Keluarga Freeman

4 Julai 2019

TUNAI EPIC

EPIC PRIVATE TUNAI

EPIC

Sistem Cash Electronic Peer-to-Peer

STORE NILAI + PENGANTAR EXCHANGE + UNIT AKAUN

1.7 bilion orang dewasa tidak mempunyai akses kepada sistem kewangan global, manakala 1.3 bilion lagi adalah kurang mendapat perkhidmatan. Epic Cash membuka potensi manusia dengan menyambung individu untuk pasaran global. Cepat, hampir bebas untuk digunakan, dan terbuka kepada semua.

versi 7.1b

kandungan

I. abstrak

Epic tunai adalah titik akhir dalam perjalanan ke arah tunai internet P2P benar, asas sistem kewangan swasta. Mata wang Epic bertujuan untuk menjadi bentuk privasi melindungi paling berkesan di dunia wang digital. Bagi memenuhi matlamat tersebut, ia memenuhi tiga fungsi utama wang:

1. Kedai Nilai- **boleh disimpan, diambil dan ditukar pada masa yang lain, dan nilai yang diramalkan apabila diambil;**
2. Pengantar Exchange- **apa-apa diterima sebagai mewakili standard nilai dan ditukar dengan barangan atau perkhidmatan;**
3. Unit Akaun- **unit yang mana nilai perkara yang diambil kira dan dibandingkan.**

	$ USD	BTC	EPIC
Kedai Nilai	✗	✓	✓
Pengantar Exchange	✓	✗	✓
Unit Akaun	✓	✗	✓

Pada tahun 2009 Bitcoin muncul sebagai mata wang digital berasaskan blockchain-pertama, dan dengan itu tiga ciri-ciri tertentu terhadap mana cryptocurrencies lain dinilai:

- Trustlessness - **tiada siapa yang dikehendaki mempercayai mana-mana entiti berpusat atau pihak agar rangkaian untuk berfungsi;**
- ketetapan - **transaksi yang tidak bolehmenjadi asal;**
  a. Ia harus sangat tidak mungkin atau sukar untuk menulis semula sejarah;
  b. Ia harus menjadi mustahil untuk sesiapa sahaja tetapi pemilik kunci persendirian untuk menggerakkan dana yang berkaitan dengan kunci persendirian itu;
  c. Semua urusniaga dicatat dalam blockchain.
- buktinya - **"Blockchains dari segi politik tidak berpusat (tidak ada yang mengawal mereka) dan seni bina berpusat (tiada titik infrastruktur kegagalan) ..."[1].**

Bitcoin berkobar laluan baru teknologi di samping mematuhi asas-asas yang telah teruji dalam struktur dasar monetarinya. kejayaan Bitcoin yang amat berkaitan dengan bekalan terhad digabungkan dengan yg tak dpt dipercaya, tidak berubah, dan blockchain berpusat. Epic tunai mengemulasi dasar monetari Bitcoin sebanyak mengurangkan inflasi dan bekalan yang terhad untuk memastikan mata wang Epic boleh berfungsi sebagai kedai yang berkesan untuk nilai.

Walaupun kejayaan Bitcoin ini, beberapa kelemahan telah diturunkan sejak penubuhannya 10 tahun lalu. Projek-projek lain telah cuba untuk mengatasi kelemahan ini dan kami telah disiasat yang terbaik ini untuk digunakan sebagai titik permulaan kita. Kami diputuskan menggunakan pangkalan kod Grin dan kerja-kerja yang sangat baik daripada beberapa projek lain untuk membantu kami sempurna pada pencapaian keras memenangi dan mendapati kesalahan yang terdahulu Epic Cash. Epic tunai memiliki kualiti yang utama untuk menjadi mata wang ideal:

- Fungibility - **Nilai unit tertentu Epic mesti sentiasa sama dengan satu lagi unit Epic, hanya sebagai salah satu Yen atau Yuan adalah sentiasa sama dengan dan diganti dengan yang lain Yen atau Yuan. Pencapaian fungibility sebahagian besarnya bergantung kepada privasi.**
- berskala - **Epic tunai mengekalkan blockchain berkesan ruang, di mana baru nod mudah ditubuhkan tanpa peralatan sumber. The blockchain Epic tunai mampu sekurang-kurangnya dua kali gandapemprosesan Bitcoin.**
- Privasi- **The blockchain Epic tunai melindungi ketanpanamaan pemegang Epic dan pengguna dengan melindungi butiran transaksi daripada pihak ketiga, dan direka untuk menjadi kedua-dua tidak dapat dikesan dan tidak dapat dilihat dengan pengawasan.**
- kelajuan- **Urusniaga Epic tunai adalah lancar, berterusan dan dilaksanakan lebih cepat daripada dalam generasi sebelumnya teknologi blockchain. Manakala Bitcoin memerlukan enam blok 10 minit untuk mencapai pengesahan transaksi lengkap, transaksi Epic berlaku dalam pengesahan blok tunggal secepat blok 1 minit telah dilombong.**

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

II. Privasi

Penggunaan moden wang boleh difahami sebagai pemindahan kolektif unit akaun antara manusia dan institusi. Landskap wang pada bila-bila masa boleh dipetakan dengan menjawab soalan-soalan berikut:

1. *Yang memegangnya, dan berapa banyak yang mereka memegang?*
2. *Yang menjalankan transaksi dengan siapa, dan berapa banyak?*

Untuk mata wang fiat tradisional, dan sememangnya Bitcoin juga, kita boleh menjawab soalan-soalan. Dengan berbuat demikian, banyak yang boleh mendedahkan tentang kehidupan manusia, seperti corak penggunaan, pemilikan, dan rakan niaga urus niaga. Agak kesimpulan tepat yang boleh dibuat mengenai minat dan niat seseorang individu dengan mengesan pemindahan nilai. Tanpa privasi, data transaksi boleh menjadi maklumat berbahaya di tangan pihak ketiga pemangsa.

penggunaan dekad lalu terhadap cryptocurrency menunjukkan kesinambungan "privasi" dalam pelbagai blockchain pelaksanaan. Skala privasi, seseorang itu perlu dipertimbangkan, antara terbuka dan terkenal pada satu hujung ke hujung tanpa nama yang lain. Privasi menghakis, satu asas penting dalam cryptocurrency, trustlessness, mempersendakan. Seperti yang dibuktikan oleh kejayaan perkhidmatan analisis Bitcoin blockchain, Bitcoin terletak lebih ke arah akhirnya terkenal telus spektrum privasi. Pengguna semakin mesti mengambil langkah-langkah untuk memastikan mereka tidak secara tidak sengaja berurus niaga dalam dicemari Bitcoin. Penyelesaian Epic tunai buaian jarum ke arah tanpa nama dan mengembalikan harta penting ini dengan memastikan bahawa kedua-dua privasi individu dan privasi transaksi kejuruteraan ke dalam sistem di peringkat asas.

