Sách Trắng Bitcoin Vault

Eyal Avramovich, Kacper Wiśniewski, Piotr Kozłowski, Radek Popiel et Anon

Sách Trắng v1.0

Tóm tắt

Năm 2009, một cá nhân ẩn danh hoặc một nhóm các nhà phát triển ẩn danh đã tạo ra mạng ngang hàng đầu tiên dựa trên công nghệ blockchain cho phép người dùng chuyển tiền giữa các địa chỉ băm ẩn danh. Cuộc cách mạng Bitcoin đã bắt đầu. Nó dẫn đến một loạt các fork của khái niệm ban đầu.

Một trong số đó đã dẫn đến khái niệm Bitcoin Vault.

Mục đích của chúng tôi với tư cách các nhà phát triển là nâng cấp blockchain hiện có với các tính năng độc đáo giúp người dùng có sự kiểm soát tốt hơn và nâng cao mức độ an toàn của họ với cách quản lý địa chỉ ví, lưu trữ khóa cá nhân và khóa công khai cũng như tài sản được chuyển giữa các cá nhân. Chúng tôi muốn tạo ra một đồng tiền cung cấp tất cả các lợi thế của Bitcoin với các tính năng bổ sung để người dùng có thể kiểm soát tối đa tài sản của họ một cách dễ dàng và thuận tiện mà không ảnh hưởng đến tính linh hoạt mà tiền điện tử mang lại.

Với tính bất biến của blockchain là tính năng chính đằng sau sổ cái phân tán, chúng tôi không chỉ thấy được những lợi thế mà còn – từ kinh nghiệm của chính mình – những mối nguy hiểm liên quan đến tiền bị mất, thất lạc hoặc bị đánh cắp. Với một số thay đổi trong mã và cách sử dụng khóa riêng và khóa công khai trong hệ sinh thái blockchain, chúng tôi đã đưa ra ý tưởng làm cho các giao dịch không thể đảo ngược có thể đảo ngược mà không ảnh hưởng đến tính bất biến của blockchain.

Nội dung

Giới thiệu

Bitcoin Vault (BTCV) được ra mắt vào năm 2019 dưới dạng alpha chain. Nó đã được phát triển mạnh mẽ từ tháng 12 năm 2019 đến tháng 11 năm 2020, chứng kiến việc phát hành tính năng chính cho phép các giao dịch có thể đảo ngược trên blockchain.

Bitcoin Vault là tiền điện tử đầu tiên trên thế giới cho phép người dùng hủy giao dịch sau khi chúng được đăng lên blockchain. Cách tiếp cận mang tính chất cách mạng này có thể thực hiện được với một giao thức blockchain tùy chỉnh xác nhận các khoản thanh toán trong vòng 144 khối (hoặc khoảng 24 giờ). Tính năng này bảo vệ người dùng khỏi bị mất tiền trong trường hợp xảy ra các vụ trộm chìa khóa thông thường, lỗi của người dùng hoặc lỗi hệ thống.

Bitcoin Vault là một hard fork của Bitcoin Royale, được thêm một khóa cá nhân vào quy trình, nâng tổng số lên ba. Kể từ khi ra mắt vào cuối năm 2019, chúng tôi đã mở rộng nền tảng kỹ thuật và thị trường phù hợp với lộ trình đầy tham vọng kéo dài đến năm 2022 và hơn thế nữa.

Mô tả vấn đề

Theo Báo cáo Chống Rửa tiền và Tội phạm Tiền điện tử Mùa xuân 2020 của CipherTrace, trong 5 tháng đầu năm 2020, tổng số tiền trộm cắp, hack và gian lận tiền điện tử đạt 1,36 tỷ đô la.

Các sàn giao dịch tiền điện tử luôn phải thu hồi tiền của người dùng đã bị gửi nhầm đến sai địa chỉ hàng ngày. Điều này khiến họ tốn kém cả thời gian và tiền bạc và không đảm bảo rằng tiền của người dùng sẽ được thu hồi.

Không có nguồn đáng tin cậy về số lượng tài sản tiền điện tử, tiền điện tử, tiền mã hóa đang được chuyển mỗi ngày đến các địa chỉ lừa đảo nổi tiếng, tin tặc hoặc đang bị mất do các loại tấn công Man-In-The-Middle.

Chúng tôi tin rằng có thể tránh được một phần đáng kể những điều nêu trên nếu người dùng có khả năng hủy và đảo ngược các giao dịch gửi đi ngay khi nhận ra rằng mình mắc lỗi, tài sản đã bị đánh cắp hoặc ai đó có quyền truy cập trái phép vào ví tiền điện tử.

