Freeman Family

4 Juli 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

Sistem Cash Elektronik yang *Peer-to-Peer*

PENYIMPAN NILAI + ALAT TUKAR + SATUAN HITUNG

1,7 miliar orang dewasa tidak memiliki akses ke sistem keuangan global, sementara 1,3 miliar lainnya tidak terlayani. Epic Cash membuka Potensi manusia dengan menghubungkan individu ke pasar global. Dengan transaksi yang Cepat, menghampiri "gratis" untuk digunakan, dan terbuka untuk semua kalangan.

Version 7.1b **Indonesian**

Konten

II. Privasi

Penggunaan uang modern dapat dipahami sebagai peralihan kolektif dari unit-unit akun antara orang dan institusi. pandangan terhadap uang pada suatu titik waktu tertentu dapat dipetakan dengan menjawab pertanyaan-pertanyaan berikut:

1. *Siapa yang memegangnya, dan berapa banyak yang mereka pegang?*
2. *Siapa yang bertransaksi dengan siapa, dan berapa banyak?*

Untuk mata uang fiat tradisional, dan bahkan Bitcoin juga, kami dapat menjawab pertanyaan-pertanyaan itu. Dalam melakukan hal itu, banyak yang dapat diungkapkan tentang kehidupan orang-orang, seperti pola konsumsi, kepemilikan, dan mitra pengimbang transaksional. Kesimpulan yang cukup akurat dapat ditarik tentang minat dan niat individu dengan melacak transfer pada nilai. Tanpa privasi, data transaksi dapat menjadi informasi berbahaya di tangan pihak ketiga yang buas.

Penggunaan cryptocurrency selama dekade terakhir menunjukkan rangkaian kesatuan "privasi" dalam berbagai implementasi blockchain. Skala privasi, harus dipertimbangkan, berkisar dari yang terbuka dan terkenal di satu sisi ke anonim pada yang lainnya. Saat privasi terkikis, satu landasan penting dari cryptocurrency, "tanpa kepercayaan", akan menurun. Sebagaimana dibuktikan oleh keberhasilan layanan analisis blockchain Bitcoin, Bitcoin berada lebih ke terkenal transparan (buruk) di akhir spektrum privasi. Pengguna harus semakin mengambil langkah-langkah untuk memastikan mereka secara tidak sengaja bertransaksi dalam Bitcoin yang terkontaminasi. Solusi Epic Cash mengarah ke anonim dan mengembalikan properti penting ini dengan memastikan bahwa privasi individu dan privasi transaksi direkayasa ke dalam sistem pada tingkat yang mendasar.

Privasi Identitas

Privasi Transaksi

Privasi Identitas

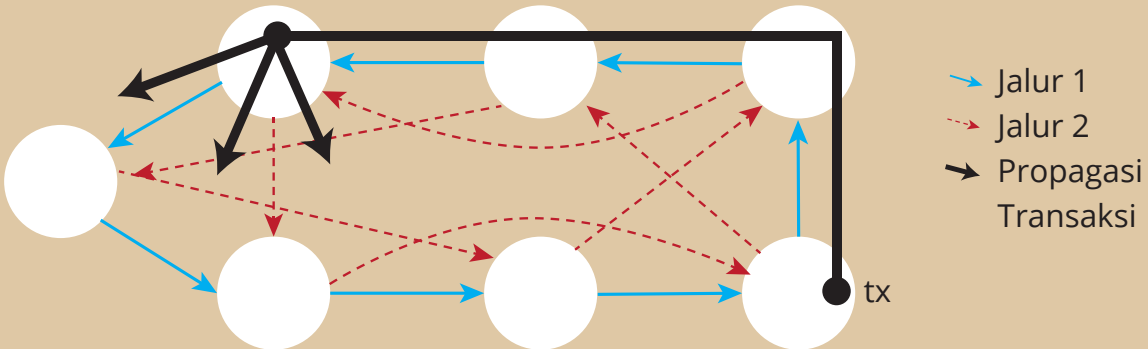
Sebagian besar cryptocurrency seperti Bitcoin disimpan di dompet yang alamatnya merujuk pada *public key* yang berasal dari private key dompet. Alamat-alamat ini dapat dianggap sebagai pelacak ruang pribadi seseorang di dunia digital. Blockchain Epic Cash menghilangkan alamat seluruhnya dan sebagai gantinya menerapkan satu *multisignature* yang besar dari mana semua *public key* dan *private* dihasilkan berdasarkan penggunaan tunggal.

