Freeman Family

Ngày 4 Tháng 7, 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

Một hệ thống tiền điện tử ngang hàng

LƯU TRỮ GIÁ TRỊ + PHƯƠNG TIỆN GIAO DỊCH + ĐƠN VỊ TÍNH TOÁN

Hiện nay, có khoảng 1,7 tỷ người trưởng thành không có khả năng tiếp cận đến hệ thống tài chính toàn cầu, trong khi 1,3 tỷ người khác chưa được phục vụ. Epic Cash mở ra tiềm năng cho chúng ta bằng cách kết nối các cá nhân với thị trường toàn cầu. Nhanh chóng, sử dụng gần như miễn phí, và dành cho tất cả mọi người.

Version 7.1b Vietnamese

Mục lục

I. Mở đầu

Epic Cash là đích đến cuối cùng trong cuộc hành trình hướng tới tiền mặt trên Internet P2P thực sự, nền tảng của một hệ thống tài chính cá nhân. Tiền tệ Epic nhắm đến mục tiêu trở thành loại tiền kỹ thuật số bảo vệ sự riêng tư hiệu quả nhất trên thế giới. Để hiện thực mục tiêu này, nó đáp ứng được ba chức năng chính của tiền tệ:

1. **Lưu trữ giá trị** – có thể tiết kiệm, lấy ra, và giao dịch sau một thời gian, và có giá trị dự đoán được khi lấy ra;
2. **Phương tiện giao dịch** – bất cứ điều gì được chấp nhận như là đại diện cho một tiêu chuẩn giá trị và trao đổi hàng hoá, dịch vụ;
3. **Đơn vị tính toán** – đơn vị mà giá trị của một thứ được tính và so sánh.

	$ USD	BTC	EPIC
Lưu trữ giá trị	✗	✓	✓
Phương tiện giao dịch	✓	✗	✓
Đơn vị tính toán	✓	✗	✓

Năm 2009 Bitcoin nổi lên như một loại tiền tệ kỹ thuật số dựa trên blockchain đầu tiên, và cùng với đó là ba đặc điểm xác định để đánh giá các loại tiền mã hóa:

- **Không cần tin cậy** – không ai bị yêu cầu phải tin tưởng bất kỳ thực thể tập trung hoặc đối tác nào để mạng lưới có thể hoạt động;
- **Tính bất biến** – giao dịch không thể thay đổi;
  a. Dường như là bất khả thi hoặc rất khó để viết lại lịch sử;
  b. Nếu không sở hữu một Khóa cá nhân (Private Key), bạn không thể di chuyển số tiền liên quan đến khóa cá nhân đó;
  c. Tất cả các giao dịch được ghi lại trên blockchain.
- **Sự phi tập trung** – "Blockchain là phi tập trung về mặt chính trị (không ai kiểm soát chúng) và phi tập trung về mặt kiến trúc (không có điểm lỗi về mặt hạ tầng)..."[1].

Bitcoin đã thắp sáng nên những con đường mới trong công nghệ khi tôn trọng các nguyên tắc cơ bản đã được thử nghiệm theo thời gian trong cấu trúc chính sách tiền tệ của nó. Sự thành công của Bitcoin gắn liền với nguồn cung hạn chế kết cùng blockchain không cần sự tin cậy, bất biến và phi tập trung. Epic Cash mô phỏng lại chính sách tiền tệ bao gồm sự giảm phát và nguồn cung hạn chế của Bitcoin để đảm bảo Epic Cash có thể đóng vai trò như một nơi lưu trữ giá trị hiệu quả.

Mặc dù Bitcoin đã rất thành công, nó vẫn để lộ những thiếu sót nhất định kể từ khi thành lập cách đây 10 năm. Các dự án khác đã cố gắng khắc phục những thiếu sót này và chúng tôi đã nghiên cứu những điều tốt nhất trong số này để sử dụng làm điểm khởi đầu cho mình. Chúng tôi quyết định sử dụng codebase (cơ sở mã) của Grin và cả kết quả tuyệt vời từ một số dự án khác để giúp chúng tôi hoàn thành những điều khó đạt được và phát hiện ra sai sót của những dự án đi trước. Epic Cash sở hữu những tính chất quan trọng để trở thành một loại tiền tệ lý tưởng:

- **Tính linh hoạt** – Giá trị của một đơn vị Epic nhất định phải luôn bằng một đơn vị Epic khác, giống như một Yên hoặc Yuan luôn bằng và có thể thay thế với một Yên hoặc Yuan khác. Việc đạt được tính linh hoạt đặt nền móng quan trọng cho sự riêng tư.
- **Khả năng mở rộng** – Epic Cash duy trì một blockchain hiệu quả về không gian, theo đó bạn có thể dễ dàng cài đặt các nodes mới mà không cần các thiết bị tốn quá nhiều tài nguyên. Blockchain Epic Cash có khả năng cung cấp thông lượng ít nhất gấp đôi Bitcoin.
- **Tính riêng tư** – Blockchain Epic Cash bảo vệ tính ẩn danh của người giữ và người dùng Epic bằng cách bảo vệ chi tiết giao dịch khỏi các bên thứ ba và được thiết kế để không ai có thể theo dõi và vô hình với những ai muốn giám sát.
- **Tốc độ** – Các giao dịch của Epic Cash diễn ra trơn tru, liên tục và được thực thi nhanh hơn nhiều so với những công nghệ blockchain thế hệ trước. Mặc dù Bitcoin yêu cầu 6 khối, mỗi khối 10 phút để hoàn toàn xác nhận giao dịch, các giao dịch Epic xảy ra trong một xác nhận khối duy nhất ngay khi khối 1 phút được khai thác.

[1] Buterin, Vitalik, ***The Meaning of Decentralization***, 6 Tháng 2, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Tính riêng tư

Việc sử dụng tiền tệ ngày nay có thể được hiểu là việc chuyển nhiều đơn vị tính toán giữa con người và các tổ chức. Bối cảnh tiền tệ tại bất kỳ thời điểm nào đưa ra có thể được xác định bằng cách trả lời các câu hỏi sau:

1. Ai đang giữ nó, và giữ bao nhiêu?

2. Ai đang giao dịch với ai, và với giá bao nhiêu?

Đối với các loại tiền fiat truyền thống, và kể cả Bitcoin, chúng ta có thể trả lời những câu hỏi đó. Bằng cách này, nhiều thứ có thể được tiết lộ về cuộc sống mọi người, chẳng hạn như mô hình tiêu dùng, quyền sở hữu, và các đối tác giao dịch. Một kết luận tương đối chính xác về sở thích và ý định của một cá nhân có thể được đưa ra bằng cách lần theo giao dịch của họ. Nếu không có sự riêng tư, dữ liệu giao dịch thể là thông tin nguy hiểm trong tay của những kẻ săn mồi thuộc bên thứ ba.

Việc sử dụng tiền mã hóa trong một thập kỷ qua cho thấy mức độ "riêng tư" thay đổi liên tục trong các blockchain khác nhau được triển khai. Một thang đo về sự riêng tư nên được xem xét, thay đổi từ mức độ mở và rõ ràng ở điểm đầu cho đến mức ẩn danh ở điểm cuối. Khi tính riêng tư bị xâm phạm, đó là nền tảng thiết yếu cho việc ra đời những đồng tiền mã hóa không cần sự tin tưởng, giảm giá trị. Bằng chứng là sự thành công của các dịch vụ phân tích blockchain Bitcoin, Bitcoin đang dần hướng đến tính minh bạch thực sự ở điểm cuối trong thang đo về sự riêng tư. Người dùng ngày càng phải cẩn thận để đảm bảo mình không vô tình giao dịch với Bitcoin bẩn. Giải pháp Epic Cash hướng đến sự ẩn danh và khôi phục đặc điểm thiết yếu này bằng cách đảm bảo cho cả sự riêng tư của cá nhân và sự riêng tư của các giao dịch đều được thiết kế vào trong hệ thống ở mức cơ bản.

