Freeman Family

4 de julho de 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

Um Sistema de Dinheiro Eletrônico Peer-to-Peer

RESERVA DE VALOR + MOEDA DE TROCA + VALOR UNITÁRIO

1,7 bilhão de adultos não têm acesso ao sistema financeiro global, enquanto outros 1,3 bilhão são carentes. Epic Cash desbloqueia o potencial humano conectando indivíduos ao mercado global. Rápido, praticamente gratuito e aberto a todos.

Version 7.1b **Portuguese**

Conteúdo

I. Abstrato

Epic Cash é o ponto final da jornada em direção ao verdadeiro dinheiro da internet P2P, a pedra fundamental de um sistema financeiro privado. A moeda Epic tem como objetivo tornar-se a forma de dinheiro digital com proteção de privacidade monetária mais eficaz do mundo. Para cumprir esse objetivo, satisfaz as três principais funções do dinheiro:

1. **Reserva de valor** – pode ser guardado, recuperado e trocado mais tarde, e de valor previsível quando recuperado;
2. **Moeda de Troca** – qualquer coisa aceita como representando um padrão de valor e trocável por bens ou serviços;
3. **Valor Unitário** – a unidade pela qual o valor de uma coisa é contabilizado e comparado.

	$ USD	BTC	EPIC
Reserva de valor	✗	✓	✓
Moeda de Troca	✓	✗	✓
Valor Unitário	✓	✗	✓

Em 2009, o Bitcoin emergiu como a primeira moeda digital baseada em blockchain e, com ela, três características definidoras, contra as quais outras criptomoedas são avaliadas.:

- **Confiabilidade** – ninguém é obrigado a confiar em qualquer entidade centralizada ou contraparte para que a rede funcione;
- **Imutabilidade** – transações não podem ser desfeitas;
  a. Deve ser altamente improvável ou difícil reescrever a história;
  b. Deveria ser impossível para qualquer pessoa, exceto o dono de uma chave privada para mover fundos associados a essa chave privada;
  c. Todas as transações são registradas no blockchain.
- **Decentralização** – "Os blockchains são politicamente descentralizados (ninguém os controla) e arquitetonicamente descentralizados (nenhum ponto infraestrutural de falha)..."[1].

Bitcoin abriu novos caminhos tecnologicamente enquanto aderia aos fundamentos testados pelo tempo na estrutura de sua política monetária. O sucesso do Bitcoin está fortemente relacionado à sua oferta limitada combinada com blockchain sem confiança, imutável e descentralizado. Epic Cash emula a política monetária do Bitcoin de diminuir a inflação e a oferta limitada para garantir que a moeda da Epic possa servir como uma reserva efetiva de valor.

Apesar do sucesso do Bitcoin, certas deficiências foram reveladas desde a sua criação há 10 anos. Outros projetos tentaram superar essas deficiências e nós investigamos o melhor deles para usar como nosso ponto de partida. Decidimos utilizar o código base do Grin e o excelente trabalho de vários outros projetos para nos ajudar a aperfeiçoar as conquistas obtidas com muito esforço e descobrir as falhas dos antecessores do Epic Cash. Epic Cash possui as principais qualidades para ser uma moeda ideal:

- **Fungibilidade** – O valor de uma determinada unidade de Epic deve sempre ser igual a outra unidade de Epic, assim como um Yen ou Yuan é sempre igual a e substituível por outro Yen ou Yuan. A obtenção da fungibilidade em grande parte depende da privacidade.
- **Escalabilidade** – A Epic Cash mantém uma blockchain de espaço-eficiente, sobre a qual novos nós cser facilmente estabelecido sem equipamento intensivo de recursos. O blockchain da Epic Cash é capaz de pelo menos duas vezes a taxa de transferência do Bitcoin.
- **Privacidade** – O blockchain da Epic Cash protege o anonimato dos detentores e usuários da Epic, protegendo os detalhes das transações de terceiros, e é projetado para ser indetectável e invisível à vigilância..
- **Velocidade** – As transações da Epic Cash são suaves, contínuas e executadas muito mais rapidamente do que nas gerações anteriores de tecnologia blockchain. Enquanto o Bitcoin requer seis blocos de 10 minutos para obter a confirmação completa da transação, as transações da Epic ocorrem dentro de uma confirmação de um único bloco assim que um bloco de 1 minuto é minerado..

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

II. Privacidade

O uso moderno do dinheiro pode ser entendido como a transferência coletiva de valores unitários entre pessoas e instituições. O cenário do dinheiro em qualquer ponto no tempo pode ser mapeado respondendo às seguintes perguntas:

1. *Quem o detém e quanto estão detendo?*
2. *Quem está negociando com quem e por quanto?*

Para as moedas tradicionais e também para o Bitcoin, podemos responder a essas perguntas. Ao fazer isso, muito pode ser revelado sobre a vida das pessoas, como padrões de consumo, propriedade e contrapartes transacionais. Podem ser tiradas conclusões razoavelmente precisas sobre os interesses e intenções de um indivíduo, rastreando as transferências de valor. Sem privacidade, os dados da transação podem ser informações perigosas nas mãos de terceiros predatórios.

O uso da criptomoeda na década passada mostra um continuum de "privacidade" em diversas implementações de blockchain. A escala de privacidade, caso seja considerada, varia de aberta e notória de um lado a anônima do outro. À medida que a privacidade se deteriora, uma das pedras angulares essenciais da criptomoeda, a falta de confiança, degrada. Como evidenciado pelo sucesso dos serviços de análise de blockchain Bitcoin, o Bitcoin está mais situado no final notoriamente transparente do espectro da privacidade. Os usuários devem cada vez mais tomar medidas para garantir que não realizem transações inadvertidamente em Bitcoin contaminado. A solução Epic Cash muda o foco para o anonimato e restaura essa propriedade essencial, garantindo que tanto a privacidade do indivíduo quanto a privacidade das transações sejam projetadas no sistema em um nível fundamental.