Karena alamat dompet Bitcoin adalah pelacak ruang di dunia digital, dompet itu dapat dilacak ke alamat Internet Protocol (IP) pemilik, yang mengarahkan pemiliknya ke komputer di lokasi yang unik pada titik waktu tertentu. Secara sederhana dijelaskan: ketika transaksi Bitcoin terjadi, transaksi disiarkan dari hub komunikasi yang disebut 'node' dan kemudian disebarkan ke node lain yang disebut *'peer'*. Informasi itu kemudian dengan cepat menyebar ke masing-masing node *peer* secara berurutan di seluruh jaringan. Proses ini secara tepat dinamai "*Gossip Protocol*". Sederhananya, setiap Bitcoin memiliki posisi online yang terlihat dan lokasi fisik di mana Bitcoin, atau lebih tepatnya pemilik Bitcoin, dapat ditemukan. Seperti yang dicatat oleh jurnalis Grace Caffyn, Bitcoin "tidak ada lagi rahasia , dibandingkan pencarian Google dari koneksi internet di rumah."[2]

Selain menghilangkan alamat dompet, blockchain Epic Cash mengamankan privasi identitas dengan memastikan alamat IP tidak dapat dilacak. Ini dilakukan melalui integrasi ***Dandelion ++ Protocol***. Memperbaiki pendahulunya, ***Dandelion Protocol*** asli, ***Dandelion ++ Protocol*** adalah hasil dari kerja tujuh peneliti yang berkelanjutan untuk memerangi serangan deanonimisasi pada blockchain. Melalui ***Dandelion ++***, transaksi dilewatkan melalui jalur tersimpul yang acak, atau 'kabel', dan kemudian tiba-tiba menyebar ke jaringan besar dari node, seperti kelopak bunga Dandelion ketika ditiup dari batangnya (Gambar 1). ia membuat hampir mustahil untuk melacak transaksi kembali ke asalnya, dan tentunya pada alamat IP asalnya.

Gambar 1: Menganonimkan transaksi dengan *Dandelion++ Protocol.*

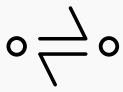
Dandelion++ meneruskan pesan melalui salah satu dari dua jalur yang saling terkait pada grafik reguler-4, kemudian disiarkan menggunakan difusi. Dalam gambar, transaksi merambat di atas jalur solid biru3. Proses ini membuatnya sangat sulit untuk melacak transaksi kembali ke sumbernya, sehingga dapat menjaga 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

[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

Privasi Transaksi



Blockchain Epic Cash menjamin privasi transaksi dengan mengaburkan jumlah dan hubungan pengirim ke penerima dari suatu transaksi. hal Ini dicapai melalui penerapan ide-ide yang familiar dari ***Confidential Transactions (CT)***[4] dan ***CoinJoin***[5], metode yang sebagian besar dikembangkan oleh Gregory Maxwell (Bitcoin Core developer, Co-Founder dan CTO dari Blockstream).

CT, awalnya dibuat oleh Adam Back kemudian disempurnakan oleh Maxwell, bekerja dengan memecah transaksi menjadi bagian-bagian yang lebih kecil melalui *homomorphic encryption*, sebuah metode melakukan perhitungan pada informasi yang dienkripsi tanpa mendekripsi terlebih dahulu untuk menjaga privasi. Setelah dibagi, pengamat tidak dapat melihat jumlah sebenarnya dari transaksi karena *faktor blinding* , sebuah sistem yang melemparkan angka acak ke dalam campuran fragmen transaksi untuk menyembunyikan nilai-nilai fragmen tersebut. Pada akhirnya, hanya pihak yang bertransaksi yang tahu nilai pertukaran, sementara transaksi diverifikasi oleh jaringan melalui konfirmasi bahwa jumlah nilai output sama dengan jumlah nilai input, dan jumlah output faktor *blinding* sama dengan jumlah input faktor *blinding*.

Untuk semakin memperumit tugas yang privat, semua transaksi Epic Cash diselubungi dengan ***CT*** dan kemudian dicampur bersama untuk menyembunyikan koneksi antara pihak yang bertransaksi. Ini dilakukan melalui konsep kedua Maxwell, ***CoinJoin***.

Untuk mengilustrasikan ***CoinJoin*** secara sederhana, bayangkan A, B, dan C masing-masing mengirimkan Epic ke X, Y dan Z. Dikirim melalui media ***CoinJoin***, semua yang diketahui adalah bahwa A, B dan C sedang mengirim dan X, Y dan Z menerima, sementara jumlah transaksi tetap tidak terlihat. Sistem CoinJoin sangat penting bagi Epic Cash melalui *One-Way Aggregate Signatures (OWAS)*, yang menggabungkan semua transaksi di dalam blok menjadi satu transaksi.

Privasi: Rangkuman

Blockchain Epic Cash melindungi privasi individu dan transaksi mereka dengan:

- ***Menghilangkan alamat dompet*** – **Tidak ada pengidentifikasi lokasi untuk brankas digital di dalam blockchain. Transaksi dibangun langsung dari orang ke orang berbasis dompet ke dompet;**
- ***Dandelion++ Protocol*** – **mengaburkan jalur digital transaksi dari alamat IP transaksi pengirim;**
- ***Transaksi yang Rahasia*** – **membagi transaksi menjadi beberapa bagian dan memasukkan - faktor *blinding* ke dalam kumpulan potongan-potongan itu, sehingga nilai-nilai dari potongan-potongan dan parameter transaksi lainnya tidak dapat diketahui;**
- ***CoinJoin*** – **menggabungkan transaksi ke dalam bundel untuk menutupi hubungan antara pihak yang bertransaksi.**