Bảo mật danh tính

Bảo mật giao dịch

Bảo mật danh tính

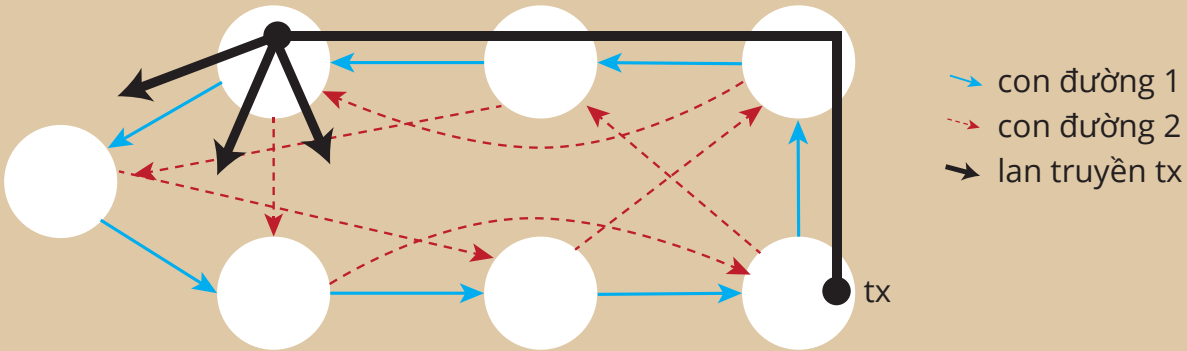
Hầu hết các loại tiền mã hóa như Bitcoin được lưu trữ trong ví có địa chỉ liên quan đến đến khóa công khai (public key) có nguồn gốc từ khóa cá nhân của một ví. Những địa chỉ này có thể được coi là định vị cho một két sắt cá nhân trong thế giới kỹ thuật số. Epic Cash blockchain loại bỏ hoàn toàn các địa chỉ và thay vào đó áp dụng một ví đa chữ ký lớn từ đó tất cả các khóa công khai và khóa cá nhân được tạo ra mỗi một lần sử dụng.

Vì địa chỉ ví Bitcoin là định vị cho một két sắt trong thế giới kỹ thuật số, ví có thể được tra từ địa chỉ Giao thức Internet (IP) của một chủ sở hữu, gắn chủ sở hữu với một máy tính ở một địa điểm duy nhất tại một thời điểm nhất định. Giải thích một cách đơn giản: khi một giao dịch Bitcoin diễn ra, giao dịch được truyền đi từ một trung tâm thông tin gọi là 'nút' và sau đó truyền đến các nút khác gọi là 'peer'. Thông tin này sau đó nhanh chóng lan truyền đến từng nút peer liên tục trên toàn bộ mạng lưới. Quá trình này được khéo léo đặt tên là "Giao thức Gossip". Rất đơn giản, mỗi Bitcoin có một vị trí trực tuyến và một vị trí địa lý hữu hình nơi nó hay đúng hơn là chủ sở hữu Bitcoin có thể được tìm thấy. Như nhà báo Grace Caffyn đã nói, Bitcoin là "không có gì bí mật hơn tìm kiếm Google từ một kết nối internet tại nhà."[2]

Ngoài việc loại bỏ địa chỉ ví, blockchain của Epic Cash còn bảo mật danh tính bằng cách đảm bảo các địa chỉ IP không thể theo dõi. Nó thực hiện điều này thông qua việc tích hợp ***Giao thức Dandelion++ (Giao thức hoa Bồ công anh)***. Được cải thiện so với người tiền nhiệm của nó là ***Giao thức Dandelion gốc***, ***Giao thức Dandelion++*** là một thành tựu của 7 nhà khoa học đã làm việc không ngừng để chống lại các cuộc tấn công vô hiệu hóa tính nặc danh (deanonymization) trên blockchain. Thông qua ***Dandelion++***, các giao dịch được chuyển qua các con đường đan xen ngẫu nhiên, hoặc qua 'cáp', và sau đó được khuếch tán đột ngột đến một mạng lưới các nút lớn, giống như vỏ hoa Bồ công anh khi được thổi bay khỏi thân cây (Hình 1). Điều này làm cho chúng ta gần như không thể tra được nguồn gốc của các giao dịch kể cả địa chỉ IP gốc của chúng.

Hình 1: Giao dịch ẩn danh với *Giao thức Dandelion++*.

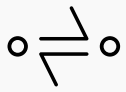
Dandelion++ chuyển tiếp thông điệp qua một trong hai con đường đan xen trên đồ thị tứ phân, sau đó truyền đi bằng cách sử dụng cách khuếch tán. Trong hình, giao dịch lan truyền trên con đường màu xanh lam[3]. Quá trình này khiến việc truy tìm nguồn gốc giao dịch của chúng cực kỳ khó khăn, do đó giữ được sự riêng tư.



[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

Bảo mật giao dịch



Blockchain Epic Cash đảm bảo bảo mật cho giao dịch bằng cách ẩn số tiền và mối liên hệ giữa người gửi và người nhận giao dịch. Nó có khả năng này thông qua việc áp dụng các ý tưởng quen thuộc từ các phương pháp ***Giao dịch tuyệt mật (Confidential Transactions - CT)***[4] và ***CoinJoin***[5], những phương pháp phần lớn được Gregory Maxwell phát triển (nhà phát triển Bitcoin Core, Đồng sáng lập kiêm CTO của Blockstream).

CT, ban đầu được tạo ra bởi Adam Back và về sau được tinh chỉnh bởi Maxwell, hoạt động theo cách chia các giao dịch thành các phần nhỏ hơn thông qua mã hóa đồng cấu (homomorphic encryption), một phương pháp thực hiện tính toán trên thông tin đã được mã hóa mà không cần phải giải mã nó trước để bảo vệ sự riêng tư. Sau khi chia nhỏ giao dịch ra, người quan sát không thể thấy số tiền thực tế trong giao dịch bởi các yếu tố gây mù (blinding factors), đó là một hệ thống đưa các số ngẫu nhiên vào những phần giao dịch đã bị chia nhỏ được trộn lẫn để che giấu giá trị của các phần đó. Cuối cùng, chỉ các bên tham gia giao dịch biết giá trị của giao dịch đó, trong khi giao dịch được xác thực bởi mạng lưới thông qua việc xác nhận rằng tổng các giá trị đầu ra bằng tổng các giá trị đầu vào, và tổng các yếu tố gây mù đầu ra bằng tổng các yếu tố gây mù đầu vào.

Để gây thêm sự phức tạp và khó khăn cho những kẻ tò mò, tất cả giao dịch của Epic Cash đều được gắn với *CT* và sau đó được trộn lẫn với nhau để che giấu các kết nối giữa các bên tham gia giao dịch. Điều này được thực hiện thông qua ý tưởng thứ hai của Maxwell là ***CoinJoin***.