Sứ mệnh & tầm nhìn

BTCV được phát triển để cung cấp thêm một cấp độ bảo mật dựa trên Giải pháp Bảo mật 3 Khóa cho phép người dùng đảo ngược một số loại giao dịch nhất định trên blockchain. Nó có tất cả sự tiện lợi của Bitcoin trong khi bổ sung các tính năng quan trọng cho phép người dùng minh bạch và tự do. Bitcoin Vault là câu trả lời của chúng tôi cho các vấn đề mà cộng đồng tiền điện tử phải đối mặt trong thập kỷ qua, chủ yếu là:

1. Truy cập trái phép vào ví do bị hack hoặc truy cập khóa cá nhân của người dùng,
2. Sai lầm của con người với việc gửi tài sản tiền điện tử đến sai địa chỉ ví hoặc các loại sai lầm khác liên quan đến việc nhập nhầm số tiền chuyển hoặc trộn số tiền chuyển với số tiền gas,
3. Lỗi và các vấn đề khác liên quan đến phần mềm tiền điện tử.

Sự phát triển của BTCV tập trung vào các tính năng bảo mật và an toàn, sự tiện lợi của người dùng và trải nghiệm người dùng vì chúng tôi tin rằng đó là những thách thức chính ngăn cản phần lớn xã hội trở thành một phần của cộng đồng tiền điện tử toàn cầu.

Cách tiếp cận của BTCV

Tiền điện tử cho phép người dùng tự do và chịu trách nhiệm về cách họ lưu trữ, quản lý và chuyển tiền trên các mạng P2P. Trong sách trắng này, chúng tôi giả định rằng mọi người dùng tiền điện tử nên quen thuộc với khái niệm khóa cá nhân và khóa công khai và biết cách lưu trữ và bảo mật khóa một cách an toàn. Dựa trên giả định này, chúng tôi đã phát triển một cách tiếp cận mới để quản lý khóa và cách sử dụng nó cho các loại giao dịch khác nhau.

Giải pháp bảo mật 3 khóa

Bitcoin Vault đã phát triển Giải pháp Bảo mật 3 Khóa yêu cầu người dùng tạo ba khóa Elliptic Curve Digital Signature Algorithm (ECDSA) – một khóa được lưu trữ tự động trong ứng dụng và hai khóa còn lại cần được người dùng quản lý. Thiết lập hiện tại trong Bitcoin Vault cho phép người dùng hủy giao dịch đã bắt đầu và chuyển ngược nó sang địa chỉ ví hiện có hoặc địa chỉ ví mới.

Giải pháp hỗ trợ ba khóa ECDSA với các vai trò khác nhau trong hệ sinh thái:

- Khóa Giao dịch Tiêu chuẩn được tạo tự động và hoạt động ở chế độ nền. Khóa này cần thiết để bắt đầu tất cả các giao dịch và để khôi phục ví trong trường hợp bị hack hoặc gặp sự cố kỹ thuật.
- Khóa Giao dịch Hủy cho phép người dùng thực hiện các giao dịch Hủy trong khoảng 24 giờ, sau khi 144 khối được tạo.
- Khóa Giao dịch Nhanh cung cấp cho người dùng khả năng thực hiện các giao dịch Nhanh An toàn và chuyển BTCV chỉ trong vài phút.

Hệ sinh thái Bitcoin Vault

Hệ sinh thái của Bitcoin Vault bao gồm ba ứng dụng được tạo nội bộ chỉ nhằm mục đích lưu trữ và quản lý BTCV. Cùng với nhau, chúng tạo thành một công cụ mạnh mẽ đảm bảo tiêu chuẩn cao hơn về bảo mật, minh bạch và tự do.