[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. Kesetaraan

Charlie Lee, pencipta Litecoin, menyatakan bahwa kesetaraan adalah satu-satunya properti dari komoditas yang hilang dari Bitcoin dan Litecoin, mengakui bahwa privasi dan kesetaraan adalah medan pertempuran berikutnya untuk koin-koin itu[6]. Andreas Antonopoulos, salah satu pakar blockchain terkemuka di dunia, mengklaim bahwa "... koin yang tercemar bersifat merusak. Jika Anda melanggar Kesetaraan dan privasi, maka Anda melanggar mata uang."[7]

Kesetaraan adalah properti dari sekumpulan barang atau aset yang memastikan unit individu dari set tersebut bernilai sama dan dapat dipertukarkan. Inilah yang membedakan bentuk mata uang paling awal dari sistem barter mereka yang terdahulu. Tanpa kepercayaan akan uang yang dapat dipertukarkan, uang dengan cepat kehilangan kegunaannya. Seperti yang akan diilustrasikan di bawah ini, kesetaraan dari sebagian besar cryptocurrency tidak pasti, sedangkan arsitektur privasi Epic Cash memastikannya kebal terhadap ancaman yang sama.

Sebagian besar cryptocurrency mirip dengan Bitcoin, dengan sifat blockchain transparan di mana mereka berada, dapat dilacak secara diverifikasi melalui setiap dompet tempat mereka disimpan. Pihak ketiga privat dan pemerintah sama-sama memantau blockchain Bitcoin dengan cara yang semakin canggih untuk dengan cepat mengidentifikasi koin yang digunakan dalam kegiatan sebelumnya. Hal ini tentu saja menimbulkan kekhawatiran bahwa koin yang terkontaminasi suatu hari nanti mungkin dilarang pada transaksi, sehingga pemegang dengan niat yang baik mereka yang berikutnya rugi.

Pada tanggal 19 Maret 2018, *U.S. Office of Foreign Asset Control* (OFAC) mengumumkan bahwa ia sedang mempertimbangkan untuk memasukkan alamat mata uang digital pada *Specially Designated Nationals* (SDN) , yang merupakan entitas yang dilarang oleh orang atau bisnis AS untuk melakukan transaksi. Yang lebih meresahkan, OFAC belum mengesampingkan pencantuman alamat yang saat ini memegang koin terkontaminasi ke dalam daftar SDN, yang secara efektif akan menempatkan pemilik mata uang kripto yang tidak bersalah berada pada daftar hitam kriminal karena afiliasi koin tercemar yang dimiliki. hal Ini telah mendorong profesor hukum Universitas New York, Andrew Hinkes, untuk menyindir, "selamat tinggal kesetaraan," dan bahwa masyarakat harus mengharapkan "sesuatu yang premium pada koin yang baru dicetak, atau menelusuri koin yang murni..."[8].

Melalui perkembangan ini, tidak sulit untuk membayangkan kehebohan di pasar crypto dan kesengsaraan, atau bahkan kepunahan, dari banyak cryptocurrency yang telah mapan. Namun, Epic adalah salah satu dari sedikit cryptocurrency yang menghindari masalah ini sepenuhnya karena fitur privasi yang kuat , yang dijelaskan sebelumnya dalam paper ini. Dengan menghapus tautan antara identitas dan kepemilikan, dan hubungan antara pihak-pihak yang bertransaksi, Epic tidak pernah dapat berafiliasi dengan seseorang atau suatu kegiatan. Dengan demikian, nilai Epic tetap independen dari penggunanya dan memberikan privasi dan keamanan tingkat tinggi , yang tidak dapat dengan mudah dimanipulasi oleh kriminal, finansial, atau arena politik.

> **“...KOIN TERKONTAMINASI SIFATNYA MERUSAK. JIKA ANDA MELANGGAR KESETARAAN DAN PRIVASI, MAKA ANDA MELANGGAR MATA UANG.”**
>
> **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. Skalabilitas

Epic Cash adalah implementasi blockchain MimbleWimble yang menghasilkan kemajuan skalabilitas sebagai hasil dari desain ruang yang efisien yang melepaskan data transaksi yang berlebihan. Fungsi *Cut Through* yang bertanggung jawab untuk hal ini memastikan bahwa blockchain menumbuhkan lebih banyak ruang efisien dari waktu ke waktu tidak seperti kebanyakan cryptocurrency, termasuk Bitcoin, dan bahwasannya, node baru dapat dibuat dengan investasi yang minimal pada memori dan daya komputasi. Dengan tetap efisien dalam ruang, ia meningkatkan kapasitas jaringan yang tersebar luas dan mendorong desentralisasi. Selain itu, ketika setiap node Bitcoin harus menyimpan seluruh rantai, maka node Epic Cash dapat berkontribusi untuk keamanan jaringan berdasarkan pada sebagian kecil blok.

Sebagian besar cryptocurrency memerlukan penyimpanan tidak terbatas dari semua data transaksi pada blockchain mereka. Rantai Bitcoin saat ini memperoleh 0,1353 GB memori per hari, sementara rantai Ethereum meningkat pada tingkatan yang lebih cepat lagi yaitu 0,2719 GB sehari. Jika rantai Bitcoin terus tumbuh pada tingkat saat ini, pada akhirnya akan mencapai sekitar 6 TB pada saat blok reward terakhir ditambang pada tahun 2140. Ethereum akan melampaui 10 TB pada tahun tersebut[9]. Di sebagian besar blockchains tanpa MimbleWimble, transaksi harus diverifikasi oleh node di seluruh dunia. Ketika data meningkat, demikian juga beban pada setiap node. Bahkan hanya 200 GB (ukuran perkiraan rantai Bitcoin saat ini), menyinkronkan data memerlukan jaringan yang stabil dan kemampuan *read* (membaca) dan *write* (menulis) berkecepatan tinggi pada disk.