Privacidade da Identidade

Privacidade da Transação

Privacidade da Identidade

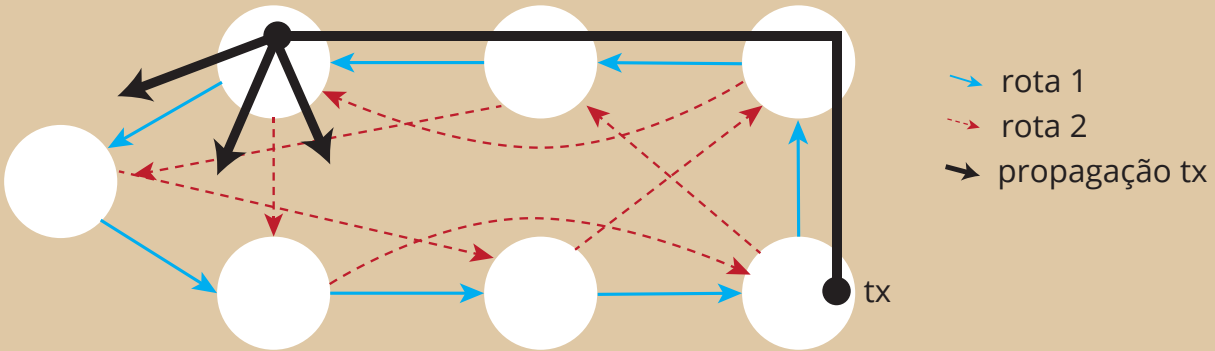
A maioria das criptomoedas como o Bitcoin são armazenadas em carteiras cujos endereços se referem a chaves públicas derivada das chaves privadas de uma carteira. Esses endereços podem ser considerados como localizadores do cofre particular no mundo digital. O blockchain Epic Cash elimina endereços inteiramente e, em vez disso, utiliza uma grande multiassinatura a partir da qual todas as chaves públicas e privadas são geradas em base de uso único.

Como os endereços de carteira do Bitcoin são um localizador de cofre no mundo digital, essa carteira pode ser rastreada até o Endereço IP do proprietário, que ancora o proprietário a um computador em um local exclusivo em um determinado momento. Explicado de forma simples: quando ocorre uma transação Bitcoin, a transação é transmitida de um hub de comunicação chamado de "nó" e, em seguida, propagada para outros nós chamados "peers". Essa informação então se espalha rapidamente para cada um desses pares de nós consecutivamente em toda a rede. Este processo é apropriadamente chamado de "Protocolo de Gossip". Simplesmente, cada Bitcoin tem uma posição online visível e um local físico onde ele, ou melhor, o proprietário do Bitcoin, pode ser encontrado. Como observou a jornalista Grace Cañn, o Bitcoin "não é mais secreto do que uma pesquisa no Google a partir de uma conexão de internet doméstica."[2]

Além de eliminar os endereços de carteira, o blockchain da Epic Cash protege a privacidade da identidade, garantindo que os endereços IP não possam ser rastreados. Isso é feito através da integração do ***Protocolo Dandelion++***. Melhorando seu antecessor, o original ***Protocolo Dandelion***, o ***Protocolo Dandelion++*** é o resultado do trabalho contínuo de sete pesquisadores para combater os ataques de desanonimização no blockchain. Através do ***Dandelion++***, as transações são passadas por caminhos entrelaçados aleatórios, ou 'cabos', e então subitamente são difundidos para uma grande rede de nós, como as vagens de uma flor de dente-de-leão quando soprados de seu caule (Figura1). Isso torna quase impossível rastrear as transações de volta à sua origem e, assim, seus endereços IP de origem.

Figura 1: Anonimizando transações com o *Protocolo Dandelion++*.

Dandelion++ encaminha mensagens através de uma das duas rotas entrelaçadas em um gráfico regular de 4, em seguida, difunde usando a distorção. Na figura, a transação se propaga pela sólida rota3 azul. Esse processo torna extremamente difícil rastrear as transações de volta à sua origem, preservando assim a privacidade..



[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

Privacidade da Transação

O blockchain da Epic Cash garante a privacidade das transações obscurecendo os valores e o relacionamento emissor-receptor de uma transação. Isto é conseguido através da aplicação de ideias familiares a ***Transações Confidenciais (CT)***[4] e ***CoinJoin***[5], métodos em grande parte desenvolvidos por Gregory Maxwell (Desenvolvedor Bitcoin Core, Co-Fundador e CTO da Blockstream).

CT, originalmente criado por Adam Back e posteriormente refinado por Maxwell, trabalha quebrando as transações em partes menores através de criptografia homomórfica, um método de executar cálculos em informações criptografadas sem descriptografá-las primeiro para preservar a privacidade. Uma vez divididos, os observadores não podem ver os valores reais das transações devido aos fatores cegantes, um sistema que lança números aleatórios na mistura de fragmentos de transação para ocultar os valores desses fragmentos. Por fim, apenas as partes responsáveis pelas transações sabem o valor de uma troca, enquanto a transação é verificada pela rede por meio da confirmação de que a soma dos valores de saída é igual à soma dos valores de entrada e a soma dos valores dos fatores cegantes de saída à soma dos fatores cegantes de entrada.

Para complicar ainda mais a tarefa dos olhares indiscretos, todas as transações da Epic Cash são encobertas pela ***CT*** e depois misturadas para esconder as conexões entre as partes envolvidas. Isso é feito através do segundo conceito de Maxwell, ***CoinJoin***.

Para ilustrar o ***CoinJoin*** de forma simplista, imagine que A, B e C estão enviando Epic para X, Y e Z, respectivamente. Enviado pelo meio ***CoinJoin***, tudo o que se sabe é que A, B e C estão enviando e X, Y e Z estão recebendo, enquanto os valores da transação permanecem invisíveis. O sistema ***CoinJoin*** é fundamental para a Epic Cash através da One-Way Aggregate Signatures (OWAS), que combinam todas as transações dentro de um bloco em uma única transação.

