sa kasunod na mga transaksyon.
Paghahati (para sa Bitcoin)	nangyayari tuwing 4 na taon. Ang rate ng suplay ay bumababa ng 50% pagkatapos ng bawat kaganapan na paghahati.
Paglabas	ang paglikha ng mga bagong Epic nakuha ng mga minero sa mga block reward. Ang Epic ay nililikha bawat 60 segundo habang ang mga transaksyon ay nakumpirma sa blockchain.
Pedersen Commitment Scheme	isang primarya na kriptograpiko na nagbibigay-daan sa isang salawikain na gumawa sa isang napiling halaga nang hindi ibubunyag ang anumang impormasyon tungkol dito at nang walang kasabihan na makapagtagumpay sa paggawa sa halaga.
Private Key	ang private key ay isang maliit na maliit na code na ipinares sa isang public susi upang i-set off ang mga algorithm para sa pag-encrypt ng teksto at decryption. Ito ay nilikha bilang bahagi ng public key na kriptograpiya sa panahon ng asymmetric-key encryption at ginamit upang i-decrypt at ibahin ang anyo ng isang mensahe sa isang mababasa na format
Proof of Work (PoW)	isang piraso ng data na mahirap (magastos at ubos oras) mabuo, ngunit madali para sa iba na mapatunayan, at kung saan ay nasiyahan ang ilang mga kinakailangan. Ang Proofs of Work ay madalas na ginagamit sa henerasyon ng block ng cryptocurrency.
Public Key	ang public key ay nilikha sa public key na pag-encrypt ng krograpiya na gumagamit ng mga algorithm ng asymmetric-key encryption. Ang mga public key ay ginagamit upang i-convert ang isang mensahe sa isang hindi mababasang format.
RAM (Random Access Memory)	mabilis na pag-access ng data sa chips ng imbakan sa isang kagamitan ng kompyuter kung saan ang operating system (OS), mga programa ng aplikasyon at data sa kasalukuyang paggamit ay pinapanatili upang mabilis itong maabot ng processor ng kagamitan.
Rangeproof	pangako na nagpapatunay na kung saan nagbeberipika na ang kabuuan ng mga input ng transaksyon ay mas malaki kaysa sa kabuuan ng mga output ng transaksyon at na ang lahat ng mga halaga ng transaksyon ay positibo. Tinitiyak ng mga Rangeproof na hindi nai-tamped ang suplay ng pananalapi.
Signature (Digital)	isang karaniwang bahagi ng isang protocol ng blockchain, higit sa lahat na ginagamit para sa pag-secure ng mga transaksyon at mga block ng mga transaksyon, paglilipat ng impormasyon, pamamahala sa kontrata at anumang iba pang mga kaso kung saan mahalaga ang pag-alis at pag-iwas sa anumang panlabas na pag-babago. Nagbibigay sila ng tatlong bentahe ng pag-iimbak at paglilipat ng impormasyon sa blockchain • Inihayag nila kung ang data na ipinadala ay nabago; • Patunayan ang paglahok ng isang partikular na partido sa transaksyon • Maaaring maging ligtas sa batas.
Sobra (MimbleWimble)	ang pagkakaiba sa pagitan ng mga output at mga input, kasama ang mga signature (para sa pagpapatunay at upang patunayan ang non-inflation).
SRAM (Static Random Access Memory)	Random Access Memory (RAM) na nagpapanatili ng mga bits ng data sa memorya nito hangga't ang power ay naibahagi.
Throughput	ang sukatan ng mga transaksyon sa bawat segundo na maaaring isagawa ng isang ibinigay na protocol ng cryptocurrency.
Umiikot na Suplay	ang bilang ng Epic sa nasabing oras.

[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 PRIVATE INTERNET CASH