Privasi Identiti

Privasi Transaksi

Privasi Identiti

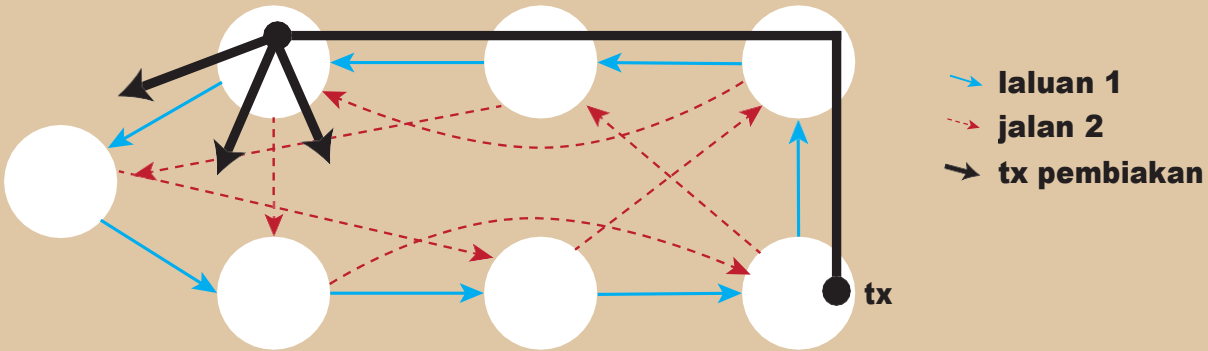
Kebanyakan cryptocurrencies seperti Bitcoin disimpan dalam dompet yang alamat rujuk kunci awam diperolehi daripada kunci-kunci peribadi dompet itu. Ini alamat boleh dianggap sebagai Locator peti besi peribadi seseorang dalam dunia digital. The blockchain Epic tunai menghapuskan alamat sepenuhnya dan bukannya digunakan satu grandmultisignature dari mana semua kunci awam dan swasta dijana secara sekali guna.

Kerana Bitcoin alamat wallet adalah pencari bilik kebal di dunia digital, dompet yang boleh dikesan ke alamat pemilik Protokol Internet (IP), yang sauh pemilik komputer di lokasi yang unik pada titik tertentu dalam masa. Hanya menjelaskan: apabila transaksi Bitcoin berlaku, urus niaga itu disiarkan dari hab komunikasi dipanggil 'node' dan kemudian disebarkan kepada nod lain yang dikenali sebagai 'rakan-rakan'. Maklumat itu kemudian dengan cepat merebak kepada setiap rakan-rakan mereka nod 'berturut-turut di seluruh rangkaian. Proses ini dinamakan "Protokol Gossip". Secara ringkasnya, setiap Bitcoin mempunyai kedudukan dalam talian yang boleh dilihat dan lokasi fizikal di mana ia, atau sebaliknya pemilik Bitcoin, boleh didapati. Sebagai wartawan Grace Caffyn berkata, Bitcoin adalah "tidak lebih rahsia daripada carian Google daripada sambungan internet di rumah."[2]

Selain menghapuskan alamat wallet, yang blockchain Epic tunai menjamin privasi identiti dengan memastikan alamat IP tidak dapat dikesan.Ia melakukan ini melalui integrasi Protokol ++ Dandelion. Meningkatkan atas pendahulunya, Protokol Dandelion asal, Protokol ++ Dandelion adalah hasil daripada kerja terus tujuh penyelidik untuk memerangi serangan deanonymization pada blockchain. Melalui Dandelion ++, transaksi melewati laluan yang saling berkaitan rawak, atau 'kabel', dan kemudian tiba-tiba tersebar ke rangkaian besar nod, seperti buah bunga Dandelion apabila ditiup dari batang mereka (Rajah 1). Ini menjadikan ia hampir mustahil untuk mengesan transaksi kembali kepada asal-usul mereka, dan dengan itu alamat IP berasal mereka.

Rajah 1: Urus niaga tanpa nama dengan*Dandelion ++ Protokol.*

***Dandelion* ++ke hadapan mesej melalui salah satu daripada dua laluan saling berkaitan pada graf 4-biasa, kemudian menyiarkan menggunakan resapan. Dalam rajah, transaksi merambat atas jalan pepejal biru[3]. Proses ini menjadikan ia amat sukar untuk mengesan transaksi kembali kepada sumber mereka, dengan itu memelihara privasi.**



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

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

Privasi Transaksi

The blockchain Epic tunai menjamin privasi transaksi oleh mengaburkan jumlah dan hubungan Pengguna-penerima transaksi. Ini dicapai melalui aplikasi idea biasa dari Transaksi Sulit (CT) 4 dan CoinJoin5, kaedah sebahagian besarnya dibangunkan oleh Gregory Maxwell (Pemaju Bitcoin Core, Pengasas Bersama dan Ketua Pegawai Teknikal Blockstream).

CT, **Pada asalnya dicipta oleh Adam Kembali dan kemudian ditapis oleh Maxwell, kerja-kerja oleh urus niaga memecah masuk ke dalam bahagian yang lebih kecil melalui homomorphic penyulitan, Satu kaedah melaksanakan pengiraan maklumat disulitkan tanpa decrypting terlebih dahulu untuk mengekalkan privasi. Setelah dibahagikan, pemerhati tidak boleh melihat jumlah sebenar urusniaga kerana faktor pembutaan, Satu sistem yang melemparkan nombor rawak ke dalam campuran transaksi serpihan untuk menyembunyikan nilai-nilai mereka serpihan. Akhirnya, hanya transaksi pihak tahu nilai pertukaran, manakala urus niaga itu disahkan oleh rangkaian melalui pengesahan bahawa jumlah nilai output sama dengan jumlah nilai input, dan jumlah output pembutaan faktor sama dengan jumlah yang input**

Untuk merumitkan lagi tugas mata prying, semua urus niaga Epic Tunai diselaputi dengan CT dan kemudian dicampurkan bersama-sama untuk menyembunyikan hubungan antara pihak-pihak yang berurus niaga. Ini dilakukan melalui konsep kedua Maxwell, CoinJoin.

Untuk menggambarkan CoinJoin simplistik, bayangkan bahawa A, B dan C menghantar Epic untuk X, Y dan Z, masing-masing. Dihantar melalui medium CoinJoin, semua yang diketahui ialah A, B dan C adalah menghantar dan X, Y dan Z menerima, manakala jumlah transaksi terus kekal tidak kelihatan. Sistem CoinJoin adalah asas kepada Epic Tunai melalui One-Way Agregat Signatures (OWAS), Yang menggabungkan semua transaksi dalam satu blok ke dalam satu transaksi.