Akibatnya, penambangan menjadi semakin terpusat di antara *pool* besar yang memanfaatkan sumber daya komputasi yang mahal. **Jika seluruh riwayat blockchain Bitcoin disimpan di blockchain Epic Cash, ia akan masuk ke dalam ruang yang hampir 90% lebih sedikit.** Lebih kecil akan membuatnya lebih cepat karena setiap transaksi membutuhkan sedikit waktu untuk mengirim dan mengamankan.

MimbleWimble memecahkan dilema penyimpanan ini dengan metode inovatif pada pemangkasan blok, yang disebut sebagai '*Cut-Through*'. Untuk memahami bagaimana *Cut-Through* bekerja, yang terbaik adalah pertama-tama melihat bagaimana transaksi dan blok disusun dalam blockchain MimbleWimble.

Input:

Mereferensikan ke output yang lama;

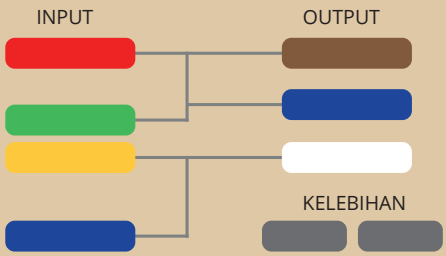
Output:

Output dan ***rangeproofs***
Transaksi rahasia ;

Kelebihan:

Perbedaan antara output dan input, ditambah **signature** (untuk otentikasi dan untuk membuktikan non-inflasi).

Gambar 2:
Bagian transaksi MimbleWimble.



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

Semua blok Epic Cash berisi:

Merkle Trees pada input transaksi;

***Merkle Trees* pada output dan *rangeproof* transaksi;**

Daftar dari nilai tambah dan signature.

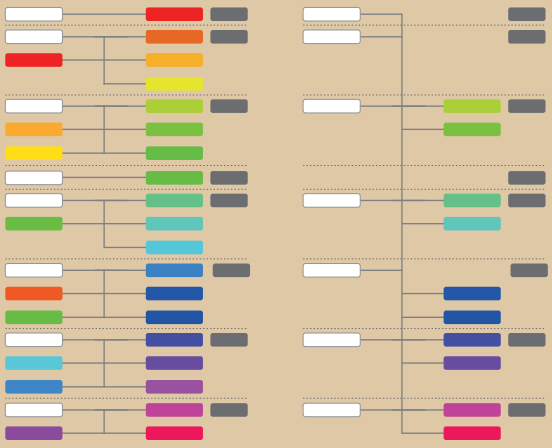
Dalam Gambar 2 dan 3, diadaptasi dari presentasi Andrew Poelstra[10], kita dapat melihat Epic yang baru ditambang digambarkan sebagai sel input putih. Sel-sel berwarna identik mewakili output dengan input yang cocok dihabiskan. Dengan proses *Cut-Through*, input dan output yang cocok dikeluarkan untuk membebaskan ruang di dalam blok, yang mengurangi jumlah data yang perlu disimpan di blockchain. Ketika transaksi dihilangkan dari buku besar (*ledger*), kelebihan dari kernel yang tersisa (hanya 100 byte) secara permanen mendokumentasikan bahwa transaksi berlangsung.

Saat blok terus dibuat, MimbleWimble menerapkan *Cut-Through* lintas blok, sehingga dalam jangka panjang semua yang tersisa adalah header blok (sekitar 250 byte), transaksi yang tidak digunakan, dan kernel transaksi (sekitar 100 byte). *Grin*, implementasi MimbleWimble kedua yang akan diluncurkan, menunjukkan bahwa rantai MimbleWimble dengan jumlah transaksi yang serupa dengan rantai Bitcoin akan hampir 10% dari ukuran rantai Bitcoin[11]. Selain itu, ukuran sebuah node akan "sesuai urutan beberapa GB untuk rantai berukuran Bitcoin, dan berpotensi dioptimalkan hingga beberapa ratus megabyte."[12]

Ini sangat berbeda dengan Bitcoin, di mana seluruh blockchain harus disimpan oleh setiap node. Seiring waktu, karena efisiensi ruang dari blockchain Epic Cash tumbuh relatif terhadap blockchain Bitcoin, demikian juga efisiensi biaya relatif terhadap partisipasi node dalam jaringan Epic Cash. Hambatan yang lebih rendah untuk berpartisipasi membantu memastikan elastisitas yamg penting pada lapisan node pada desain jaringan.