Để minh họa ***CoinJoin*** một cách đơn giản, hãy tưởng tượng A, B và C đang gửi Epic cho X, Y và Z tương ứng. Bằng cách gửi qua phương thức ***CoinJoin***, tất cả những gì được biết là A, B và C đang gửi và X, Y và Z đang nhận, trong khi số tiền giao dịch vẫn được ẩn đi. Hệ thống ***CoinJoin*** là nền tảng cho Epic Cash thông qua Chữ ký tổng hợp một chiều (One-Way Aggregate Signatures - OWAS), kết hợp tất cả các giao dịch bên trong một khối thành một giao dịch duy nhất.

Tính riêng tư: Tóm tắt

Epic Cash blockchain bảo vệ tính riêng tư của cá nhân và các giao dịch bằng cách:

- **Loại bỏ các địa chỉ ví –** Hiện tại không có nhận dạng vị trí nào cho két sắt kỹ thuật số trong blockchain. Giao dịch được xây dựng trực tiếp giữa người với người dựa trên ví;
- ***Giao thức Dandelion++*** **–** che giấu đường đi kỹ thuật số của một giao dịch từ địa chỉ IP của người gửi giao dịch;
- ***Giao dịch tuyệt mật*** **–** chia giao dịch thành nhiều phần và đưa các yếu tố gây mù vào tập hợp các phần đó, nhờ vậy không thể biết được giá trị của các phần và các thông số giao dịch khác;
- ***CoinJoin*** **–** kết hợp các giao dịch thành các gói để che dấu mối liên hệ giữa các bên tham gia giao dịch.

[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. Tính linh hoạt

Charlie Lee, người tạo ra Litecoin đã chỉ ra rằng tính linh hoạt là tính chất duy nhất mà những đồng tiền ổn định như Bitcoin và Litecoin đang còn thiếu, thừa nhận rằng tính riêng tư và tính linh hoạt sẽ là điểm cạnh tranh tiếp theo cho những đồng coin đó[6]. Andreas Antonopoulos, một trong những chuyên gia về blockchain hàng đầu thế giới đã tuyên bố rằng "... những đồng coin bẩn có tính phá hoại. Nếu bạn phá vỡ tính linh hoạt và tính riêng tư, bạn phá vỡ tiền tệ."[7]

Tính linh hoạt là tính chất của một tập các loại hợp hàng hóa hoặc tài sản được đảm bảo các đơn vị riêng lẻ có giá trị như nhau và có thể thay thế cho nhau của tập hợp đó. Đó là những yếu tố phân biệt các hình thức tiền tệ sớm nhất với các hệ thống trao đổi trước đó của chúng. Nếu không có sự bí mật trong tính linh hoạt của đồng tiền, đồng tiền đó nhanh chóng mất đi tiện ích của nó. Như được minh họa dưới đây, tính linh hoạt của hầu hết các loại tiền mã hóa còn khá mơ hồ, trong khi kiến trúc bảo mật của Epic Cash đảm bảo cho nó không bị ảnh hưởng bởi các mối đe dọa tương tự.

Hầu hết các loại tiền mã hóa đều tương tự như Bitcoin vì bản chất là chúng đang hoạt động trên các blockchain minh bạch, có thể theo dõi chính xác mọi ví mà chúng được giữ. Các công ty tư nhân thứ ba và chính phủ cũng giám sát blockchain Bitcoin bằng các phương tiện ngày càng tinh vi để nhanh chóng xác định những hoạt động mà đồng coin đã được sử dụng trước đó. Điều này theo tự nhiên dẫn đến mối lo ngại rằng một ngày nào đó những đồng coin bẩn có thể bị cấm giao dịch, khiến cho những người lương thiện giữ chúng về sau bị mất số đó.

Vào ngày 19 tháng 3 năm 2018, Văn phòng Kiểm soát Tài sản Nước ngoài (OFAC) của Hoa Kỳ tuyên bố rằng họ đang cân nhắc việc đưa các địa chỉ tiền kỹ thuật số vào danh sách các Quốc Gia được Chỉ định Đặc biệt (SDNs), đó là những đối tượng mà người dân hoặc doanh nghiệp Hoa Kỳ bị cấm giao dịch. Thậm chí đáng lo ngại hơn khi OFAC chưa loại trừ khả năng sẽ tính cả các địa chỉ hiện đang giữ các đồng coin bẩn trong danh sách SDN, điều này sẽ khiến những người chủ sở hữu coin bẩn vô tội hiện tại bị đưa vào danh sách đen hình sự do dính líu đến các đồng coin bẩn từ những chủ sở hữu trước. Điều này đã khiến giáo sư về pháp lý Andrew Hinkes của Đại học New York mỉa mai, "hôn tạm biệt tính linh hoạt", và công chúng nên mong đợi "một bảo hiểm cho những đồng coin mới được tạo ra hoặc những đồng coin sạch..."[8].

Nếu điều này tiếp tục tiến triển, không khó để tưởng tượng một biến động trong thị trường crypto và sự sụt giảm hay thậm chí cái chết của nhiều loại tiền mã hóa cho dù có được thiết lập tốt. Tuy nhiên, Epic là một trong số ít các loại tiền mã hóa hoàn toàn tránh được vấn đề này do những tính năng bảo mật mạnh mẽ đã được mô tả trong tài liệu này. Bằng cách loại bỏ liên kết giữa danh tính và quyền sở hữu cũng như mối quan hệ giữa các bên giao dịch, Epic sẽ không bao giờ bị liên kết với một người hoặc một hoạt động. Do đó, giá trị của Epic sẽ vẫn tách biệt với người dùng và đem lại cấp độ riêng tư và bảo mật cao, các tác nhân độc hại không thể dễ dàng thao túng nó trong phạm vi hình sự, tài chính hoặc chính trị.

> **“...NHỮNG ĐỒNG COIN BẨN CÓ TÍNH PHÁ HOẠI. NẾU BẠN PHÁ VỠ TÍNH LINH HOẠT VÀ TÍNH RIÊNG TƯ, BẠN PHÁ VỠ TIỀN TỆ.”**
>
> **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. Khả năng mở rộng

Epic Cash triển khai blockchain MimbleWimble mang lại những tiến bộ về khả năng mở rộng nhờ một thiết kế hiệu quả về mặt không gian giúp loại bỏ những dữ liệu giao dịch thừa. Chức năng Cut-Through (cắt xuyên) chịu trách nhiệm cho vấn đề này đảm bảo cho blockchain phát triển không gian hiệu quả hơn theo thời gian, không giống như hầu hết các loại tiền mã hóa khác, kể cả Bitcoin, và có thể tạo ra các nút mới với chỉ một khoản đầu tư tối thiểu vào bộ nhớ và sức mạnh tính toán. Bằng cách duy trì không gian hiệu quả, nó tạo ra một mạng lưới phân tán rộng rãi và đẩy mạnh sự phi tập trung. Hơn nữa, trong khi mỗi nút Bitcoin phải lưu trữ toàn bộ dữ liệu của chuỗi, các nút Epic Cash có thể đóng góp vào bảo mật mạng lưới chỉ cần dựa trên một tập hợp các khối nhỏ.