Privasi: Ringkasan

The blockchain Epic tunai melindungi privasi individu dan urus niaga mereka dengan:

- Menghapuskan alamat wallet - Tiada pengecam lokasi ke bilik kebal digital dalam blockchain. Transaksi dibina langsung orang-ke-orang di
secara wallet-to-wallet;
- *Dandelion ++ Protokol* - mengaburi laluan digital daripada transaksi dari alamat IP Pengguna transaksi ini;
- *Transaksi sulit*- Urus niaga terbahagi kepada beberapa keping dan memperkenalkan pembutaan faktor ke dalam koleksi potongan-potongan daging, supaya nilai-nilai satu bahagian dan lain-lain
- *CoinJoin*- menggabungkan urus niaga ke dalam berkas untuk topeng

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

III. Fungibility

Charlie Lee, Pencipta Litecoin, menyatakan bahawa fungibility adalah satu-satunya harta wang bunyi hilang daripada Bitcoin dan Litecoin, mengakui bahawa privasi dan fungibility adalah medan pertempuran yang akan datang bagi mereka coins6.Andreas Antonopoulos, Salah seorang pakar blockchain terkemuka dunia, mendakwa bahawa "... syiling tercemar yang merosakkan. Jika anda memecahkan fungibility dan privasi, anda memecahkan mata wang. "7

Fungibility adalah hakmilik satu set barangan atau harta yang memastikan unit individu set yang mempunyai nilai yang sama dan boleh ditukar. Ia adalah apa yang membezakan bentuk terawal mata wang daripada sistem sebelumnya mereka tukar barang. Tanpa keyakinan dalam fungibility wang, wang yang cepat kehilangan utiliti. Seperti yang akan ditunjukkan di bawah, fungibility kebanyakan cryptocurrencies tidak pasti, manakala seni bina privasi Epic tunai memastikan ia adalah telus kepada ancaman sama.

Kebanyakan cryptocurrencies sama dengan Bitcoin, oleh sifat blockchains telus di mana mereka ada, dapat verifiably dikesan melalui setiap dompet di mana mereka telah disimpan. pihak ketiga swasta dan kerajaan sama-sama memantau blockchain Bitcoin dengan cara yang semakin canggih untuk mengenal pasti dengan cepat syiling digunakan dalam aktiviti sebelumnya. Ini secara semulajadi membawa kepada kebimbangan bahawa syiling tercemar mungkin suatu hari nanti diharamkan daripada urus niaga, meninggalkan pemegang niat baik mereka yang berikutnya rugi.

Pada 19 Mac, 2018, Pejabat US Kawalan Aset Asing (OFAC) Mengumumkan ia sedang mempertimbangkan termasuk alamat mata wang digital kepada senarai Warganegara Ditentukan Khas (SDNs), Yang adalah entiti dengan siapa US orang atau perniagaan adalah dilarang untuk menjalankan urusan. Yang lebih merisaukan, yang OFAC tidak menolak kemasukan alamat kini memegang syiling tercemar ke senarai SDN, yang berkesan akan meletakkan pemilik tidak bersalah cryptocurrency tercemar pada senarai hitam jenayah disebabkan oleh gabungan syiling tercemar dimiliki. Ini telah membawa University New York profesor undang-undang, Andrew Hinkes, untuk quip, "mencium fungibility selamat tinggal," dan bahawa orang ramai perlu mengharapkan "premium pada syiling yang baru dicetak, atau syiling bersih dikesan ..."[8].

Dengan perkembangan ini dalam fikiran, ia tidak sukar untuk membayangkan pergolakan dalam pasaran kripto dan penderitaan, atau kepupusan, banyak cryptocurrencies mantap. Walau bagaimanapun, Epic adalah salah satu cryptocurrencies beberapa yang mengelakkan masalah ini sepenuhnya kerana privasi yang kukuh ciri-ciri sebelum ini digambarkan dalam kertas ini. Dengan menghapuskan hubungan antara identiti dan pemilikan, dan hubungan antara pihak-pihak yang menjalankan transaksi, Epic tidak boleh bergabung dengan seseorang atau sesuatu aktiviti. Oleh itu, nilai Epic kekal bebas dari pengguna dan menyediakan ijazah tinggi privasi dan keselamatan yang tidak boleh dengan mudah dimanipulasi oleh pelakon berniat jahat dalam arena jenayah, kewangan, atau politik.

> "... COINS tercemar yang merosakkan. IFANDA BREAK FUNGIBILITY DAN PRIVASI, ANDA BREAK THE CURRENCY."
>
> 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. berskala

Epic Cash ialah MimbleWimble pelaksanaan blockchain yang menghasilkan kemajuan dalam berskala akibat reka bentuk ruang yang cekap yang bangsal data transaksi berlebihan. Yang Memotong fungsi bertanggungjawab ini memberi jaminan bahawa blockchain tumbuh lebih banyak ruang berkesan dari masa ke masa tidak seperti kebanyakan cryptocurrencies, termasuk Bitcoin, dan nod baru boleh diwujudkan dengan pelaburan minimum dalam ingatan dan kuasa pengkomputeran. Dengan baki ruang yang cekap, ia capacitates rangkaian tersebar secara meluas dan menggalakkan desentralisasi. Tambahan lagi, walaupun setiap nod Bitcoin perlu menyimpan keseluruhan rantaian, nodus Epic tunai dapat menyumbang kepada keselamatan rangkaian berdasarkan subset kecil blok.

Kebanyakan cryptocurrencies memerlukan penyimpanan yang tidak terbatas semua data transaksi di blockchains mereka. Rantaian Bitcoin kini memperoleh 0,1353 GB memori setiap hari, manakala kenaikan rantaian Ethereum pada kadar yang lebih cepat daripada 0,2719 GB sehari. Jika rangkaian Bitcoin terus berkembang pada kadar semasa, lama kelamaan ia akan mencapai anggaran 6 TB saiz dengan masa yang blok ganjaran terakhir dilombong pada tahun 2140. Ethereum akan melepasi 10 TB pada tarikh itu[9]. Dalam kebanyakan blockchains tanpa MimbleWimble, transaksi perlu disahkan oleh nod di seluruh dunia. Dengan meningkatnya data, begitu juga beban kepada setiap nod. Walaupun pada hanya 200 GB (saiz anggaran rantaian Bitcoin semasa), penyegerakan data yang memerlukan rangkaian yang stabil dan cakera kelajuan tinggi membaca dan menulis keupayaan.