Privacidade: Resumo

A blockchain da Epic Cash protege a privacidade dos indivíduos e suas transações por:

- **Eliminando endereços de carteiras – Não há identificadores de localização para cofres digitais dentro do blockchain. As transações são construídas diretamente de pessoa-a-pessoa em uma base de carteira-a-carteira;**
- ***Transações Confidenciais* – divida as transações em várias partes e introduza fatores cegantes na coleção dessas peças, para que os valores das peças e outros parâmetros de transação não sejam conhecidos;**
- ***Protocolo Dandelion++* – oculta os caminhos digitais de uma transação do endereço IP do remetente da transação;**
- ***CoinJoin* – combina transações em pacotes para mascarar as relações entre as partes envolvidas.**

[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. Fungibilidade

Charlie Lee, o criador do Litecoin, afirmou que a fungibilidade era a única propriedade sadia do dinheiro em falta no Bitcoin e Litecoin, admitindo que a privacidade e a fungibilidade eram os próximos campos de batalha para essas moedas[6]. Andreas Antonopoulos, um dos maiores especialistas em blockchain do mundo, afirmou que "... as moedas contaminadas são destrutivas. Se você quebra a fungibilidade e a privacidade, você quebra a moeda."[7]

A fungibilidade é a propriedade de um conjunto de bens ou ativos que garante que as unidades individuais desse conjunto sejam de igual valor e sejam intercambiáveis. É o que diferencia as primeiras formas de moeda de seus sistemas precedentes de permuta. Sem confiança na fungibilidade do dinheiro, esse dinheiro perde rapidamente sua utilidade. Como será ilustrado abaixo, a fungibilidade da maioria das criptomoedas é incerta, enquanto a arquitetura de privacidade da Epic Cash garante que ela seja imune às mesmas ameaças.

A maioria das criptomoedas semelhantes ao Bitcoin, pela natureza das blockchains transparentes em que elas existem, podem ser rastreadas através de todas as carteiras em que foram guardadas. Terceiros e governos privados monitoram o blockchain Bitcoin com meios cada vez mais sofisticados para identificar rapidamente moedas usadas em atividades anteriores. Isso naturalmente leva a preocupações de que as moedas contaminadas possam, um dia, ser banidas das transações, deixando seus subseqüentes detentores de boa fé no prejuízo..

Em 19 de Março de 2018, o U.S. Office of Foreign Asset Control (OFAC) anunciou que estava considerando incluir endereços de moeda digital na lista de Cidadãos Especialmente Designados (SDNs), que são entidades com as quais pessoas ou empresas dos EUA estão proibidas de realizar transações. Ainda mais preocupante, o OFAC não descartou a inclusão de endereços descartou a inclusão de endereços que atualmente continham as moedas contaminadas na lista SDN, o que efetivamente colocaria os proprietários inocentes de criptomoedas contaminados em uma lista negra criminal devido à afilição das moedas contaminadas em sua posse. Isso levou o professor de direito da Universidade de Nova York, Andrew Hinkes, a brincar, "adeus a fungibilidade", e que o público deveria esperar "um prêmio em moedas recém-cunhadas, ou moedas limpas rastreadas..."[8].

Com esses desenvolvimentos em mente, não é difícil imaginar uma reviravolta no mercado cripto e o sofrimento, ou mesmo a extinção, de muitas criptomoedas bem estabelecidas. No entanto, Epic é uma das poucas criptomoedas que evita esse problema inteiramente devido aos fortes recursos de privacidade descritos anteriormente neste documento. Ao remover o vínculo entre identidade e propriedade, e a relação entre as partes envolvidas, a Epic nunca pode ser afetada por uma pessoa ou por uma atividade. Como tal, o valor da Epic permanece independente de seus usuários e oferece altos níveis de privacidade e segurança que não podem ser facilmente manipulados por agentes maliciosos em áreas criminais, financeiras ou políticas..

> **"MOEDAS CONTAMINADAS SÃO DESTRUTIVAS. SE VOCÊ QUEBRA A FUNGIBILIDADE E A PRIVACIDADE, VOCÊ QUEBRA A MOEDA."**
>
> **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. Escalabilidade

Epic Cash é uma implementação de blockchain MimbleWimble que produz avanços na escalabilidade como resultado do design espacial e eficiente que elimina dados de transação redundantes. A funcionalidade Cut-Through responsável por isso assegura que o blockchain cresça mais espaço-eficiente ao longo do tempo, ao contrário da maioria das criptomoedas, incluindo o Bitcoin, e que novos nós possam ser criados com investimentos mínimos em memória e poder de computação. Ao permanecer espaço-eficiente, capacita uma rede amplamente dispersa e promove a descentralização. Além disso, embora cada nó Bitcoin deva armazenar toda a cadeia, os nós da Epic Cash podem contribuir para a segurança da rede com base em um pequeno subconjunto de blocos.

A maioria das criptomoedas requer armazenamento indefinido de todos os dados de transação em suas blockchains. A cadeia Bitcoins atualmente recebe 0,1353 GB de memória por dia, enquanto a cadeia Ethereum aumenta a uma taxa ainda mais rápida de 0,2719 GB por dia. Se a rede Bitcoin continuar crescendo em sua taxa atual, ela atingirá um tamanho aproximado de 6 TB no momento em que seu último bloco de recompensas for extraído no ano 2140. Ethereum ultrapassará 10 TB nessa data[9]. Na maioria dos blockchains sem MimbleWimble, as transações devem ser verificadas por nós em todo o mundo. Conforme os dados aumentam, o mesmo acontece com o ônus de cada nó. Mesmo com apenas 200 GB (o tamanho aproximado da cadeia atual do Bitcoin), a sincronização dos dados requer uma rede estável e capacidade de leitura e gravação em disco de alta velocidade.

Consequentemente, a mineração tornou-se cada vez mais centralizada entre grandes pools, alavancando recursos computacionais caros. **Se toda a história do blockchain do Bitcoin fosse armazenada no blockchain da Epic Cash, ela ocuparia quase 90% menos espaço.** Menor é mais rápido porque cada transação requer menos tempo para transmitir e proteger.