Phần lớn các loại tiềnmã hóa đều yêu cầu lưu trữ vĩnh viễn tất cả dữ liệu giao dịch trên blockchain của họ. Chuỗi Bitcoin hiện đang tăng thêm 0,153 GB bộ nhớ mỗi ngày, trong khi chuỗi Ethereum tăng với tốc độ thậm chí còn nhanh hơn là 0,2719 GB mỗi ngày. Nếu chuỗi Bitcoin tiếp tục tăng trưởng với tốc độ hiện tại, nó sẽ đạt kích cỡ khoảng 6 TB khi khối phần thưởng cuối cùng được khai thác vào năm 2140, và vào thời điểm đó Ethereum sẽ vượt qua mức 10 TB[9]. Trong hầu hết các blockchains không sử dụng công nghệ MimbleWimble, giao dịch phải được xác nhận qua toàn bộ các nút. Khi dữ liệu tăng lên thì gánh nặng trên mỗi nút cũng tăng theo. Thậm chí chỉ ở mức 200 GB (kích thước xấp xỉ của chuỗi Bitcoin hiện tại), đồng bộ hóa dữ liệu đòi hỏi một mạng lưới ổn định và ổ cứng có dung lượng cũng như tốc độ đọc và viết cao .

Do đó, việc khai thác đã trở nên ngày càng tập trung giữa các Pool khai thác lớn đang tận dụng nguồn tài nguyên tính toán đắt đỏ. **Nếu toàn bộ lịch sử blockchain của Bitcoin được lưu trữ trên blockchain Epic Cash, nó sẽ chỉ chiếm không gian ít hơn gần 90%.** Nhỏ hơn có nghĩa là nhanh hơn vì mỗi giao dịch cần ít thời gian hơn để truyền đi và bảo mật.

MimbleWimble giải quyết vấn đề nan giải trong việc lưu trữ này bằng một phương pháp lược bớt khối sáng tạo, được gọi là 'Cut-Through'. Để hiểu cách thức hoạt động của Cut-Through, trước hết hãy tìm hiểu cách các giao dịch và khối được tạo trong một blockchain MimbleWimble.

Đầu vào:

Tham chiếu đến đầu ra cũ;

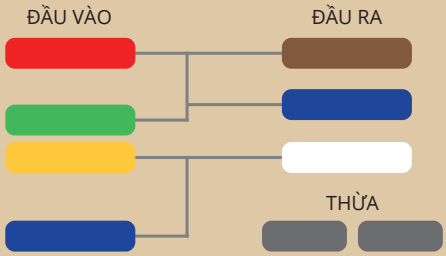
Đầu ra:

Đầu ra *Giao dịch tuyệt mật* và **rangeproofs**;

Vượt quá::

Sự khác biệt giữa đầu ra và đầu vào, cộng với **chữ ký** (để xác thực và để chứng minh không lạm phát).

Hình 2:
Các thành phần giao dịch của MimbleWimble.



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

Tất cả các khối của Epic Cash bao gồm:

Cây Merkle của đầu vào giao dịch;

Cây Merkle của đầu ra giao dịch và rangeproofs;

Danh sách các giá trị và chữ ký thừa.

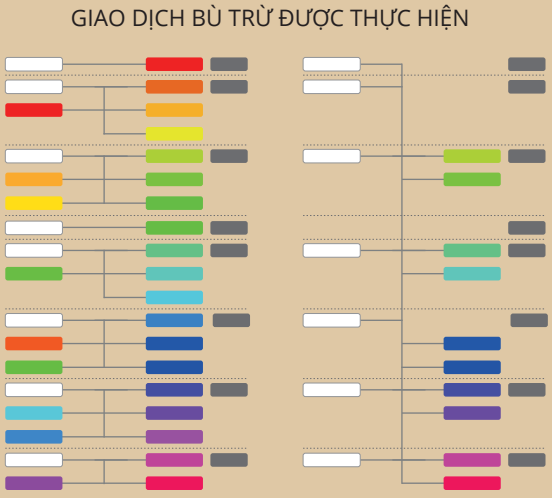
Ở Hình 2 và 3, được điều chỉnh từ các bài thuyết trình của Andrew Poelstra[10], chúng ta có thể thấy Epic được khai thác mới dưới dạng các ô đầu vào màu trắng. Các ô có màu giống nhau đại diện cho đầu ra với đầu vào tương ứng. Với quá trình Cut-Through, đầu vào và đầu ra phù hợp đã được loại bỏ để giải phóng không gian trong khối, giúp giảm lượng dữ liệu cần được lưu trữ trên blockchain. Trong khi các giao dịch được bỏ qua từ sổ cái, các kernel (hạt nhân) thừa còn lại (vỏn vẹn 100 byte) ghi nhận vĩnh viễn rằng các giao dịch đã diễn ra.

Khi các khối tiếp tục được tạo ra, MimbleWimble áp dụng Cut-Through vào các khối, nhờ vậy mà trong thời gian dài nó chỉ để lại các tiêu đề khối (khoảng 250 byte), giao dịch chưa được dùng và kernel giao dịch (khoảng 100 byte). Grin, dự án MimbleWimble thứ hai được triển khai, cho thấy một chuỗi MimbleWimble có số lượng giao dịch tương tự với chuỗi Bitcoin, gần bằng 10% kích thước của chuỗi Bitcoin[11]. Hơn nữa, kích thước của một nút sẽ "theo trình tự vài GB cho một chuỗi có kích thước cỡ Bitcoin, và có khả năng tối ưu hóa đến vài trăm MB."[12]

Nó tương phản rõ rệt với Bitcoin, nơi mỗi nút phải lưu trữ toàn bộ blockchain. Theo thời gian, khi hiệu quả không gian của blockchain Epic Cash tăng lên so với blockchain của Bitcoin, các nút tham gia vào mạng lưới Epic Cash cũng đạt được hiệu quả chi phí. Rào cản tham gia thấp hơn giúp đảm bảo khả năng phục hồi quan trọng ở lớp nút của thiết kế mạng lưới.

Thông qua việc triển khai MimbleWimble và áp dụng lược bỏ chuỗi với quy trình Cut-Through, blockchain Epic Cash mang lại khả năng mở rộng theo cách thường bị bỏ qua bởi cộng đồng tiền mã hóa. Nó nắm bắt được bản chất của Bitcoin và các dự án cùng chung ý tưởng: sự phi tập trung. Bất kể có bao nhiêu giao dịch mỗi giây một đồng coin có thể xử lý, nó có lợi ích gì nếu nó không thể được duy trì bởi một mạng lưới rộng lớn và đa dạng? Nếu yêu cầu bộ nhớ là như vậy mà việc xác nhận cuối cùng hấp dẫn các tập đoàn khai thác lớn, sau đó tất cả những nỗ lực của cộng đồng tiền mã hóa để tạo ra một hệ sinh thái phi tập trung đã bị ngăn cản. Để cung cấp thêm thông lượng, việc triển khai Lớp 2 theo kiểu Lightning đã được lên kế hoạch như một mục tiêu ngắn hạn trong lộ trình phát triển của Epic Cash.