Akibatnya, perlombongan telah menjadi berpusat di kalangan kumpulan besar memanfaatkan sumber pengkomputeran mahal. Jika seluruh blockchainsejarah Bitcoin adalah untuk disimpan pada Epic tunai blockchain sebaliknya, ia akan dimuatkan ke dalam ruang hampir 90% kurang. **Yang lebih kecil adalah lebih cepat kerana setiap transaksi memerlukan masa yang kurang untuk menghantar dan selamat.**

MimbleWimble menyelesaikan dilema simpanan ini dengan kaedah inovatif blok mencantas, yang disebut sebagai 'Cut-Through'. Untuk memahami bagaimana Potong Melalui kerja-kerja, anda perlu untuk mula-mula melihat bagaimana urus niaga dan blok terdiri dalam blockchain MimbleWimble.

input:

Rujukan kepada output lama;

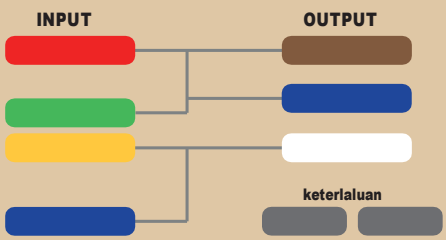
output:

*Transaksi sulit***output dan**rangeproofs**;**

Berlebihan:

Perbezaan antara output dan input, plustandatangan **(Untuk pengesahan dan untuk membuktikan bukan inflasi).**

Rajah 2:
Bahagian transaksi



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

Semua blok Epic tunai mengandungi:

Merkle Trees input transaksi; + Merkle Trees output transaksi dan rangeproofs; + Senarai nilai berlebihan dan tandatangan.

Dalam Rajah 2 dan 3, disesuaikan daripada persembahan Andrew Poelstra ini[10], Kita boleh lihat yang baru dilombong Epic diwakili kerana sel-sel input putih. Sepercaman sel-sel berwarna mewakili output dengan sepadan input dibelanjakan. Dengan proses Cut-Melalui, input dan pemadanan menghabiskan output dikeluarkan untuk mengosongkan ruang dalam blok, yang mengurangkan jumlah data yang perlu disimpan pada blockchain. Manakala urus niaga tidak dimasukkan dalam lejar, biji lebihan baki (hanya 100 bytes) kekal mendokumenkan bahawa urusniaga berlaku.

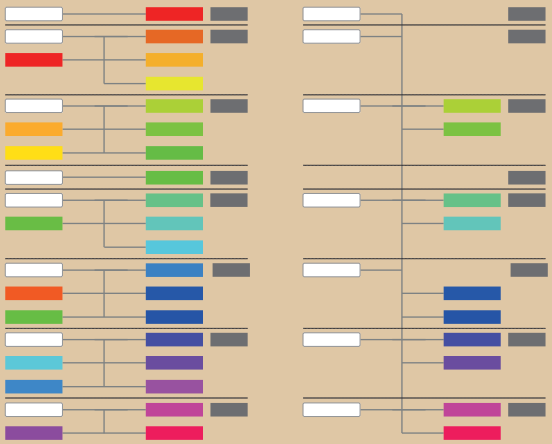
Sebagai blok terus diwujudkan, MimbleWimble digunakan Cut- Melalui blok seluruh, supaya dalam jangka panjang semua yang Jenazah tajuk blok (kira-kira 250 bytes), urus niaga yang tidak dibelanjakan, dan biji transaksi (kira-kira 100 bytes). Grin, pelaksanaan MimbleWimble kedua yang dilancarkan, menunjukkan bahawa rantaian MimbleWimble dengan nombor yang sama transaksi kepada rantaian Bitcoin yang akan menjadi hampir 10% daripada saiz rantaian Bitcoin[11]. Tambahan pula, saiz nod akan "atas perintah beberapa GB untuk rangkaian Bitcoin bersaiz, dan berpotensi optimizable untuk beberapa ratus megabait."[12]

Ini berdiri berbeza sekali dengan Bitcoin, di mana keseluruhan blockchain mesti disimpan oleh setiap nod. Dari masa ke masa, kerana kecekapan ruang daripada blockchain Epic tunai tumbuh relatif kepada blockchain Bitcoin, begitu juga akan kecekapan kos berbanding dengan penyertaan nod dalam rangkaian Epic Tunai. halangan rendah untuk mengambil bahagian membantu memastikan daya tahan penting pada lapisan nod reka bentuk rangkaian.

Melalui pelaksanaannya MimbleWimble dan aplikasi rantaian pemangkasan dengan proses Cut-Through itu, blockchain Epic Cash menawarkan berskala dengan cara sering diabaikan oleh masyarakat cryptocurrency. Ia adalah salah satu yang menangkap intipati Bitcoin dan projek-projek seperti yang berfikiran: buktinya. Tidak kira berapa banyak urus niaga sesaat duit syiling mungkin dapat memproses, apakah gunanya itu jika ia tidak dapat dikekalkan oleh rangkaian yang luas dan pelbagai? Jika keperluan memori adalah seperti itu pengesahan akhirnya gravitates terhadap konglomerat perlombongan kuat, maka semua usaha masyarakat cryptocurrency untuk mewujudkan ekosistem yang berpusat sedang disingkirkan oleh. Untuk mengadakan peruntukan bagi pemprosesan tambahan, gaya Lightning Layer 2 pelaksanaan dirancang sebagai objektif jangka pendek dalam pelan hala tuju pembangunan Epic Tunai.

Rajah 3: MimbleWimble transaksi sebelum dan selepas Cut-Through.

URUSNIAGA PENYIMPANAN YANG DIPERLUKAN



[10] SF Bitcoin Developers, MimbleWimble dengan Andrew Poelstra, 24 November, 2016, https://www.youtube.com/watch?v=aHTRIbCaUyM&t=940s

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

[12] GandalfThePink, Pengenalan kepada Mimblewimble dan Grin, March 28, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Polisi kewangan

Dasar monetari Epic Tunai dan Bitcoin adalah sama. Cash Epicberedar bekalan pertama berkembang dengan pesat dan kemudian menyegerakkan dengan bekalan beredar Bitcoin pada 2028. Ia meningkatkan selepas itu pada kadar yang menurun sehingga mencapaibekalan maksimum 21 juta Epic dalam 2140. Epic Cash mempunyai kualiti untuk menjadi kedai yang selamat nilai jangka panjang kerana bekalan beredar diketahui pada sebarang titik yangpelepasan kitaran hayat dan memuncak dalam bekalan maksimum yang ditetapkan. Epic tunai dasar kewangan mempunyai ciri-ciri yang berikut empat ciri-ciri:

- pelepasan pesat sejak sembilan tahun pertama jangka hayatnya, di mana 20.343.750 Epic (96,875% daripada jumlah penawaran) dikehendaki dilombong. kadar pelepasan yang tepat adalah yang digariskan dalampelepasan jadual seksyen kertas ini;
- Bekalan maksimum 21 juta Epic akan dicapai pada tahun 2140, pada masa yang hampir sama seperti apabila Bitcoin mencapai bekalan maksimum 21 juta unit;
- Epic beredar bekalan dan pelepasan kadar menyegerakkan dengan orang-orang Bitcoin padaSingularity Epic sekitar 24 Mei 2028. Berikutan Singularity, kadar pelepasan berkurangan pada kadar yang semakin meningkat, manakala bekalan beredar tumbuh pada kadar yang berkurangan;
- Epic mempunyai struktur dibagi 8 perpuluhan, yang mana: 1 Epic adalah sama dengan 100,000,000 orang merdeka (seperti 1 Bitcoin adalah sama dengan 100,000,000 Satoshi).