Melalui penerapan MimbleWimble dan penerapan pemangkasan rantai dengan proses *Cut-Through*, blockchain Epic Cash menawarkan skalabilitas dengan cara yang sering diremehkan oleh komunitas cryptocurrency. Ini adalah salah satu yang menangkap esensi Bitcoin dan proyek-proyek yang berpikiran sama: desentralisasi. Terlepas dari berapa banyak transaksi per koin yang mungkin dapat diproses, apa untungnya jika tidak dapat dipertahankan oleh jaringan yang luas dan beragam? Jika persyaratan memori yang sedemikian rupa, sehingga validasi pada akhirnya mengarah pada konglomerat pertambangan yang kuat, maka semua upaya komunitas cryptocurrency untuk menciptakan ekosistem terdesentralisasi dapat dihilangkan. Untuk menyediakan *throughput* tambahan, implementasi Layer 2 *Lightning-style* direncanakan sebagai tujuan jangka pendek dalam roadmap pengembangan Epic Cash.

Gambar 3:
Transaksi MimbleWimble sebelum dan sesudah *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. Kebijakan Moneter

Kebijakan moneter Epic Cash dan Bitcoin sangat mirip. Suplai yang beredar dari Epic Cash pertama kali berkembang dengan pesat dan kemudian disinkronkan dengan suplai Bitcoin yang beredar di tahun 2028. Ia meningkat setelah itu dengan laju yang menurun hingga mencapai suplai maksimum 21 juta Epic pada tahun 2140. Epic Cash memiliki kualitas untuk menjadi penyimpan yang aman dengan nilai jangka panjang karena suplai yang beredar diketahui pada titik mana saja , di sepanjang siklus emisinya dan memuncak pada suplai maksimum yang tetap. Kebijakan moneter Epic Cash ditandai oleh empat fitur berikut:

- Emisi yang cepat selama sembilan tahun pertama pada masa pakainya, di mana 20.343.750 Epic (96,875% dari total suplai) harus ditambang. Tingkat emisi yang tepat diuraikan dalam bagian Jadwal Emisi dari paper ini;
- Suplai yang beredar dari Epic dan tingkat emisinya disinkronkan dengan Bitcoin pada *Epic Singularity* kira-kira tanggal 24 Mei 2028. Setelah *Singularity*, tingkat emisi menurun pada rate yang meningkat, sementara suplai yang beredar bertumbuh pada tingkat yang menurun;
- Suplai maksimum 21 juta Epic akan tercapai pada tahun 2140, pada waktu yang hampir sama dengan Bitcoin ketika mencapai suplai maksimum 21 juta unit;
- Epic memiliki struktur 8 desimal yang dapat dibagi, sehingga: 1 Epic = 100.000.000 warga (sama seperti 1 Bitcoin setara dengan 100.000.000 satoshi).

Kebijakan moneter Epic Cash dibentuk setelah Bitcoin karena alasan berikut:

- Kesepakatan dengan dasar-dasar ekonomi Bitcoin, yaitu kelangkaan dan kepastian suplai yang beredar mendasari penyimpanan yang kuat pada nilai dari properti;
- Publik sudah terbiasa dengan model Bitcoin dan rekam jejak yang terbukti selama sepuluh tahun terakhir sejak permulaannya. Dengan menyinkronkan dengan suplai Bitcoin yang beredar, dan mencerminkan struktur pasokan dan suplai maksimum Bitcoin, Epic menempuh jalur dengan reseistan yang paling terhadap adopsi massal.

VII. Penambangan

Blockchain Epic Cash mengikuti desentralisasi dengan menyambut berbagai macam perangkat keras komputasi. Penambangan epic awalnya tersedia untuk CPU, GPU, dan ASIC, menggunakan tiga algoritma hashing masing-masing: RandomX, ProgPow, dan CuckATOo31 +. Algoritma dapat ditukar dengan mudah tanpa mengganggu integritas rantai.

1 RandomX dan CPU

RandomX merupakan algoritma *Proof-of-Work* (PoW) dioptimalkan untuk CPU dengan kebutuhan umum. Ia menggunakan eksekusi program acak dengan beberapa teknik *memory-hard* untuk mencapai tujuan berikut:

- Pencegahan pada pengembangan ASIC chip tunggal;
- Minimalkan keuntungan efisiensi dari perangkat keras khusus pada CPU untuk tujuan umum.

Menambang Epic dengan CPU memerlukan alokasi 2 GB RAM fisik , 16 KB L1 cache , 256 KB L2 cache , dan 2 MB dari L3 cache per thread mining[13]. Perangkat Windows 10 membutuhkan 8 GB atau lebih RAM. Bukan tidak mungkin bahwa suatu hari di masa depan ponsel tidak terlalu lama dapat menjadi node penambangan yang layak. Integrasi CPU awal dalam jaringan penambangan Epic Cash adalah peluang yang sangat baik bagi banyak orang dengan hanya komputasi yang sederhana , dapat menghasilkan reward blok dengan membantu mengamankan jaringan Epic Cash.