MimbleWimble resolve este dilema de armazenamento com um método inovador de desbaste de blocos, conhecido como 'Cut-Through'. Para entender como o Cut-Through funciona, é melhor primeiro observar como as transações e os blocos são compostos dentro de um blockchain MimbleWimble.

Entradas:

Referências a entradas antigas;

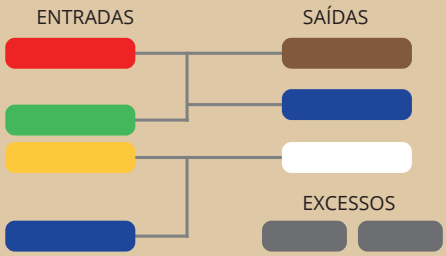
Saídas:

Saídas de *Transações Confidenciais* e **rangeproofs**;

Excesso:

A diferença entre saídas e entradas, mais **assinaturas** (para autenticação e prova de não-inflação).

Figura 2:
Partes de transação MimbleWimble.



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

Todo bloco Epic Cash contém:

Merkle Trees de transações de entrada;

Merkle Trees de transações de saída e rangeproofs;

Uma lista de valores em excesso e assinaturas.

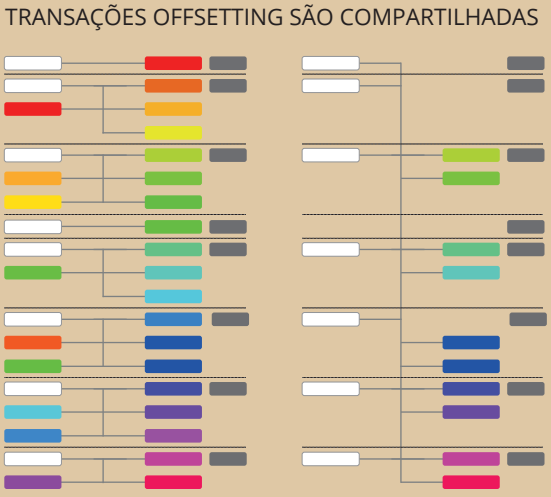
Nas Figuras 2 e 3, adaptado das apresentações de Andrew Poelstra[10], podemos ver Epic recém-minerado representado como as células de entradas brancas. Células coloridas idênticas representam saídas com entradas correspondentes de gastos. Com o processo Cut-Through, entradas e correspondentes saídas de gastos são removidas para liberar espaço dentro do bloco, o que reduz a quantidade de dados que precisam ser armazenados no blockchain. Enquanto as transações são omitidas do ledger, os demais kernels excedentes (meros 100 bytes) documentam permanentemente que as transações ocorreram.

À medida que os blocos continuam sendo criados, o MimbleWimble aplica Cut-Through em blocos, de modo que a longo prazo tudo o que resta são as cabeça do bloco (aproximadamente 250 bytes), transações não gastas e kernels de transação (aproximadamente 100 bytes). Grin, a segunda implementação do MimbleWimble a ser lançada, mostrou que uma cadeia MimbleWimble com um número similar de transações para a cadeia Bitcoins seria de quase 10% do tamanho da cadeia Bitcoin[11]. Além disso, o tamanho de um nó será "da ordem de alguns GB para uma cadeia do tamanho da de Bitcoin e potencialmente otimizável para algumas centenas de megabytes."[12]

Isto está em contraste marcante com o Bitcoin, onde todo o blockchain deve ser armazenado por cada nó. Com o passar do tempo, à medida que aumenta a eficiência espacial do blockchain da Epic Cash em relação à blockchain do Bitcoin, o mesmo acontecerá com as eficiências de custo em relação à participação de nós na rede da Epic Cash. Barreiras menores para participar ajudam a garantir a resiliência crucial na camada de nós do design de rede.

Através da implementação do MimbleWimble e da aplicação do desbaste de cadeia com o processo Cut-Through, o blockchain da Epic Cash oferece escalabilidade de uma forma muitas vezes negligenciada pela comunidade de criptomoeda. É aquele que capta a essência do Bitcoin e projetos que pensam da mesma forma: a descentralização. Independentemente de quantas transações por segundo uma moeda possa processar, o que é bom se não puder ser sustentado por uma rede ampla e diversificada? Se os requisitos de memória são tais que a validação, em última instância, atrai os conglomerados de mineração, então todos os esforços da comunidade de criptomoeda para criar um ecossistema descentralizado são evitados. Para fornecer taxa de transferência adicional, uma implementação da Camada 2 no estilo Lightning é planejada como um objetivo de curto prazo no roteiro de desenvolvimento da Epic Cash..

Figura 3:
Transações MimbleWimble antes e depois da 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. Política Monetária

A política monetária da Epic Cash e Bitcoin são muito semelhantes. A oferta circulante de Epic Cashprimeiro expande-se rapidamente e depois sincroniza com o estoque circulante de Bitcoin em 2028. Ele aumenta a partir de então a uma taxa decrescente até atingir a oferta máxima de 21 milhões Epic em 2140. Epic Cash tem as qualidades para se tornar uma reserva segura de valor a longo prazo, porque a oferta circulante é conhecida em qualquer ponto ao longo de seu ciclo de vida de emissão e culmina com uma oferta máxima fixa. A política monetária da Epic Cash caracteriza-se pelas quatro características seguintes:

- Emissão rápida ao longo dos primeiros nove anos de sua vida útil, durante a qual 20.343.750 Epics (96,875% da oferta total) devem ser minerados. As taxas exatas de emissão são descritas na seção Cronograma de Emissão deste paper;
- A oferta de circulação e a taxa de emissão da Epic sincronizam com as da Bitcoin no Epic Singularity por volta de 24 de maio de 2028. Segundo a Singularity, a taxa de emissão diminui a uma taxa crescente, enquanto a oferta circulante cresce a uma taxa decrescente;
- Um suprimento máximo de 21 milhões de Epic será alcançado no ano 2140, aproximadamente ao mesmo tempo em que Bitcoin atinge uma oferta máxima de 21 milhões de unidades;
- Epic tem uma estrutura de divisibilidade decimal de 8, tal que: 1 Epic é igual a 100,000,000 freeman (assim como 1 Bitcoin é igual a 100,000,000 satoshi).