Epic tunai dasar monetari dimodelkan selepas Bitcoin kerana sebab berikut:

- Perjanjian dengan asas-asas ekonomi Bitcoin, iaitu bahawa kekurangan dan kebolehramalan beredar bekalan mendasari kedai yang kukuh ciri-ciri nilai;
- Orang ramai sudah biasa dengan model Bitcoin dan rekod prestasi yang terbukti dalam tempoh sepuluh tahun yang lalu sejak penubuhannya. Oleh kira-kira penyegerakan dengan bekalan beredar Bitcoin, dan mencerminkan bekalan dan dibagi struktur maksimum Bitcoin, Epic mengambil jalan yang kurang rintangan ke arah penggunaan besar-besaran.

VI. Jadual pelepasan

Epic Cash mempunyai sejumlah 33 era perlombongan, setiap ditakrifkan oleh penurunan dalam ganjaran blok, Berbanding dengan era sebelumnya mereka. yang Epic Kejadian, Tarikh Epic blok # 1 dilombong, berlaku pada Ogos, 2019. Blok dilombong di satu per minit. Yang pertama lima era menghasilkan hampir 97% daripada bekalan maksimum Epic, yang hampir sama 20 tahun pelepasan Bitcoin dalam kira-kira sembilan tahun. Ini boleh dianggap sebagai satu peluang untuk 'kembali jam' bagi mereka yang terlepas kenaikan menakjubkan Bitcoin.

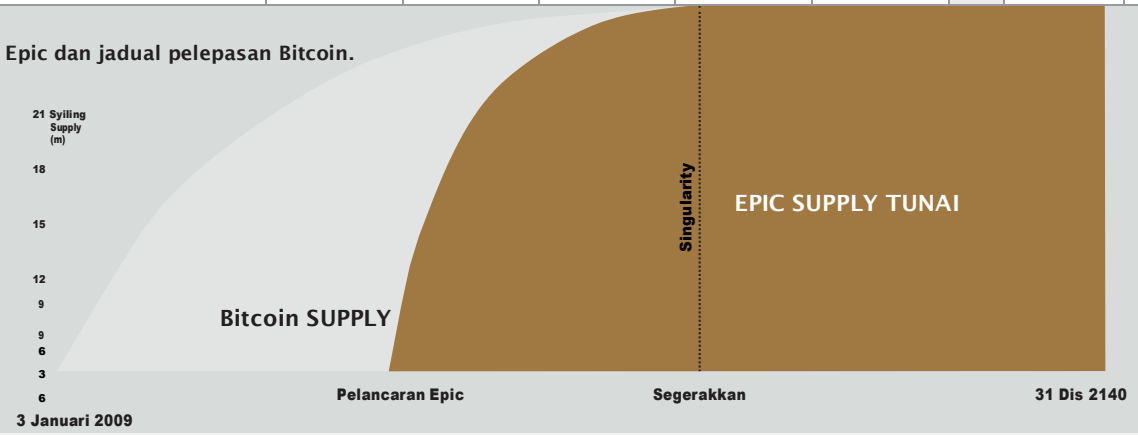
Jadual pelepasan dalam jadual 1 menggariskan mula dan tamat tarikh tujuh era pertama perlombongan, ganjaran blok sama mereka, dan yang berikutnya beredar bekalan bagi setiap era. Era 8-33 tidak termasuk dalam jadual untuk singkatnya. Bagi mereka era, ia sudah memadai untuk memahami bahawa setiap era berikutnya akan mempunyai ganjaran blok iaitu separuh jumlah pahala era sebelumnya, betul-betul seperti dalam Bitcoin. Jumlah Epic dipancarkan pada setiap era ini akan menjadi jumlah ganjaran blok dalam era 4 tahun (anggaran 1460 hari).

Di Epic Singularity (2028), yang beredar bekalan Epic bersilang jumlah bekalan beredar Bitcoin ini, di mana titik Epic tunai mengamalkan blok ganjaran Bitcoin dan pengurangan separuh corak, yang melihat ganjaran blok menurun sebanyak separuh setiap empat tahun. Satu-satunya pengecualian adalah yang menghalang Epic terus dilombong pada kadar masing-masing satu minit, berbanding kadar Bitcoin ini satu blok setiap sepuluh minit. Dengan cara ini, beredar bekalan Epic mengekalkan pariti anggaran dengan bekalan beredar Bitcoin untuk baki kewujudan mereka.

Jadual 1: Jadual emisi bagi tujuh era perlombongan pertama. Tarikh adalah anggaran rapat.

Zaman	1	2	3	4	5	Singularity	6	7
blok Ganjaran	16	8	4	2	1		0,15625	0.078125
Tarikh mula	Ogos 1, 2019	Jun 29, 2020	Okt 11, 2021	Jun 3, 2023	Ogos 10, 2025		Mei 24, 2028	Mei 22, 2032
Tarikh tamat	Jun 29, 2020	Okt 11, 2021	Jun 3, 2023	Ogos 10, 2025	Mei 24, 2028		Mei 22, 2032	20 Mei 2036
Panjang (dalam hari)	334	470	601	800	1019		1460	1460
bermula Supply	0	7.695.360	13.109.760	16.571.520	18.875.520		20.342.880	20.671.380
akhir Supply	7.695.360	13.109.760	16.571.520	18.875.520	20.342.880		20.671.380	20.835.630
% Daripada Supply maksimum	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Rajah 4: Epic dan jadual pelepasan Bitcoin.



VII. perlombongan

The blockchain Epic tunai mengejar buktinya oleh mengalu-alukan pelbagai perkakasan pengiraan. perlombongan Epic pada awalnya disediakan untuk CPU,GPUs, dan ASIC, Dengan menggunakan tiga masing-masing hashing algoritma: RandomX, ProgPow dan CuckAToo31 +. Algoritma boleh trivially panas bertukar tanpa menjejaskan integriti rantai.