2 ProgPow dan GPU

Programmatic Proof-of-Work (ProgPow) adalah algoritma yang bergantung pada bandwidth memori dan komputasi inti dari urutan matematika acak, yang memanfaatkan banyak fitur komputasi GPU dan dengan cara tersebut , menangkap total biaya energi perangkat keras secara efisien . Karena ProgPow dirancang khusus untuk memanfaatkan komoditas GPU yang sepenuhnya, maka akan sulit dan mahal untuk mencapai efisiensi yang lebih tinggi melalui perangkat keras khusus. Dengan demikian, algoritma ProgPow memitigasi insentif untuk pool ASIC yang besar agar mengalahkan GPU, yang sering terlihat pada banyak algoritma PoW lainnya, seperti Bitcoin SHA-256. GPU, meskipun tidak populer seperti CPU, ia masih sangat sering tersedia. Dengan pengembangan teknologi yang digerakkan oleh pembangkit tenaga listrik, Nvidia dan AMD, GPU mampu memproses paralel pada banyak solusi penambangan di atas CPU berdasarkan basis per unit. Karena kombinasi dari manapun dan daya pemrosesan yang tinggi inilah , GPU akan menjadi *backbone* dari banyak aktivitas penambangan selama waktu permulaan, seperti yang ditunjukkan pada Tabel 2.

3 CuckATOo+31 dan ASIC

CuckATOo31 + adalah permutasi ASIC yang *friendly* dari algoritma Cuckoo Cycle yang dikembangkan oleh ilmuwan komputer Belanda, John Tromp. Berkaitan dengan ASIC resistant , CuckARoo29, CuckATOo31 + menghasilkan grafik bipartit acak dan memberikan tugas kepada penambang untuk menemukan lingkaran dengan panjang tertentu 'N' yang melewati node-node dari grafik itu.

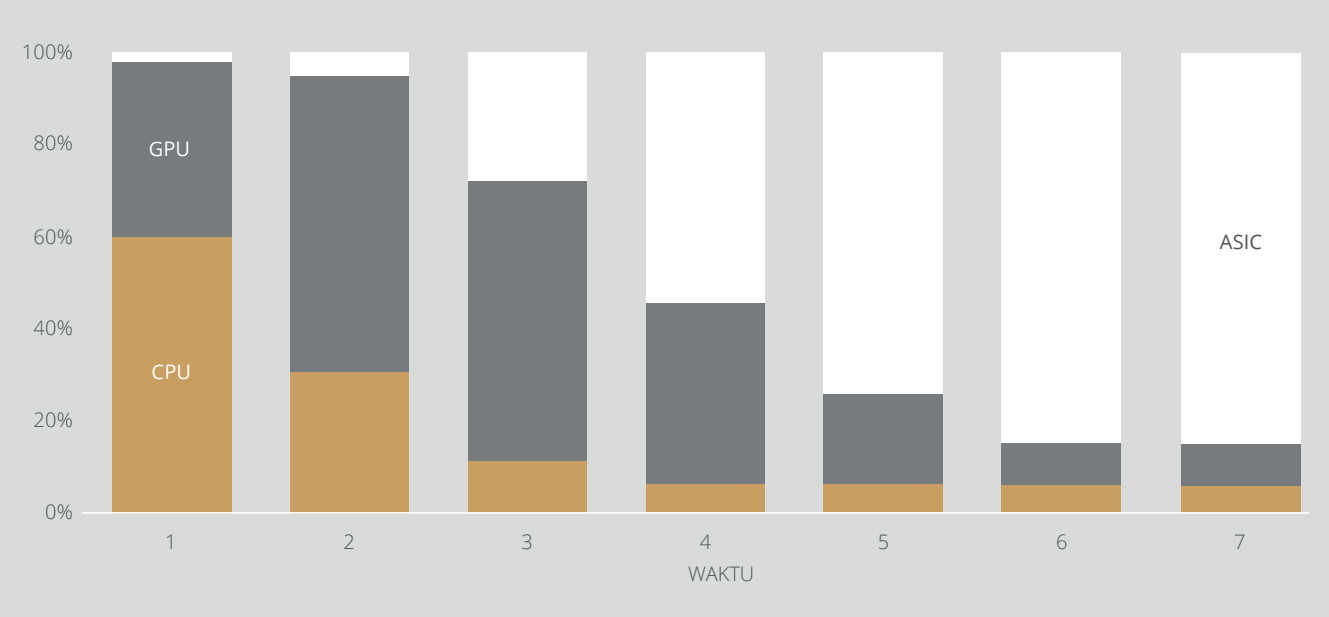
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Ini adalah tugas *memory bound*, artinya waktu solusi terikat oleh bandwidth memori dibandingkan *raw processor* atau kecepatan GPU. Akibatnya, algoritma Cuckoo Cycle menghasilkan panas yang lebih sedikit serta mengkonsumsi energi yang secara signifikan lebih sedikit dibandingkan algoritma PoW tradisional. CuckATOo31+ yang cocok dengan ASIC yang mengizinkan peningkatan efisiensi dibandingkan GPU yang menggunakan ratusan MB SRAM ketika tetap dihambat oleh memori I/O[14]. Pada Akhirnya, ASIC menawarkan potensi ekonomi skala terbesar dari tiga opsi penambangan. Namun, demi kepentingan inklusivitas, meskipun mereka dialokasikan bagian kecil dari reward pertambangan yang relatif terhadap CPU dan GPU, alhasil ASIC lah yang mengasumsikan saham mayoritas dari reward blok yang ditambang, dengan perkiraan akan ada ekosistem kompetitif dari produsen perangkat untuk CuckATOo31+.

Tabel 2: Pembagian reward menambang. Tergantung pada revisi. Pembagian akan diarahkan untuk mencapai desentralisasi maksimum dan konsisten dengan kepentingan jangka panjang pada jaringan.