A política monetária da Epic Cash é modelada a partir do Bitcoin pelas seguintes razões:

- Acordo com os fundamentos econômicos do Bitcoin, ou seja, que a escassez e a previsibilidade do fornecimento circulante fundamentam seu forte armazenamento de propriedades de valor;
- O público já está familiarizado com o modelo Bitcoin e seu histórico comprovado nos últimos dez anos desde a sua criação. Ao sincronizar aproximadamente com a oferta de circulação do Bitcoin, e espelhando a estrutura máxima de fornecimento e divisibilidade do Bitcoin, a Epic toma o caminho de menor resistência em direção à adoção em massa.

VI. Cronograma de Emissão

Epic Cash tem um total de 33 eras de mineração, cada uma definida por decréscimos nas recompensas do bloco, em relação à sua anterior era. O Epic Genesis, a data em que o bloco Epic #1 foi minerado ocorreu em agosto de 2019. Os blocos são minerados um por minuto. As primeiras cinco eras produzem quase 97% da oferta máxima de Epic, correspondendo a 20 anos de emissões de Bitcoin em aproximadamente nove anos. Isso pode ser pensado como uma chance de "voltar o relógio" para aqueles que perderam a ascensão espetacular do Bitcoin.

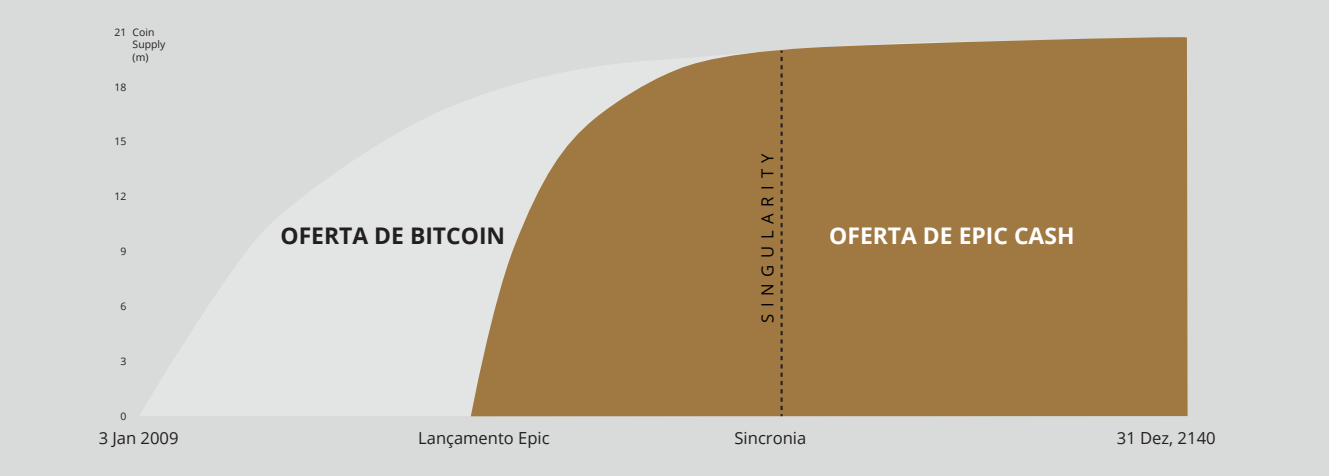
O cronograma de emissão na tabela 1 descreve as datas de início e término das primeiras sete eras de mineração, suas correspondentes recompensas de bloco e as ofertas circulantes que se seguiram para cada era. As eras 8 a 33 não estão incluídas na tabela por questão de brevidade. Para essas eras, deve-se entender que cada época subseqüente terá uma recompensa em bloco que é metade do valor da recompensa da era anterior, exatamente como em Bitcoin. A quantidade de Epic emitida durante cada uma dessas eras será a soma das recompensas de bloco dentro da era de 4 anos (aproximadamente 1460 dias).).

Na Epic Singularity (2028), a oferta circulante de Epic intercepta o número de oferta circulante do Bitcoin, ponto em que o Epic Cash adota o padrão de a recompensa e halving do bloco Bitcoin, que vê as recompensas do bloco diminuírem pela metade a cada quatro anos. A única exceção é que os blocos Epic continuam a ser minerados a uma taxa de um a cada minuto, contra a taxa de Bitcoin de um bloco a cada dez minutos. Ao fazer isso, a oferta de circulação Epic mantém uma paridade aproximada com a oferta circulante do Bitcoin pelo restante de sua existência.

Tabela 1: Cronograma de emissão para as primeiras sete eras de mineração. Datas são aproximações possíveis.

Era	1	2	3	4	5	SINGULARITY	6	7
Recompensa do Bloco	16	8	4	2	1		0.15625	0.078125
Data de Início	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
Data Final	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
Duração (em dias)	334	470	601	800	1019		1460	1460
Oferta Inicial	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Oferta Final	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% da Oferta Máxima	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Figura 4: Cronograma de emissão de Epic e Bitcoin.



VII. Mineração

O blockchain da Epic Cash busca a descentralização por aceitar uma grande variedade de hardware de computação. A mineração Epic está inicialmente disponível para CPUs, GPUs, e ASICs, usando três respectivos hashing algorítmos: RandomX, ProgPow, e CuckAToo31+. Algorítimos pode ser trivialmente trocados (hot-swap) sem comprometer a integridade da cadeia.

1 RandomX e CPUs

RandomX é uma algorítmo Proof-of-Work (PoW) otimizado para CPUs de uso geral. Utiliza execuções aleatórias de programas com várias técnicas memory-hard para alcançar os seguintes objetivos:

- Prevenção do desenvolvimento de chip único ASICs;
- Minimizar a vantagem de eficiência do hardware especializado sobre CPUs de uso geral.