1 RandomX dan CPU

RandomX ialah Bukti-of-Work (POW) algoritma dioptimumkan untuk CPU kegunaan umum. Ia menggunakan hukuman mati program rawak dengan beberapa memori-keras teknik untuk mencapai matlamat berikut:

- **Pencegahan pembangunan ASIC cip tunggal;**
- **Mengurangkan kelebihan kecekapan perkakasan khusus lebih CPU kegunaan umum.**

Perlombongan Epic dengan CPU memerlukan peruntukan berdampingan 2 GB fizikal Ram, 16 KB L1 cache, 256 KB L2 cache, dan 2 MB cache L3 setiap thread13 perlombongan. Windows 10 peranti memerlukan 8 GB atau lebih RAM. Ia tidak mustahil bahawa satu hari di tidak terlalu jauh telefon mudah alih masa depan boleh menjadi nod perlombongan berdaya maju. Awal integrasi CPU dalam rangkaian perlombongan Epic Tunai adalah satu peluang yang baik untuk banyak dengan hanya pengkomputeran sederhana bermakna untuk mendapat ganjaran blok dengan membantu untuk menjamin rangkaian Epic Tunai.

2 ProgPow dan GPUs

Perancangan Bukti-of-Work (ProgPow) Adalah satu algoritma yang bergantung kepada lebar jalur memori dan pengiraan teras urutan matematik rawak, yang mengambil kesempatan daripada banyak ciri-ciri pengkomputeran GPU dan dengan itu cekap menangkap kos tenaga sejumlah perkakasan. Sebagai ProgPow direka khusus untuk mengambil kesempatan penuh daripada GPUs komoditi, ia adalah kedua-dua sukar dan mahal untuk mencapai kecekapan yang lebih tinggi melalui perkakasan khusus. Oleh itu, algoritma ProgPow yang mengurangkan insentif untuk kolam ASIC besar untuk outcompete GPUs, seperti yang sering dilihat dengan banyak algoritma PoW lain, seperti Bitcoin SHA-256. GPUs, walaupun tidak seperti yang lazim seperti CPU, masih yang biasa terdapat. Dengan perkembangan teknologi didorong oleh kuasa besar, Nvidia dan AMD, GPUs dapat selari proses banyak gandaan penyelesaian perlombongan di atas CPU secara seunit. Ia adalah disebabkan oleh gabungan ini sentiasa ada dan kuasa pemprosesan yang tinggi yang GPUs akan menyediakan tulang belakang kepada banyak aktiviti perlombongan semasa era awal, seperti yang ditunjukkan dalam Jadual 2.

3 CuckAToo + 31 dan ASIC

CuckAToo31 + adalah atur mesra ASIC algoritma Cuckoo Cycle dibangunkan oleh saintis komputer Belanda, John Tromp. A relatif tahan ASIC CuckARoo29, CuckAToo31 + menjana rawak graf bipartit dan membentangkan pelombong dengan tugas mencari gelung diberi panjang 'N' melalui mercu graf itu.

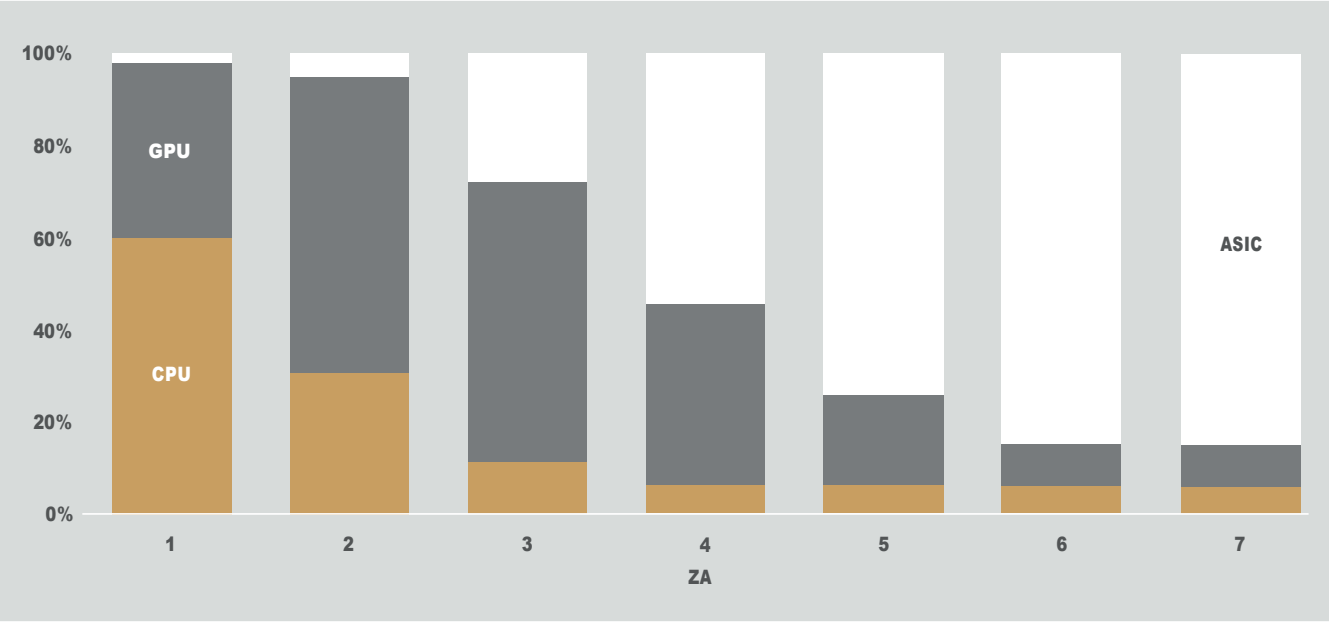
[13] Tevador, *RandomX*, 28 March, 2019, https://github.com/tevador/RandomX

Ini adalah satu tugas memori terikat, bermakna masa penyelesaian adalah terikat dengan bandwidth memori bukannya pemproses mentah atau kelajuan GPU. Hasilnya, algoritma Cuckoo Kitaran menghasilkan kurang haba dan menggunakan tenaga yang kurang daripada algoritma PoW tradisional. The CuckATоo31 friendly ASIC + membolehkan peningkatan kecekapan lebih GPUs dengan menggunakan beratus-ratus MB SRAM manakala selebihnya bottlenecked oleh memori I / O[14]. Akhirnya, ASIC menawarkan ekonomi besar potensi skala tiga pilihan perlombongan. Demi kepentingan keterangkuman, bagaimanapun, walaupun mereka diperuntukkan sebahagian kecil ganjaran perlombongan berbanding dengan CPU dan GPU awal, akhirnya ASIC menganggap kepentingan majoriti daripada ganjaran blok dilombong, pada andaian akan ada ekosistem yang berdaya saing pengeluar peranti untuk CuckATоo31 +.

Jadual 2: Mining pemberian ganjaran. Tertakluk kepada semakan. Pemberian akan diarahkan untuk mencapai desentralisasi maksimum dan selaras dengan kepentingan jangka panjang rangkaian.