Hình 3:
Giao dịch MimbleWimble trước và sau 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. Chính sách tiền tệ

Chính sách tiền tệ của Epic Cash và Bitcoin rất giống nhau. Nguồn cung lưu hành của Epic Cash ban đầu mở rộng nhanh chóng và sau đó đồng bộ với tổng cung lưu hành Bitcoin vào năm 2028. Sau đó nó tăng với tốc độ giảm dần cho đến khi đạt đến tổng cung tối đa 21 triệu Epic vào năm 2140. Epic Cash có những tính chất để trở thành một nơi lưu trữ giá trị lâu dài an toàn vì tổng cung lưu hành được xác định tại bất kỳ thời điểm nào trong chu trình phát hành của nó và đạt đến mức tổng cung tối đa cố định. Chính sách tiền tệ của Epic Cash được đặc trưng bởi 4 tính năng sau:

- Phát hành nhanh chóng trong 9 năm đầu tiên, trong đó 20.343.750 Epic (96.875% tổng nguồn cung) sẽ được khai thác. Tỷ lệ phát hành chính xác được nêu trong phần Lịch trình phát hành của tài liệu này;
- Tổng cung tối đa 21 triệu Epic sẽ đạt được vào năm 2140, gần như cùng với lúc Bitcoin đạt tổng cung tối đa 21 triệu đơn vị;
- Tỷ lệ tổng cung lưu hành và phát hành của Epic đồng bộ hóa với Bitcoin tại Điểm kì dị Epic vào khoảng ngày 24 tháng 5 năm 2028. Theo Điểm kì dị (Singularity), tỉ lệ phát hành giảm ngày càng nhanh, trong khi nguồn cung lưu hành tăng ngày càng chậm;
- Epic có cấu trúc 8 chữ số thập phân, sao cho: 1 Epic tương đương với 100.000.000 freeman (như 1 Bitcoin tương đương với 100.000.000 satoshi).

Chính sách tiền tệ của Epic Cash được mô hình hóa theo Bitcoin, vì những lý do sau:

- Đồng ý với các nguyên tắc kinh tế cơ bản của Bitcoin, cụ thể là sự khan hiếm và khả năng dự đoán tổng cung lưu thông làm cơ sở cho tính chất lưu trữ giá trị mạnh mẽ của nó;
- Công chúng đã quen thuộc với mô hình Bitcoin và bản ghi có thể theo dõi đã được chứng minh trong 10 năm qua kể từ khi thành lập. Bằng cách đồng bộ hóa tương đương với tổng cung lưu hành của Bitcoin và phản ánh cấu trúc tổng cung tối đa và phân chia của Bitcoin, Epic chọn con đường ít trở ngại nhất để có thể áp dụng số lượng lớn.

VI. Lịch trình phát hành

Epic Cash có tổng cộng 33 thời kì khai thác, mỗi thời kì được xác định bằng cách giảm phần thưởng khối, liên quan đến thời kì trước của chúng. .Epic Genesis là ngày khối Epic đầu tiên được khai thác, diễn ra vào ngày tháng 8 năm 2019. Các khối được khai thác một khối mỗi phút. Năm thời kì đầu tiên tạo ra đến gần 97% tổng cung tối đa của Epic, sẽ khớp với 20 năm phát hành Bitcoin trong khoảng 9 năm. Đây có thể được coi là cơ hội để quay ngược thời gian cho những ai đã bỏ lỡ cơ hội với Bitcoin.

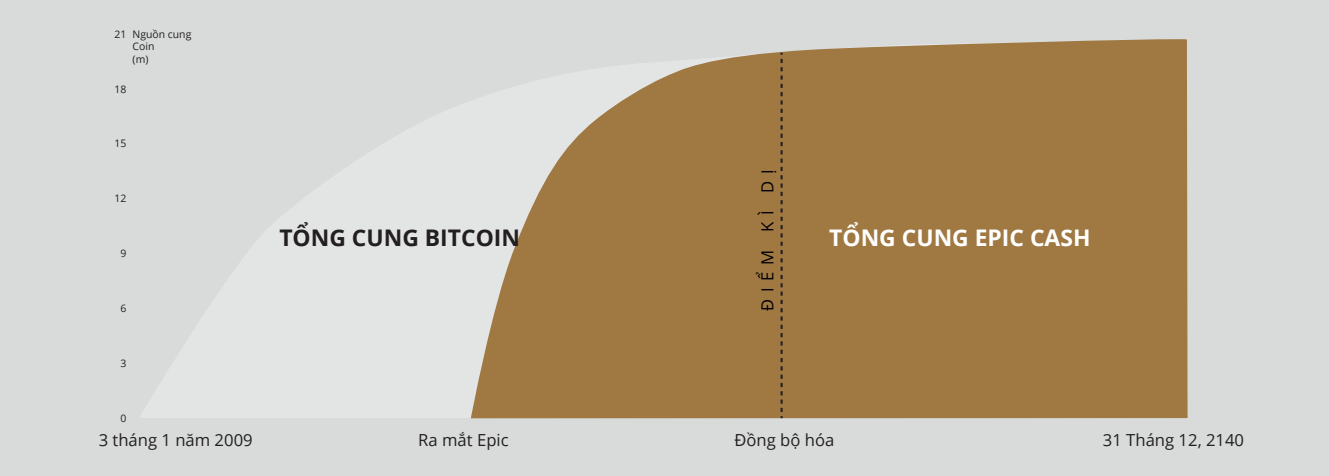
Lịch trình phát hành trong bảng 1 phác thảo ngày bắt đầu và kết thúc của 7 thời kì khai thác đầu tiên, phần thưởng khối tương ứng của chúng và tổng cung lưu thông tiếp theo cho mỗi thời kì. Các thời kì từ 8 đến 33 không được cho vào bảng để cho nó ngắn gọn hơn. Đối với những thời kì đó, chỉ cần hiểu rằng mỗi thời kì tiếp theo sẽ có phần thưởng khối bằng một nửa phần thưởng khối của thời kì ngay liền trước, chính xác như Bitcoin. Lượng Epic phát hành trong mỗi thời kì này sẽ là tổng số phần thưởng khối trong thời kì 4 năm (khoảng 1460 ngày).

Tại Điểm kì dị Epic (2028), tổng cung lưu hành Epic sẽ bằng tổng cung lưu hành Bitcoin, tại thời điểm đó, Epic Cash chấp nhận phần thưởng khối Bitcoin và mô hình halving, ở đó phần thưởng khối giảm một nửa sau mỗi 4 năm. Khác biệt duy nhất là các khối Epic tiếp tục được khai thác với tốc độ một lần mỗi phút, so với tốc độ của Bitcoin là một khối sau 10 phút. Bằng cách này, tổng cung lưu hành Epic duy trì ngang bằng với tổng cung lưu hành của Bitcoin trong phần còn lại vòng đời của chúng.

Bảng 1: Lịch trình phát hành cho 7 thời kì khai thác đầu tiên. Ngày tháng là gần đúng.

Thời kì	1	2	3	4	5	ĐIỂM KÌ DỊ	6	7
Phần thưởng khối	16	8	4	2	1		0.15625	0.078125
Ngày bắt đầu	1 Tháng 8 2019	29 Tháng 6 2020	11 Tháng 10 2021	3 Tháng 6 2023	10 Tháng 8 2025		May 24, 2028	May 22, 2032
Ngày kết thúc	29 Tháng 6 2020	11 Tháng 10 2021	3 Tháng 6 2023	10 Tháng 8 2025	24 Tháng 5 2028		May 22, 2032	May 20, 2036
Độ dài (tính theo ngày)	334	470	601	800	1019		1460	1460
Nguồn cung khi bắt đầu	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Nguồn cung lúc kết thúc	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% tổng cung tối đa	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Hình 4: Lịch trình phát hành của Epic và Bitcoin.