Minerar Epic com CPUs requer uma alocação contígua de 2 GB de RAM física, 16 KB de L1 cache, 256 KB de L2 cache, e 2 MB de L3 cache por thread de mineração[13]. Os dispositivos do Windows 10 exigem 8 GB ou mais de RAM. Não é inconcebível que um dia, num futuro não muito distante, os celulares possam se tornar nós de mineração viáveis. A integração antecipada da CPU na rede de mineração da Epic Cash é uma excelente oportunidade para muitos, com meios de computação modestos para ganhar recompensas de bloco, ajudando a proteger a rede da Epic Cash..

2 ProgPow e GPUs

Programmatic Proof-of-Work (ProgPow) é um algoritmo que depende da largura de banda da memória e do cálculo central de sequências matemáticas aleatórias, que aproveitam muitos recursos de computação da GPU e, assim, capturam de forma eficiente o custo total de energia do hardware. Como a ProgPow é projetada especificamente para aproveitar ao máximo as GPUs de commodities, é difícil e dispendioso obter eficiências significativamente mais altas por meio de hardware especializado. Como tal, o algoritmo ProgPow mitiga os incentivos para grandes pools de ASIC em superar as GPUs, como é frequentemente visto em muitos outros algoritmos de PoW, como o SHA-256 do Bitcoin. GPUs, embora não tão prevalente como CPUs, ainda estão comumente disponíveis. Com o desenvolvimento tecnológico impulsionado pelas potências, Nvidia e AMD, as GPUs são capazes de processar paralelamente muitos múltiplos de soluções de mineração acima das CPUs por unidade. É devido a essa combinação de onipresença e alto poder de processamento que as GPUs fornecerão a espinha dorsal para grande parte da atividade de mineração durante as eras iniciais, como indicado na Tabela 2.

3 CuckAToo+31 e ASICs

CuckAToo31+ é uma permutação amigável ASIC do algoritmo Cuckoo Cycle desenvolvido pelo cientista da computação holandês John Tromp. Um parente do resistente ASIC CuckARoo29, CuckAToo31+ gera bipartite graphs randômico e apresenta aos mineradores a tarefa de encontrar um loop de comprimento determinado “N” passando pelos vértices daquele gráfico.

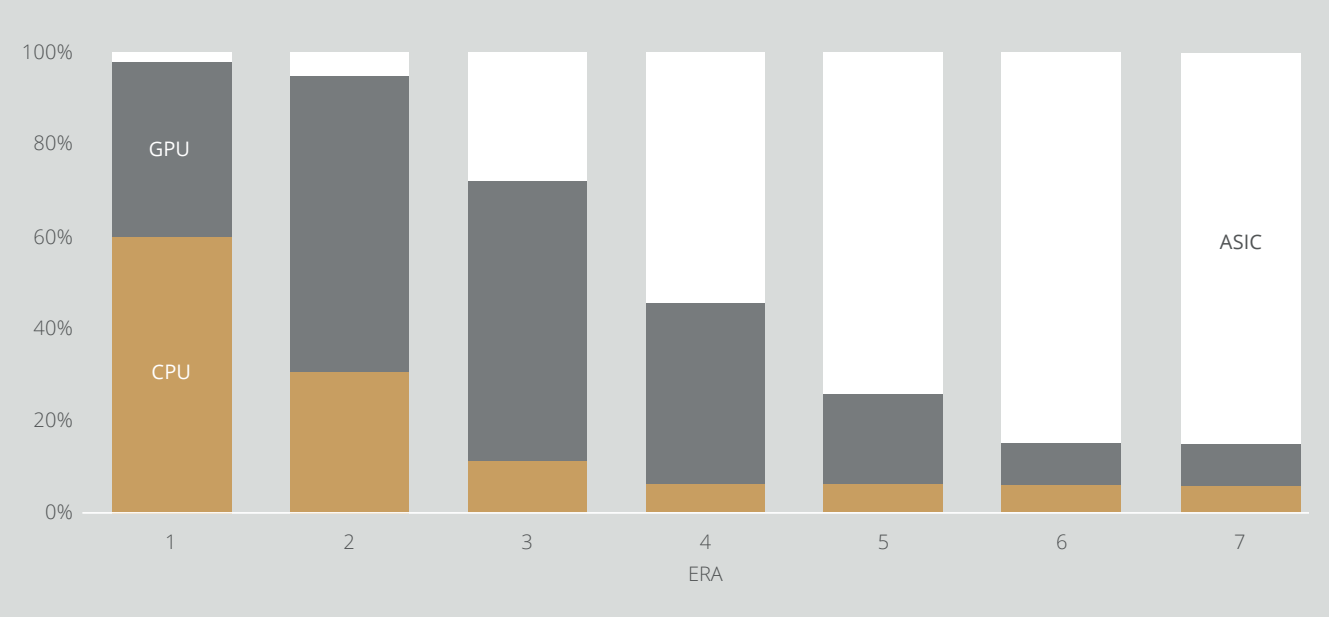
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Esta é uma tarefa vinculada à memória, o que significa que o tempo de solução é limitado pela largura de banda da memória, em vez de pelo processador bruto ou pela velocidade da GPU. Como resultado, os algoritmos do Cuckoo Cycle produzem menos calor e consomem significativamente menos energia do que os algoritmos tradicionais de PoW. O ASIC amigável CuckATOo31+ permite melhorias de eficiência sobre GPUs usando centenas de MB de SRAM enquanto permanece no gargalo por memória I/O[14]. Em última análise, os ASICs oferecem as maiores economias potenciais de escala das três opções de mineração. No interesse da inclusividade, entretanto, embora eles recebam uma pequena porção de recompensas de mineração em relação a CPUs e GPUs no começo, eventualmente os ASICs assumem uma participação majoritária nas recompensas do bloco, na suposição de que haverá um ecossistema competitivo de fabricantes de dispositivos para CuckATOo31+.