Zaman	1	2	3	4	5	6	7
hari	334	470	601	800	1019	1460	1460
CPU	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASIC	2%	5%	28%	55%	75%	85%	85%

Rajah 5: ganjaran Mining pemberian bagi setiap era mengikut Jadual 2. Tertakluk kepada semakan.



[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 Sumbangan perlombongan

Bermula pada Epic Kejadian (2019) dan menyimpulkan di Epic Singularity (2028), semasa proses perlombongan, terdapat peruntukan sebanyak Epic yang diarahkan, kerana sumbangan perlombongan, ke arah Blockchain Foundation EPIC.

The EPIC Blockchain Foundation adalah khusus untuk pembangunan teknikal dan kesedaran menggalakkan dan kebergunaan projek Epic tunai semasa tahun-tahun awal penubuhannya, dengan mewujudkan aktiviti pemasaran dan membangunkan perkongsian dalam industri teknologi kewangan.

Selepas Singularity, peranan EPIC Yayasan akan diambil alih oleh EPIC yang Diedarkan Autonomous Corporation (Edac), yang akan dibangunkan oleh yayasan itu sebelum penyerahan.

The EPIC Blockchain Yayasan dibiayai oleh peratusan ganjaran perlombongan, ditolak daripada ganjaran blok, mengikut kadar tahunan seperti berikut:

Jadual 3: Kadar Tahunan bagi sumbangan perlombongan Yayasan sebagai peratusan ganjaran perlombongan.

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

VIII. kesimpulan

matlamat epik untuk diiktiraf sebagai 'perak digital berpusat', medium pertukaran rakan ke kedudukan Bitcoin yang diiktiraf sebagai emas digital terpencar. Dengan memperkenalkan semula hilang fungibility pada yang lebih cekap tenaga dan mesra alam tulang belakang perkakasan, Epic tunai tilts baki kembali kuasa yang memihak kepada pengguna individu, berbeza sekali dengan trend pemusatan baru-baru ini. Gabungan Bitcoin ekonomi, teori permainan dan terbukti bukti-of-kerja formula dengan yang terbaik daripada hasil teknologi blockchain kontemporari dalam yg tak dpt dipercaya, tidak berubah, dan mata wang tidak berpusat (Epic) yang berskala, fungible, dan yang melindungi privasi yang pengguna. The blockchain Epic tunai terbuka, awam, sempadan, dan penapisan tahan. Ia mengekalkan privasi dan kekayaan penggunanya dan ganjaran kepada mereka yang menggunakan perkakasan mereka bagi menyokong rangkaian melalui perlombongan. Setiap Epic dilombong wujud melalui bukti kerja. Supply bermula pada sifar dan rangkaian tidak adil dilancarkan, dengan testnet berfungsi kini berjalan.

Epic Fakta Key Tunai:

- Perlombongan bermula Ogos 2019.
- The blockchain Epic wang tunai berdasarkan MimbleWimble.

  ciri-ciri yang menentukan protokol ialah:

  1. Memotong**- penyingkiran maklumat berlebihan daripada blockchain untuk menggalakkan kecekapan ruang, menggalakkan penyertaan skala luas dalam pengesahan rangkaian, dan buktinya pramugara;**
  2. *CoinJoin*- **penggabongan transaksi di dalam blok untuk memastikan fungibility daripada cryptocurrency Epic itu;**
  3. *Dandelion ++ Protokol*- **penyebaran transaksi dengan berkomunikasi di seluruh saluran saling berkaitan, dan meresap di seluruh rangkaian yang luas, nod, memutuskan hubungan antara urus niaga dan asal-usul mereka;**
  4. No Alamat Wallet**- penggunaan yang multisignature besar untuk menjana sekali guna kunci peribadi untuk transaksi pihak, menghapuskan keperluan untuk wallet menangani sepenuhnya.**

- Epic tunai dasar kewangan**direka untuk menyegerakkan beredar bekalan Epic dengan bekalan beredar Bitcoin dalam kira-kira sembilan tahun, dan mencapai bekalan maksimum yang sama 21 juta unit pada masa yang sama seperti Bitcoin, pada tahun 2140. Ini decreasingly inflasi jaminan dasar ketelusan, kebolehramalan bekalan, dan kekurangan, memupuk keselamatan simpanan nilai jangka panjang.**

- perlombongan**yang menggabungkan CPU, GPU, dan ASIC melalui sepadan RandomX, ProgPow dan CuckAToo31 + algoritma, untuk memudahkan penggunaan besar-besaran dan keberkesanan rangkaian.**

IX. Spesifikasi teknikal

Nama Projek: Cash
EpicMata wang Nama:
Epic Sekat Masa: 60
saat Block Saiz: 1 MB
Supply Bermula: 0
Supply Akhir: 21,000,000
Kejadian blok: 1 Ogos 2019
konsensus: RandomX (CPU), ProgPow (GPUs) dan CuckAToo31 + (ASIC)

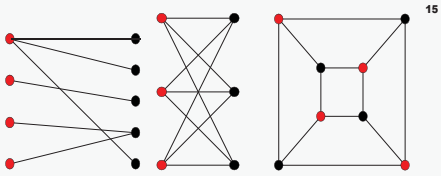
Links:

www.epic.tech

t.me/EpicCash - Telegram

t.me/EpicCashBahasaMalaysia

X. Glosari

ASIC	Permohonan Litar Bersepadu tertentu; cip yang direka untuk tujuan tunggal
bipartit Graph	satu set mercu Graf dihuraikan kepada dua set tak berkait itu bahawa tiada dua mercu Graf dalam set yang sama adalah bersebelahan.  [15]
pembutaan Factor	elemen rawak diperkenalkan ke dalam mesej digital untuk memudahkan penyulitan; rahsia dikongsi di antara kedua-dua pihak yang menyulitkan input dan output dalam bahawa transaksi tertentu serta pihak-pihak transaksi 'keys16 awam dan swasta.
blok Ganjaran	Epic baru diedarkan oleh rangkaian sebagai ganjaran untuk pengiraan dilakukan untuk mengesahkan transaksi di dalam sebuah blok baru.
cache	perkakasan atau perisian komponen yang menyimpan data supaya permintaan masa hadapan bagi data yang boleh disampaikan dengan lebih cepat.
beredar Supply	jumlah Epic wujud pada titik tertentu dalam masa.
CPU	Unit Pemprosesan Pusat: komponen komputer bertanggungjawab mentafsir dan melaksanakan sebahagian besar daripada arahan daripada perkakasan dan perisian lain komputer.
Memotong	proses blockchain MimbleWimble mana input dan pemadanan menghabiskan output dikeluarkan untuk mengosongkan ruang dalam blok, mengurangkan jumlah data yang diperlukan untuk disimpan pada blockchain.
buktinya	keadaan penyebaran operasi dan tadbir urus yang rangkaian.
Pelepasan	penciptaan Epic baru yang diperolehi oleh pelombong dalam ganjaran blok. Epic dicipta setiap 60 saat sebagai transaksi disahkan ke dalam blockchain.
Epic Singularity	titik di mana bekalan beredar Epic menyelaras dengan bekalan beredar Bitcoin (Mei 2028).
Berlebihan (MimbleWimble)	perbezaan antara output dan input, ditambah tandatangan (untuk pengesahan dan untuk membuktikan bukan inflasi).
Fungibility	harta yang baik atau komoditi di mana unit-unit individu pada dasarnya boleh ditukar ganti, dan setiap daripada bahagian-bahagiannya tidak dapat dibezakan dari sebahagian yang lain.
Kejadian (Event)	perlombongan blok Epic pertama dan penubuhannya rasmi blockchain.
GPU	Unit Pemprosesan Grafik: Satu unit yang mengandungi cip logik boleh atur cara (pemproses) khusus untuk fungsi paparan. GPUs pengguna boleh menjadi sangat sesuai untuk perlombongan cryptocurrency.
Pengurangan separuh (untuk Bitcoin)	berlaku setiap 4 tahun. Kadar bekalan berkurangan sebanyak 50% selepas setiap acara pengurangan separuh. nilai dikira dari beberapa input asas menggunakan fungsi hashing.
hash	algoritma matematik yang memetakan data saiz sewenang-wenangnya kepada olahan saiz yang tetap digunakan untuk menjana dan mengesahkan tandatangan digital, mesej pengesahan kod (Mac), dan lain-lain bentuk pengesahan.
Hashing Algoritma (fungsi)	kaedah melaksanakan pengiraan maklumat disulitkan tanpa decrypting terlebih dahulu. (Dalam pengaturcaraan) negeri di mana objek tidak boleh diubah selepas penciptaannya.
penyulitan Homomorphic	komponen transaksi MimbleWimble mewakili parti itu menghantar transaksi; dicipta dari output transaksi sebelumnya.
ketetapan	input / output; komunikasi antara sistem pemprosesan maklumat, seperti komputer, dan dunia luar, mungkin manusia atau sistem pemprosesan maklumat.
Input (MimbleWimble)	
I / O	

[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/

Maksimum Supply	jumlah Epic untuk dihubungi di mana titik bekalan beredar tidak akan meningkat selepas itu (21,000,000 Epic).
Memory-Hard	penggunaan banyak RAM untuk menghalang sambungan serentak berjalan percubaan secara selari. fungsi memori-keras algoritma yang mempunyai masa pengiraan terutamanya diputuskan oleh memori yang tersedia untuk memegang data. Juga dikenali sebagai fungsi memory-terikat.
Merkle Tree	struktur data yang digunakan dalam aplikasi sains komputer. Dalam blockchains, pokok Merkle membolehkan pengesahan cekap dan selamat daripada kandungan dalam struktur data yang besar.
MimbleWimble	yangprotocolyang dikemukakan oleh penyumbang samaran, melihat kepada moniker Tom Elvis Jedusor, dalam chatroom yang Bitcoin pemaju.
Multisignature	skim tandatangan digital yang membolehkan sekumpulan pengguna untuk menandatangani satu dokumen. Biasanya, algoritma multisignature menghasilkan tandatangan bersama yang lebih padat daripada koleksi tandatangan berbeza daripada semua users17.
nod	komputer yang bersambung dengan rangkaian blockchain dan cawangan kepada nod lain dalam rangkaian untuk mengedarkan maklumat mengenai urus niaga dan blok, dengan cara peer-to-peer.
One Way Agregat Signature (OWAS)	tandatangan transaksi terdiri daripada banyak tandatangan yang disulitkan dengan cara yang supaya ia adalah amat sukar untuk mengira tandatangan individu yang merupakan sebahagian daripada agregat.
Output Skim Komitmen	komponen transaksi MimbleWimble mewakili penerimaan transaksi; digunakan sebagai input untuk transaksi berikutnya.
(MimbleWimble) Pedersen	primitif kriptografi yang membolehkan prover untuk melakukan kepada nilai yang dipilih tanpa mendedahkan apa-apa maklumat mengenainya dan tanpa prover yang dapat membatalkan komitmen untuk nilai.
Kunci peribadi	kunci persendirian adalah sedikit kecil kod yang dipasangkan dengan kunci awam untuk menolak algoritma untuk penyulitan teks dan penyahsulitan. Ia dicipta sebagai sebahagian daripada kriptografi kunci awam semasa penyulitan kunci asymmetric- dan digunakan untuk menyahsulit dan mengubah mesej kepada format yang boleh dibaca.
Bukti Work (PoW)	sekeping data yang sukar (mahal dan memakan masa) untuk menghasilkan, tetapi mudah bagi orang lain untuk mengesahkan, dan yang memenuhi syarat-syarat tertentu. Bukti Kerja sering digunakan dalam generasi blok cryptocurrency.
Kunci awam	kunci awam dicipta di khalayak ramai kriptografi penyulitan kunci yang menggunakan algoritma penyulitan simetri utama. Kekunci umum digunakan untuk menukar mesej ke dalam format yang boleh dibaca.
RAM (Random Access Memory)	pantas akses cip penyimpanan data dalam peranti pengkomputeran di mana sistem operasi (OS), program aplikasi dan data digunakan semasa disimpan supaya ia boleh dengan cepat dicapai oleh pemproses peranti.
Rangeproof	pengesahan komitmen yang mengesahkan bahawa hasil tambah input transaksi adalah lebih besar daripada jumlah output transaksi dan bahawa semua nilai transaksi adalah positif. Rangeproofs memastikan bekalan kewangan tidak diganggu.
(Tandatangan digital	sebahagian standard protokol blockchain, terutamanya digunakan untuk mendapatkan urus niaga dan blok urus niaga, transferral maklumat, pengurusan kontrak dan mana-mana kes-kes lain di mana mengesan dan mencegah sebarang pengubahan luaran adalah penting. Mereka menyediakan tiga kelebihan menyimpan dan memindahkan maklumat mengenai blockchain: • Mereka mendedahkan jika data yang dihantar telah diganggu; • Mengesahkan penyertaan parti tertentu dalam urus niaga; • Boleh menjadi undang-undang yang mengikat.
SRAM (Static Random Access Memory)	Random Access Memory (RAM) yang mengekalkan bit data dalam ingatan selagi kuasa yang dibekalkan.
Kendalian	ukuran transaksi sesaat yang boleh dilakukan oleh protokol cryptocurrency diberikan.
Trustlessness	kualiti rangkaian cryptocurrency mematuhi peraturan protokol tanpa penguatkuasaan oleh pihak pusat.

[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

TUNAI EPIC

EPIC PRIVATE TUNAI INTERNET