VII. Khai thác

Blockchain Epic Cash theo đuổi sự phi tập trung bằng cách hỗ trợ nhiều loại phần cứng tính toán. Khai thác Epic ban đầu dành cho CPUs, GPUs, và ASICs, sử dụng 3 thuật toán băm tương ứng: RandomX, ProgPow, và CuckATOO31+. Các thuật toán có thể được hoán đổi bình thường mà không ảnh hưởng đến tính toàn vẹn của chuỗi.

1 RandomX và CPUs

RandomX là một thuật toán Bằng chứng công việc (PoW) được tối ưu hóa cho CPU với mục đích chung. Nó sử dụng các chương trình thực thi ngẫu nhiên với một số kĩ thuật memory-hard để đạt được các mục tiêu sau:

- Ngăn chặn sự phát triển của ASIC chip đơn;
- Giảm thiểu lợi thế khai thác của phần cứng chuyên dụng so với CPU với mục đích chung.

Khai thác Epic bằng CPU yêu cầu phân bổ liền kề 2 GB RAM vật lý, 16 KB L1 cache, 256 KB L2 cache, và 2 MB L3 cache mỗi thread khai thác[13]. Các thiết bị chạy Windows 10 yêu cầu RAM tối thiểu 8 GB trở lên. Không khó để tưởng tượng một ngày trong tương lai không xa điện thoại di động thể trở thành các nút khai thác khả thi. Tích hợp CPU từ sớm trong mạng khai thác Epic Cash là cơ hội tuyệt vời cho nhiều người chỉ có những thiết bị tính toán khiêm tốn để kiếm được phần thưởng khối bằng cách giúp bảo mật mạng lưới Epic Cash.

2 ProgPow và GPUs

Bằng chứng công việc có thể lập trình (ProgPow) là một thuật toán phụ thuộc vào băng thông bộ nhớ và lõi tính toán của các chuỗi toán học ngẫu nhiên, tận dụng lợi thế từ tính năng tính toán của GPU và do đó đạt được hiệu quả trong tổng chi phí năng lượng phần cứng. Vì ProgPow được thiết kế đặc biệt để tận dụng tối đa khả năng của GPU thương mại nên việ dùng phần cứng chuyên dụng đạt được hiệu quả cao hơn sẽ rất khó khăn và tốn kém. Do đó, thuật toán ProgPow giảm thiểu lợi thế của các pool ASIC lớn so với GPU, như thường thấy với nhiều thuật toán PoW khác, chẳng hạn như SHA-256 của Bitcoin. GPU mặc dù không phổ biến như CPU nhưng vẫn được dùng tương đối nhiều trong khai thác. Với sự phát triển công nghệ được thúc đẩy bởi các nhà sản xuất Nvidia và AMD, GPU có thể xử lý song song nhiều giải pháp khai thác trên mỗi đơn vị CPU. Chính vì sự kết hợp giữa tính phổ biến và khả năng xử lý cao này, GPU sẽ là xương sống cho phần lớn hoạt động khai thác trong thời kì đầu, được chỉ ra trong Bảng 2.

3 CuckATOO+31 và ASICs

CuckATOO31+ là một hoán đổi thân thiện với ASIC của thuật toán Cuckoo Cycle được phát triển bởi nhà khoa học máy tính người Hà Lan John Tromp. Một họ hàng của thuật toán CuckARoo29 kháng ASIC là CuckATOO31+ tạo ra các đồ thị lưỡng cực ngẫu nhiên và chỉ định máy đào với nhiệm vụ tìm một vòng lặp có độ dài N cho trước, đi qua các đỉnh của đồ thị đó.

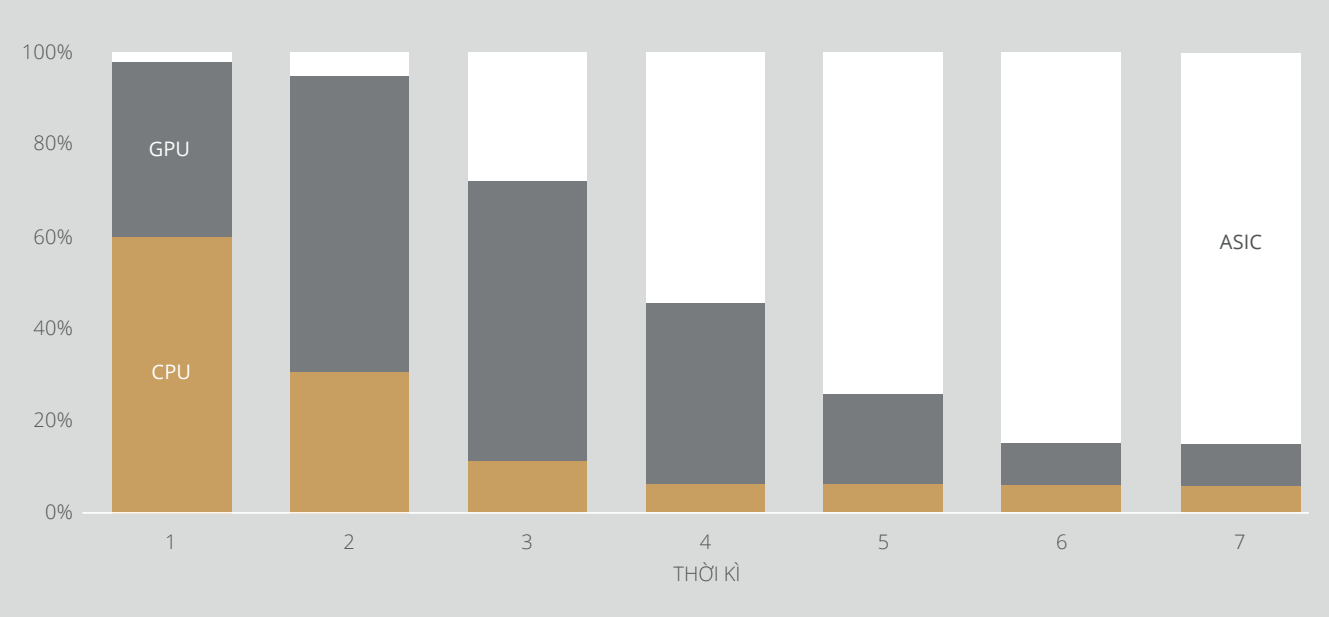
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Đây là một tác vụ giới hạn bộ nhớ, có nghĩa là thời gian giải quyết bị giới hạn bởi băng thông bộ nhớ thay vì bộ vi xử lý thô hay tốc độ xử lý của GPU. Do đó, thuật toán Cuckoo Cycle tạo ra ít nhiệt hơn và tiêu thụ năng lượng ít hơn đáng kể so với thuật toán PoW truyền thống. Thuật toán thân thiện với ASIC CuckATOo31+ giúp cải thiện hiệu quả so với GPU bằng cách sử dụng hàng trăm MB từ SRAM trong khi vẫn bị tắc nghẽn bởi I/O bộ nhớ[14]. Cuối cùng, ASIC mang lại quy mô nền kinh tế có tiềm năng lớn nhất với 3 tùy chọn khai thác. Tuy nhiên, vì lợi ích trong đó, mặc dù chúng được phân bổ một phần nhỏ phần thưởng khai thác so với CPU và GPU từ đầu thì đến cuối cùng, ASIC vẫn chiếm phần lớn stake phần thưởng được khai thác, với giả thiết là sẽ có một hệ sinh thái cạnh tranh cho các nhà sản xuất thiết bị CuckATOo31+.