Tabela 2: Atribuição de recompensa de mineração. Sujeito a revisão. As atribuições serão direcionadas para alcançar a máxima descentralização e consistentes com os interesses de longo prazo da rede..

Era	1	2	3	4	5	6	7
Dias	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%

Figura 5: Atribuições de recompensa de mineração para cada era de acordo com a Tabela 2. Sujeito a revisão.



[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 Contribuições de Mineração

Começando no Epic Genesis (2019) e concluindo no Epic Singularity (2028), durante o processo de mineração, há uma atribuição de Epic que é redirecionada, como contribuições de mineração, para a EPIC Blockchain Foundation..

A EPIC Blockchain Foundation é dedicada ao desenvolvimento técnico e à promoção da conscientização e utilidade do projeto Epic Cash durante os primeiros anos de sua criação, criando atividades de marketing e desenvolvendo parcerias dentro do setor de tecnologia financeira.

Após a Singularity, o papel da EPIC Foundation será assumido pela EDAC (Distributed Autonomous Corporation), que será desenvolvida pela fundação antes da entrega.

A Fundação EPIC Blockchain é financiada por uma porcentagem dos prêmios de mineração, deduzidos das recompensas do bloco, de acordo com as seguintes taxas anuais:

Tabela 3: Taxas anuais para contribuições de mineração da Fundação como porcentagem das recompensas de mineração.

Ano	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% das Recompensas de Mineração	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Conclusão

A Epic pretende ser reconhecida como "prata digital descentralizada", um meio de troca de contrapartida à posição reconhecida da Bitcoin como ouro digital descentralizado. Ao reintroduzir a fungibilidade perdida em um backbone de hardware muito mais eficiente energético e ecologicamente correto, a Epic Cash inclina o equilíbrio de poder de volta em favor dos usuários individuais, em contraste com as recentes tendências centralizadoras. A combinação da economia Bitcoin, teoria dos jogos e comprovada fórmula proof-of-work com o melhor da tecnologia blockchain contemporânea resulta em uma moeda sem confiança, imutável e descentralizada (Epic) que é escalável, fungível e que protege a privacidade de seus usuários. O blockchain da Epic Cash é aberto, público, sem fronteiras e resistente à censura. Ele preserva a privacidade e a riqueza de seus usuários e recompensa aqueles que implantam seu hardware em suporte à rede por meio de mineração. Cada Epic é minerado através de proof-of-work. A oferta começa em zero e a rede está praticamente lançada, com um testnet funcional atualmente ativa.

Fatos principais da Epic Cash:

- **A mineração começa em Agosto, 2019.**
- **O blockchain da Epic Cash é baseado em MimbleWimble.**

  As características de definição do protocolo são:

  1. **Cut-Through** – a remoção de informações redundantes do blockchain para promover a eficiência espacial, incentivar a participação em larga escala na validação da rede e a descentralização dos administradores;
  2. ***CoinJoin*** – o agrupamento de transações dentro de um bloco para garantir a fungibilidade da criptomoeda Epic;
  3. ***Protocolo Dandelion++*** – a propagação de transações, comunicando-se através de canais interligados, e difundindo através de uma ampla rede de nós, cortando conexões entre transações e sua origem;
  4. **Sem Endereços de Carteira** – o uso de uma grande assinatura múltipla para gerar chaves privadas de uso único para transações de partes, eliminando totalmente a necessidade de endereços de carteira.

- **A política monetária da Epic Cash** está projetada para sincronizar o suprimento circulante da Epic com a oferta circulante de Bitcoin em aproximadamente nove anos, e atingir a mesma oferta máxima de 21 milhões de unidades ao mesmo tempo que Bitcoin, no ano 2140. Essa política inflacionária decrescente garante a transparência, a previsibilidade da oferta, e escassez, promovendo a segurança do armazenamento de valor a longo prazo.

- **Mineração** que incorpora CPUs, GPUs e ASICs através dos algoritmos RandomX, ProgPow e CuckAToo31+ correspondentes, para facilitar a adoção em massa e a eficácia da rede.

IX. Especificações Técnicas

Nome do Projeto: Epic Cash
Nome da Moeda: Epic
Tempo de Bloco: 60 seconds
Tamanho do Bloco: 1 MB
Oferta Inicial: 0
Oferta Final: 21,000,000
Bloco Genesis: Agosto, 2019
Consensus: RandomX (CPUs), ProgPow (GPUs) and CuckAToo31+ (ASICs)

Links:

www.epic.tech

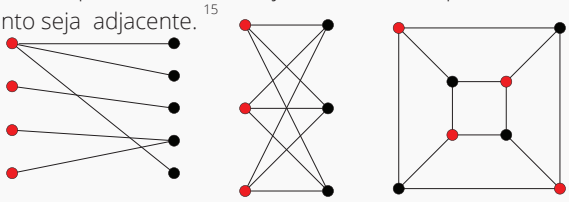
t.me/EpicCash – Telegram

t.me/EpicCashPortuguese

X. Glossário

ASIC Circuitos Integrados Específicos da Aplicação; chips que são projetados para um propósito singular

Bipartite Graph um conjunto de vértices de gráficos decompostos em dois conjuntos de forma que nenhum par de vértices do gráfico dentro do mesmo conjunto seja adjacente. [15]



Fator Cegante um elemento aleatório introduzido em uma mensagem digital para facilitar a criptografia; um segredo compartilhado entre as duas partes que criptografa as entradas e saídas nessa transação específica, bem como as chaves públicas e privadas das partes envolvidas [16].

Recompensa do Bloco a nova Epic distribuída pela rede como recompensa por cálculos realizados para verificar as transações dentro de um novo bloco.

Cache um componente de hardware ou software que armazena dados para que solicitações futuras desses dados possam ser atendidas mais rapidamente.

Oferta Circulante a quantidade de Epic em existência em um determinado ponto no tempo.

CPU Central Processing Unit: componente de computador responsável por interpretar e executar a maioria dos comandos do outro hardware e software do computador.