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

Gambar 5: Pembagian reward penambangan untuk setiap waktu sesuai Tabel 2. Tergantung pada revisi.



[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 Kontribusi Penambangan

Di Mulai dari Epic Genesis (2019) dan berakhir di Epic Singularity (2028), selama proses penambangan, ada alokasi Epic yang dialihkan, sebagai kontribusi penambangan, menuju *EPIC Blockchain Foundation*.

EPIC Blockchain Foundation didedikasikan untuk pengembangan teknis dan mempromosikan kesadaran dan kegunaan proyek Epic Cash selama tahun-tahun sejak awal didirikan, dengan menciptakan kegiatan pemasaran dan mengembangkan kemitraan dalam industri teknologi keuangan.

Setelah Singularity, peran EPIC Foundation akan diambil alih oleh *EPIC Distributed Autonomous Corporation (EDAC)*, yang akan dikembangkan oleh yayasan sebelum penyerahan.

EPIC Blockchain Foundation didanai oleh persentase dari reward penambangan, dikurangi dari reward blok, sesuai dengan biaya tahunan berikut:

Tabel 3: Biaya tahunan untuk kontribusi penambangan Yayasan sebagai persentase dari reward penambangan.

Tahun	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% Reward Penambangan	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

IX. Spesifikasi Teknis

Nama Proyek: Epic Cash
Nama MataUang: Epic
Waktu Blok: 60 detik
Ukuran Blok: 1 MB
Suplai Awal : 0
Suplai Akhir : 21,000,000
Blok Genesis : Agustus , 2019
Konsensus: RandomX (CPUs), ProgPow (GPUs) and CuckAToo31+ (ASICs)

Link:

www.epic.tech

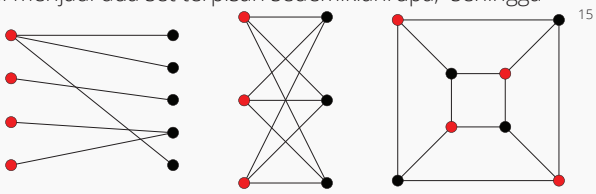
t.me/EpicCash – Telegram

t.me/EpicCashBahasaIndonesia

X. Glosarium

ASIC *Application Specific Integrated Circuits;* chip yang dirancang untuk tujuan tunggal

Grafik Bipartit satu set node grafik didekomposisi menjadi dua set terpisah sedemikianrupa, sehingga tidak ada dua node grafik dalam set yang sama berdekatan.



Faktor *Blinding* elemen acak yang dimasukkan ke dalam pesan digital untuk memfasilitasi enkripsi; rahasia bersama antara kedua pihak yang mengenkripsi input dan output dalam transaksi spesifik serta publik key dan privat dari pihak-pihak yang bertransaksi[16].

Reward Blok Epic baru didistribusikan oleh jaringan sebagai reward untuk perhitungan yang dilakukan agar memverifikasi transaksi dalam blok baru.

Cache komponen perangkat keras atau perangkat lunak yang menyimpan data sehingga permintaan di yang akan datang untuk data tersebut dapat dilayani lebih cepat.

Suplai yang beredar jumlah Epic yang ada pada waktu tertentu.

CPU *Central Processing Unit*: komponen komputer yang bertanggung jawab untuk menjelaskan dan menjalankan sebagian besar perintah dari perangkat keras dan perangkat lunak komputer lainnya.

Cut-Through proses blockchain MimbleWimble yang mana input dan pencocokan output yang dihabiskan dihapus untuk membebaskan ruang dalam blok, mengurangi jumlah data yang perlu disimpan di blockchain.

Desentralisasi kondisi penyebaran pada operasi jaringan dan tata kelolanya.

Emisi penciptaan Epic baru yang diperoleh penambang di reward blok. Epic dibuat setiap 60 detik karena transaksi dikonfirmasi ke dalam blockchain.

Epic Singularity titik di mana suplai Epic yang beredar disinkronkan dengan suplai Bitcoin yang beredar (Mei 2028).

Kelebihan (MimbleWimble) perbedaan antara output dan input, ditambah signature (untuk otentikasi dan untuk membuktikan non-inflasi).

Kesetaraan properti suatu barang atau komoditas di mana unit individu pada dasarnya dapat dipertukarkan, dan masing-masing bagiannya tidak dapat dibedakan dari bagian lain.

Genesis (*Event*) penambangan pada blok Epik pertama dan awal yang resmi pada blockchain.

GPU *Graphics Processing Unit*: Unit yang berisi chip logika (prosesor) yang dapat diprogram khusus untuk fungsi tampilan. konsumen GPU sangat cocok untuk penambangan cryptocurrency.

***Halving* (untuk Bitcoin)** terjadi setiap 4 tahun. Tingkat suplai berkurang hingga 50% setelah setiap event *halving*.

Hash nilai yang dihitung dari nomor input dasar menggunakan fungsi *hashing*.

Algoritma *Hashing* (fungsi) algoritma matematika yang memetakan data ukuran yang berubah-ubah ke *hash* dari ukuran tetap yang digunakan untuk menghasilkan dan memverifikasi *signature* digital, *message authentication codes* (MAC), dan bentuk otentikasi lainnya.