Bảng 2: Phân bổ phần thưởng khai thác. Có thể thay đổi. Phân bổ sẽ được chuyển hướng để đạt được sự phi tập trung tối đa và phù hợp với lợi ích lâu dài của mạng lưới.

Thời kì	1	2	3	4	5	6	7
Ngày	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%

Hình 5: Phân bổ phần thưởng khai thác cho từng thời kì theo Bảng 2. Có thể thay đổi.



[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 Đóng góp cho khai thác

Bắt đầu từ Epic Genesis (khối khởi thủy) (2019) và kết thúc tại Điểm kì dị Epic (2028), trong quá trình khai thác, Epic sẽ được phân bổ mà được chuyển hướng, như những đóng góp khai thác cho EPIC Blockchain Foundation.

EPIC Blockchain Foundation được thành lập dành riêng cho mục đích phát triển kỹ thuật và thúc đẩy nhận thức và tiện ích của dự án Epic Cash trong những năm đầu thành lập, bằng cách tạo ra các hoạt động marketing và phát triển quan hệ đối tác trong ngành công nghệ tài chính.

Sau thời điểm Điểm kì dị, vai trò của EPIC Foundation sẽ được đảm nhận bởi Tổ chức tự trị phân tán EPIC (EDAC), được phát triển bởi tổ chức EPIC trước khi bàn giao.

EPIC Blockchain Foundation được tài trợ bởi tỷ lệ khai thác, được trích ra từ phần thưởng khối theo tỷ lệ hàng năm như sau:

Bảng 3: Tỷ lệ đóng góp cho Tổ chức hàng năm từ khai thác theo phần trăm phần thưởng khai thác.

Năm	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% Phần thưởng khai thác	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Kết luận

Epic nhắm tới mục tiêu được công nhận là 'bạc kỹ thuật số phi tập trung', một phương tiện giao dịch so với Bitcoin được công nhận là vàng kỹ thuật số phi tập trung. Bằng cách cải thiện tính linh hoạt trên xương sống là phần cứng tiết kiệm năng lượng và thân thiện với môi trường hơn, Epic Cash giúp cân bằng lại quyền lực đem lại lợi ích cho người dùng cá nhân, trái ngược hoàn toàn với xu hướng tập trung gần đây. Sự kết hợp giữa nền kinh tế Bitcoin, lý thuyết trò chơi và công thức Bằng chứng công việc đã được chứng minh với công nghệ blockchain tốt nhất, kết quả là tạo ra một loại tiền tệ đáng tin cậy, bất biến và phi tập trung (Epic) có khả năng mở rộng, có tính linh hoạt và bảo vệ sự riêng tư của người dùng. Blockchain Epic Cash có tính mở, công khai, không biên giới và không bị kiểm duyệt. Nó bảo vệ sự riêng tư và tài sản của người dùng, thưởng cho những người sử dụng phần cứng của họ để khai thác giúp hỗ trợ mạng lưới. Mỗi Epic được khai thác tồn tại thông qua bằng chứng công việc. Nguồn cung bắt đầu từ con số 0 và mạng lưới được coi như ra mắt công bằng, với một testnet hiện đang hoạt động.

Thông tin chính của Epic Cash :

- **Khai thác bắt đầu từ ngày tháng 8, 2019.**
- **Blockchain Epic Cash dựa trên MimbleWimble.**

  Các tính năng định nghĩa nên giao thức là:

  1. **Cut-Through** – loại bỏ thông tin dư thừa ra khỏi blockchain để tăng cường hiệu quả về không gian, khuyến khích tham gia theo quy mô lớn để xác thực mạng và quản lý phi tập trung;
  2. ***CoinJoin*** – gói các giao dịch vào trong một khối để đảm bảo tính linh hoạt của tiền mã hóa Epic;
  3. ***Giao thức Dandelion++*** – việc truyền các giao dịch đi bằng cách truyền thông tin qua các kênh đan xen và khuếch tán qua một mạng lưới các nút rộng lớn, chia rẽ kết nối giữa các giao dịch và nguồn gốc của chúng;
  4. ***Không có địa chỉ ví*** – việc sử dụng ví đa chữ ký chính để tạo khóa cá nhân sử dụng một lần cho các bên giao dịch, loại bỏ hoàn toàn nhu cầu cho địa chỉ ví.

- **Chính sách tiền tệ Epic Cash** được thiết kế để đồng bộ hóa tổng cung lưu hành của Epic với tổng cung lưu hành của Bitcoin trong khoảng 9 năm và đạt tổng cung tối đa 21 triệu đơn vị cùng lúc với Bitcoin vào năm 2140. Chính sách lạm phát giảm dần này đảm bảo tính minh bạch, giúp dự đoán được nguồn cung và sự khan hiếm, đảm bảo an toàn cho việc lưu trữ giá trị lâu dài.

- **Khai thác** kết hợp CPU, GPU và ASIC thông qua các thuật toán RandomX, ProgPow và CuckATOO31+ tương ứng, để tạo thuận lợi cho việc áp dụng hàng loạt và đem lại hiệu quả cho mạng lưới.

IX. Thông số kỹ thuật

Tên dự án: Epic Cash
Tên tiền tệ: Epic
Thời gian khối: 60 giây
Kích thước khối: 1 MB
Nguồn cung ban đầu: 0
Nguồn cung cuối cùng: 21,000,000
Khối khởi thủy: Tháng 8, 2019
Thuật toán đồng thuận: RandomX (CPU), ProgPow (GPU) và CuckAToo31+ (ASIC)

Liên kết:

www.epic.tech

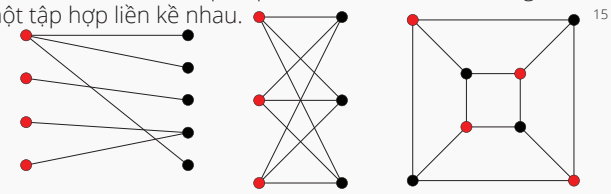
t.me/EpicCash – Telegram

t.me/EpicCashVietnamese

X. Bảng chú giải

ASIC Vi mạch tích hợp chuyên dụng; chip được thiết kế cho một mục đích duy nhất.

Đồ thị 2 phía một tập hợp các đỉnh đồ thị bị phân tách thành hai tập hợp khác nhau sao cho không có hai đỉnh đồ thị nào trong cùng một tập hợp liền kề nhau.[15]



Yếu tố gây mù một yếu tố ngẫu nhiên được đưa vào một thông điệp kỹ thuật số để hỗ trợ việc mã hóa; một bí mật chung giữa hai bên mã hóa đầu vào và đầu ra trong giao dịch cụ thể đó, cũng như khóa công khai và khóa cá nhân của các bên giao dịch[16].

Phần thưởng khối Epic mới được phân phối trong mạng lưới dưới dạng phần thưởng cho các tính toán được thực hiện để xác minh giao dịch trong một khối mới.

Cache một thành phần phần cứng hoặc phần mềm lưu trữ dữ liệu nhờ đó các yêu cầu trong tương lai cho dữ liệu đó có thể được đáp ứng nhanh hơn.

Tổng cung lưu hành số lượng Epic tồn tại tại một thời điểm nhất định.

CPU Bộ xử lý trung tâm: thành phần máy tính chịu trách nhiệm phiên dịch và thực thi hầu hết các lệnh từ máy tính cũng như phần cứng và phần mềm khác của máy tính.