Cut-Through um processo blockchain MimbleWimble pelo qual as correspondentes entradas e saídas de gasto são removidas para liberar espaço dentro do bloco, reduzindo a quantidade de dados necessários para serem armazenados no blockchain.

Decentralização o estado de dispersão das operações e governança de uma rede.

Emissão a criação de novas Epic ganhas por mineradores em recompensas de bloco. Epic é criada a cada 60 segundos quando as transações são confirmadas no blockchain.

Epic Singularity o ponto em que a oferta de circulação da Epic sincroniza com a oferta circulante da Bitcoin (Maio 2028).

Excesso (MimbleWimble) a diferença entre saídas e entradas, mais assinaturas (para autenticação e prova de não-inflação).

Fungibilidade a propriedade de um bem ou mercadoria pelo qual as unidades individuais são essencialmente intercambiáveis, e cada uma de suas partes é indistinguível de outra parte.

Genesis (Evento) a mineração do primeiro bloco Epic e o início oficial do blockchain.

GPU Graphics Processing Unit: Uma unidade contendo um chip lógico programável (processador) especializado para funções de exibição. GPUs de consumidores podem ser bem adequadas para mineração de criptomoedas.

Halving (de Bitcoin) ocorre a cada 4 anos. A taxa de oferta diminui em 50% após cada evento de halving.

Hash um valor calculado a partir de um número de entrada de base usando uma função de hashing.

Hashing Algorithm (funcão) algoritmo matemático que mapeia dados de tamanho arbitrário para um hash de um tamanho fixo usado para gerar e verificar assinaturas digitais, códigos de autenticação de mensagens (MACs) e outras formas de autenticação.

Criptografia Homomórfica um método de realizar cálculos em informações criptografadas sem descriptografá-las primeiro.

Imutabilidade (em programação) o estado em que um objeto não pode ser modificado após sua criação.

Input (MimbleWimble) o componente de uma transação MimbleWimble representando a parte de envio da transação; criado a partir de saídas de transações anteriores.

I/O input/output; a comunicação entre um sistema de processamento de informações, como um computador, e do mundo exterior, possivelmente um humano ou outro sistema de processamento de informações.

[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/

Oferta Máxima	a quantidade de Epic a ser alcançada no ponto em que a oferta circulante não vai aumentar mais (21,000,000 Epic).
Memory-Hard	o uso de muita RAM para impedir que as conexões simultâneas executem tentativas em paralelo. Funções de memória rígida são algoritmos que têm tempos de computação decididos principalmente pela memória disponível para armazenar dados. Também conhecida como funções ligadas à memória.
Merkle Tree	uma estrutura de dados usada em aplicativos de informática. Em blockchains, as árvores Merkle permitem uma verificação eficiente e segura do conteúdo em grandes estruturas de dados.
MimbleWimble	um protocolo apresentado por um colaborador sob pseudónimo, conhecido pelo apelido Tom Elvis Jedusor, em uma sala de bate-papo de desenvolvedores de Bitcoin.
Multisignature	um esquema de assinatura digital que permite que um grupo de usuários assine um único documento. Geralmente, um algoritmo de multi-assinatura produz uma assinatura conjunta que é mais compacta do que uma coleção de assinaturas distintas de todos os usuários[17].
Nó	um computador que se conecta a uma rede blockchain e se ramifica para outros nós dentro da rede para distribuir informações sobre transações e blocos, de maneira peer-to-peer.
One Way Aggregate Signature (OWAS)	uma assinatura de transação composta de muitas assinaturas que são criptografadas de uma maneira que é muito difícil calcular as assinaturas individuais que fazem parte do agregado.
Output (MimbleWimble)	o componente de uma transação MimbleWimble que representa o recibo da transação; usados como entradas para transações subseqüentes.
Pedersen Commitment Scheme	um primitivo criptográfico que permite que um provador se comprometa com um valor escolhido sem revelar qualquer informação sobre ele e sem que o provador seja capaz de rescindir o comprometimento com o valor.
Chave Privada	uma chave privada é um pequeno pedaço de código que é pareado com uma chave pública para definir algoritmos de criptografia e descriptografia de texto. É criado como parte da criptografia da chave pública durante a criptografia da chave assimétrica e usado para descriptografar e transformar uma mensagem em um formato legível.
Proof of Work (PoW)	um dado que é difícil (caro e demorado) de produzir, mas fácil de ser verificado por outros, e que satisfaz certos requisitos. Proof of Work são frequentemente usadas na geração de blocos de criptomoedas.
Chave Pública	uma chave pública é criada na criptografia da chave pública que usa algoritmos de criptografia de chave assimétrica. Chaves públicas são usadas para converter uma mensagem em um formato ilegível.
RAM (Random Access Memory)	chips de armazenamento de dados de acesso rápido em um dispositivo de computação em que o sistema operacional (SO), os programas aplicativos e os dados em uso atual são mantidos para que possam ser rapidamente alcançados pelo processador do dispositivo.
Rangeproof	uma validação de compromisso que verifica se a soma das transações de entrada é maior que a soma dos resultados das transações de saída e se todos os valores da transação são positivos. Rangeproofs garantem que a oferta monetária não tenha sido adulterada.
(Digital) Assinatura	uma parte padrão de um protocolo blockchain, usado principalmente para proteger transações e blocos de transações, transferência de informações, gerenciamento de contratos e quaisquer outros casos em que detectar e prevenir qualquer adulteração externa é importante. Elas fornecem três vantagens ao armazenar e transferir informações sobre o blockchain: • Elas revelam se os dados enviados foram adulterados; • Verificam a participação de uma determinada parte na transação; • Podem ser juridicamente vinculativas.
SRAM (Static Random Access Memory)	Random Access Memory (RAM) que retém os bits de dados em sua memória enquanto energia estiver sendo fornecida.
Throughput	a medida de transações por segundo que pode ser executada por um determinado protocolo de criptomoeda.
Trustlessness (Sem Confiança)	a qualidade de uma rede de criptomoedas para aderir às regras de um protocolo sem aplicação de lei por uma parte central.

[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