Homomorphic Encryption Immutability metode melakukan perhitungan pada informasi yang dienkripsi tanpa mendekripsi terlebih dahulu. (dalam pemrograman) keadaan di mana suatu objek tidak dapat dimodifikasi setelah dibuat.

Input (MimbleWimble) komponen transaksi MimbleWimble yang menunjukkan pihak pengirim dari transaksi; dibuat dari output transaksi sebelumnya.

I/O input output; komunikasi antara sistem pemrosesan informasi, seperti komputer, dan dunia luar, mungkin manusia atau sistem pemrosesan informasi lainnya.

[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/

Suplai Maksimal	jumlah Epic yang akan dicapai pada titik dimana suplai yang beredar tidak akan meningkat sesudahnya (21.000.000 Epic).
Memory-Hard	penggunaan banyak RAM untuk mencegah koneksi simultan dalam menjalankan upaya secara paralel. Fungsi *memori-hard* adalah algoritma yang memiliki waktu komputasi terutama ditentukan oleh memori yang tersedia untuk menyimpan data. Juga dikenal sebagai fungsi yang *memory-bound* (terikat memory).
Merkle Tree	struktur data yang digunakan dalam aplikasi ilmu komputer. Dalam blockchain, *Merkle trees* mengizinkan verifikasi konten yang efisien dan aman dalam struktur data besar.
MimbleWimble	sebuah protokol diajukan oleh kontributor dengan nama samaran, pergi dengan moniker Tom Elvis Jedusor, di chatroom pengembang Bitcoin.
Multisignature	skema tanda tangan digital yang mengizinkan sekelompok pengguna untuk menandatangani satu dokumen. Biasanya, algoritma multisignature menghasilkan tanda tangan bersama yang lebih kompak dibandingkan kumpulan tanda tangan yang berbeda dari semua pengguna[17].
Node	komputer yang terhubung ke jaringan blockchain dan bercabang ke node lain dalam jaringan untuk mendistribusikan informasi mengenai transaksi dan blok, dengan cara *peer-to-peer*.
***One Way Aggregate Signature* (OWAS)**	tanda tangan transaksi yang terdiri dari banyak tanda tangan yang dienkripsi sedemikian rupa sehingga sangat sulit untuk menghitung tanda tangan individu yang merupakan bagian dari perkumpulan.
Output (MimbleWimble)	komponen transaksi dari MimbleWimble yang mewakili tanda terima transaksi; digunakan sebagai input untuk transaksi selanjutnya.
Pedersen Commitment Scheme	kriptografi sederhana yang mengizinkan prover untuk berkomitmen pada nilai yang dipilih tanpa mengungkapkan informasi apa pun tentangnya dan tanpa prover yang mampu membatalkan komitmen terhadap nilai tersebut.
Private Key	private key adalah sedikit kode yang dipasangkan dengan public key agar mematikan algoritma untuk enkripsi dan dekripsi teks. ia dibuat sebagai bagian dari kriptografi public key selama enkripsi dari kunci asimetris dan digunakan untuk mendekripsi dan mengubah pesan menjadi format yang dapat dibaca.
Proof of Work (PoW)	potongan data yang sulit (mahal dan memakan waktu) untuk diproduksi, tetapi mudah bagi orang lain untuk memverifikasi, dan yang memenuhi persyaratan tertentu. *Proof of Work* sering digunakan dalam pembuatan blok cryptocurrency.
Public Key	kunci publik dibuat dalam kriptografi enkripsi *public key* yang menggunakan algoritma enkripsi *asymmetric-key*. *public key* digunakan untuk mengubah pesan menjadi format yang tidak dapat dibaca.
RAM (*Random Access Memory*)	chip penyimpanan data dengan akses yang cepat di perangkat komputasi tempat sistem operasi (OS), program aplikasi, dan data yang digunakan saat ini disimpan , sehingga dapat dengan cepat dijangkau oleh prosesor perangkat.
Rangeproof	validasi komitmen yang memverifikasi bahwa jumlah input transaksi lebih besar dari jumlah output transaksi dan bahwa semua nilai transaksi dalah positif. Rangeproof memastikan bahwa suplai moneter belum dirusak.
(Digital) Signature	bagian umum dari protokol blockchain, terutama digunakan untuk mengamankan transaksi dan blok transaksi, transfer informasi, manajemen kontrak dan setiap kasus lain di mana mendeteksi dan mencegah gangguan eksternal sangat penting. Mereka memberikan tiga keuntungan menyimpan dan mentransfer informasi di blockchain: • Mereka memperlihatkan jika data yang dikirim telah dirusak; • Memverifikasi partisipasi dari pihak tertentu dalam transaksi; • Dapat mengikat secara hukum.
SRAM (*Static Random Access Memory*)	*Random Access Memory* (RAM) yang mempertahankan bit data dalam memorinya selama daya disuplai.
Throughput	ukuran transaksi per detik yang dapat dilakukan oleh protokol cryptocurrency yang disetujui.
Trustlessness	kualitas jaringan mata uang kripto untuk mematuhi aturan protokol tanpa paksaan dari 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

EPIC CASH

EPIC PRIVATE INTERNET CASH