Cut-Through một quá trình của blockchain MimbleWimble theo đó những đầu vào và đầu ra khớp nhau đã bị loại bỏ để giải phóng không gian trong khối, giảm lượng dữ liệu cần được lưu trữ trên blockchain.

Phi tập trung trạng thái phân tán của hoạt động và quản trị một mạng lưới.

Phát hành việc tạo ra Epic mới kiếm được từ thợ mỏ trong phần thưởng khối. Epic được tạo ra sau mỗi 60 giây khi các giao dịch được xác nhận trên blockchain.

Điểm kì dị Epic thời điểm mà tổng cung lưu hành của Epic đồng bộ hóa với tổng cung lưu hành của Bitcoin (tháng 5 năm 2028).

Thừa (MimbleWimble) sự khác biệt giữa đầu ra và đầu vào, cộng với chữ ký (để xác thực và để chứng minh không lạm phát).

Tính linh hoạt tính chất của hàng hóa, theo đó các đơn vị riêng lẻ về cơ bản có thể hoán đổi cho nhau và mỗi bộ phận của nó không thể phân biệt được với bộ phận khác.

Khởi thủy (Sự kiện) việc khai thác khối Epic đầu tiên và sự khởi đầu chính thức của blockchain.

GPU Bộ xử lý đồ họa: Một đơn vị chứa chip logic được lập trình (bộ xử lý) chuyên dùng cho chức năng hiển thị. GPU thương mại rất phù hợp để khai thác tiền mã hóa.

Halving (cho Bitcoin) xảy ra mỗi 4 năm. Tỷ lệ nguồn cung giảm 50% sau mỗi sự kiện Halving.

Hash (băm) một giá trị được tính từ một số đầu vào cơ sở bằng cách sử dụng hàm băm.

Thuật toán băm (chức năng) thuật toán toán học ánh xạ dữ liệu có kích cỡ tùy ý thành một băm có kích thước cố định được sử dụng để tạo và xác minh chữ ký số, mã xác thực tin nhắn (MAC) và các loại xác thực khác.

Mã hóa đồng cấu một phương pháp thực hiện tính toán trên thông tin được mã hóa mà không giải mã trước.

Tính bất biến (trong lập trình) trạng thái trong đó một đối tượng không thể được sửa đổi sau khi tạo ra.

Đầu vào (MimbleWimble) thành phần của một giao dịch MimbleWimble đại diện cho bên gửi giao dịch; được tạo từ đầu ra của các giao dịch trước đó.

I/O đầu vào/ đầu ra; giao tiếp giữa một hệ thống xử lý thông tin như máy tính và thế giới bên ngoài, hoặc có thể là con người hoặc hệ thống xử lý thông tin khác.

[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/

Tổng cung tối đa số lượng Epic sẽ đạt được tại thời điểm tổng cung lưu hành không tăng về sau (21,000,000 Epic).

Memory-Hard việc sử dụng rất nhiều RAM để ngăn chặn các kết nối đồng thời đang cố chạy các tác vụ song song. Chức năng Memory-Hard là các thuật toán có thời gian tính toán chủ yếu được quyết định bởi bộ nhớ khả dụng để giữ dữ liệu. Nó còn được gọi là chức năng giới hạn bộ nhớ.

Cây Merkle một cấu trúc dữ liệu được sử dụng trong các ứng dụng khoa học máy tính. Trong blockchain, cây Merkle cho phép xác thực nội dung hiệu quả và an toàn trong những cấu trúc dữ liệu lớn.

MimbleWimble một giao thức được đưa ra bởi một người đóng góp có bút danh Tom Elvis Jedusor, trong một phòng chat của các nhà phát triển Bitcoin.

Đa chữ ký một mô hình chữ ký số cho phép một nhóm người cùng ký một tài liệu. Thông thường, thuật toán đa chữ ký tạo ra một chữ ký chung nhỏ gọn hơn một tập hợp các chữ ký riêng biệt từ tất cả người tham gia[17].

Nút một máy tính kết nối với mạng blockchain và chia nhánh đến các nút khác trong mạng lưới để phân tán thông tin về các giao dịch và khối một cách ngang hàng.

Chữ ký tổng hợp một chiều (OWAS) một chữ ký giao dịch bao gồm nhiều chữ ký được mã hóa theo cách rất khó để tính toán các chữ ký riêng lẻ trong tập hợp đó.

Đầu ra (MimbleWimble) thành phần của một giao dịch MimbleWimble đại diện cho việc nhận giao dịch; được sử dụng làm đầu vào cho các giao dịch tiếp theo.

Lược đồ cam kết Pedersen một mã hóa nguyên thủy cho phép một người cam kết với một giá trị đã chọn mà không tiết lộ bất kỳ thông tin nào về nó và không có người đó thì không thể hủy bỏ cam kết với giá trị.

Khóa cá nhân một khóa cá nhân là một đoạn mã nhỏ được ghép nối với khóa công khai để đặt ra thuật toán mã hóa và giải mã văn bản. Nó được tạo ra như một phần của mật mã khóa công khai trong quá trình mã hóa khóa bất đối xứng và được sử dụng để giải mã và chuyển đổi một thông điệp thành định dạng có thể đọc được.

Bằng chứng công việc (PoW) một loại dữ liệu khó tạo ra (tốn kém và mất thời gian), nhưng dễ dàng cho người khác xác minh và đáp ứng các yêu cầu nhất định. Bằng chứng công việc thường được sử dụng trong việc tạo khối tiền mã hóa.

Khóa công khai một khóa công khai được tạo trong mật mã mã hóa sử dụng thuật toán mã hóa khóa bất đối xứng. Khóa công khai được sử dụng để chuyển đổi thông điệp thành định dạng không thể đọc được.

RAM (Bộ nhớ truy cập tạm thời) các chip lưu trữ dữ liệu truy cập tạm thời trong một thiết bị máy tính nơi hệ điều hành (OS), các chương trình ứng dụng và dữ liệu đang sử dụng được lưu giữ để chúng có thể nhanh chóng tiếp cận với bộ xử lý của thiết bị..

Rangeproof xác thực cam kết rằng tổng đầu vào giao dịch lớn hơn tổng đầu ra giao dịch và tất cả các giá trị giao dịch đều dương. Rangeproofs đảm bảo rằng nguồn cung tiền tệ không bị giả mạo với một phần tiêu chuẩn của giao thức blockchain, chủ yếu được sử dụng để bảo mật các giao dịch và giao dịch trong khối, chuyển thông tin, quản lý hợp đồng và bất kỳ trường hợp nào yêu cầu khả năng phát hiện và ngăn chặn giả mạo bên ngoài. Chúng cung cấp ba lợi thế của việc lưu trữ và truyền thông tin trên blockchain:

Chữ ký (Số)
- Chúng tiết lộ việc dữ liệu được gửi có bị giả mạo không;
- Xác minh sự tham gia của một bên cụ thể trong giao dịch;
- Có thể ràng buộc về mặt pháp lý.

SRAM (Bộ nhớ truy cập ngẫu nhiên tĩnh) Bộ nhớ truy cập ngẫu nhiên (RAM) giữ lại các bit dữ liệu trong bộ nhớ của nó miễn là được cấp năng lượng.

Thông lượng đo lường số giao dịch mỗi giây có thể được thực hiện bởi một giao thức tiền mã hóa cụ thể.

Không cần sự tin tưởng chất lượng của một mạng lưới tiền mã hóa tuân thủ các quy tắc của giao thức mà không cần sự ép buộc của một bên trung tâm.

[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