Gold Wallet

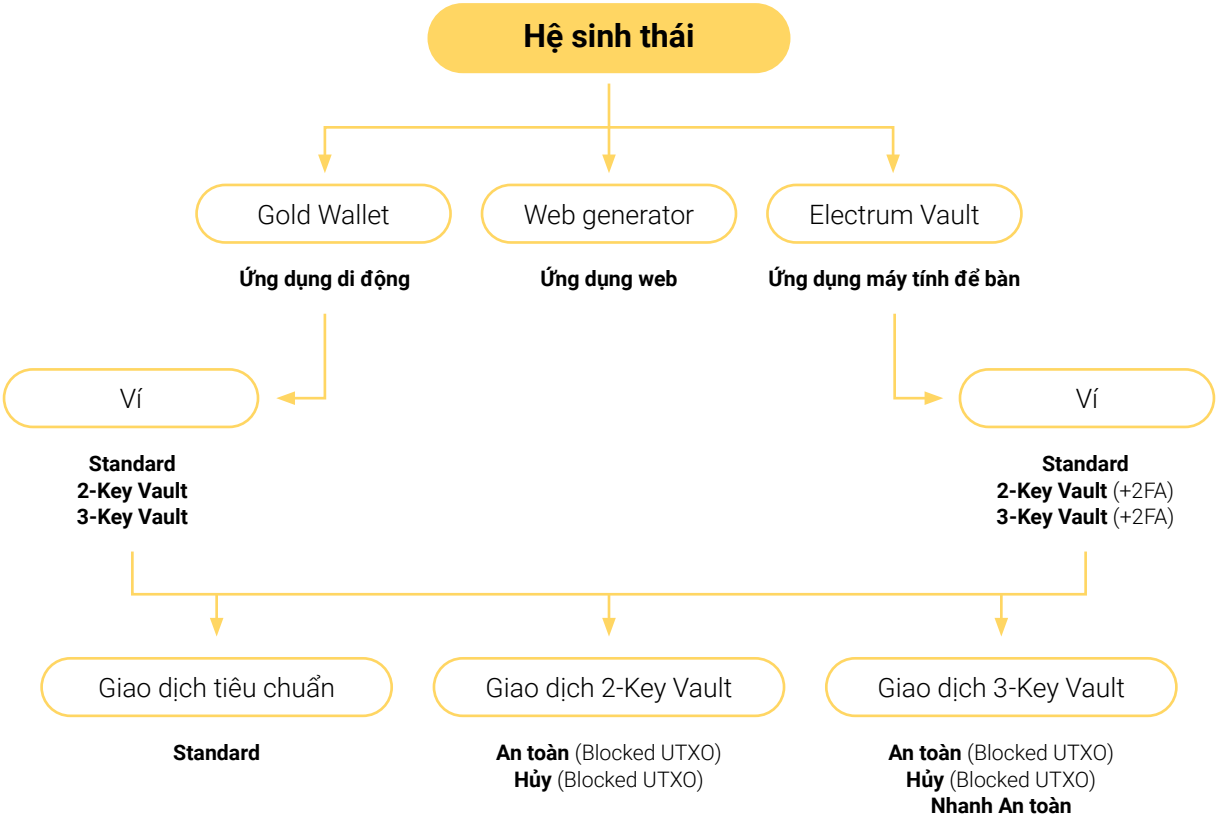
Gold Wallet là một ứng dụng dành cho thiết bị di động được thiết kế để lưu trữ, gửi và nhận BTCV. Nó cho phép người dùng tạo ba loại ví và thực hiện nhiều loại giao dịch khác nhau, bao gồm Giao dịch Nhanh An toàn, Giao dịch An toàn và Giao dịch Hủy. Gold Wallet cũng có thể được sử dụng làm công cụ xác thực cho xác thực hai yếu tố (2FA) cho ứng dụng máy tính để bàn Electrum Vault.

Key Generator

Key Generator là một ứng dụng dựa trên web để tạo ra các khóa công khai và cá nhân riêng, cần thiết để thiết lập ví và thực hiện giao dịch. Nó chỉ sử dụng tài nguyên cục bộ, có nghĩa là quá trình tạo khóa, cũng như chính các khóa, không bao giờ rời khỏi thiết bị của người dùng. Chúng không được lưu trữ ở bất cứ đâu và không thể truy cập trực tuyến. Các khóa được lưu trữ ngoại tuyến, mang lại mức độ an toàn cao nhất.

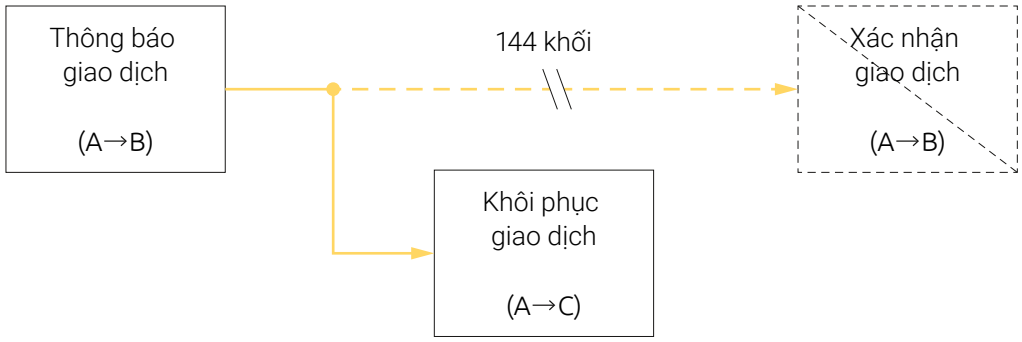
Electrum Vault

Electrum Vault là một ứng dụng dành cho máy tính để bàn dựa trên Ví Electrum mã nguồn mở. Nó có tất cả các tính năng của Gold Wallet, có nghĩa là nó có thể được sử dụng để lưu trữ, gửi và nhận BTCV, tạo ví và thực hiện các giao dịch, bao gồm Giao dịch Nhanh An toàn, Giao dịch An toàn và Giao dịch Hủy.

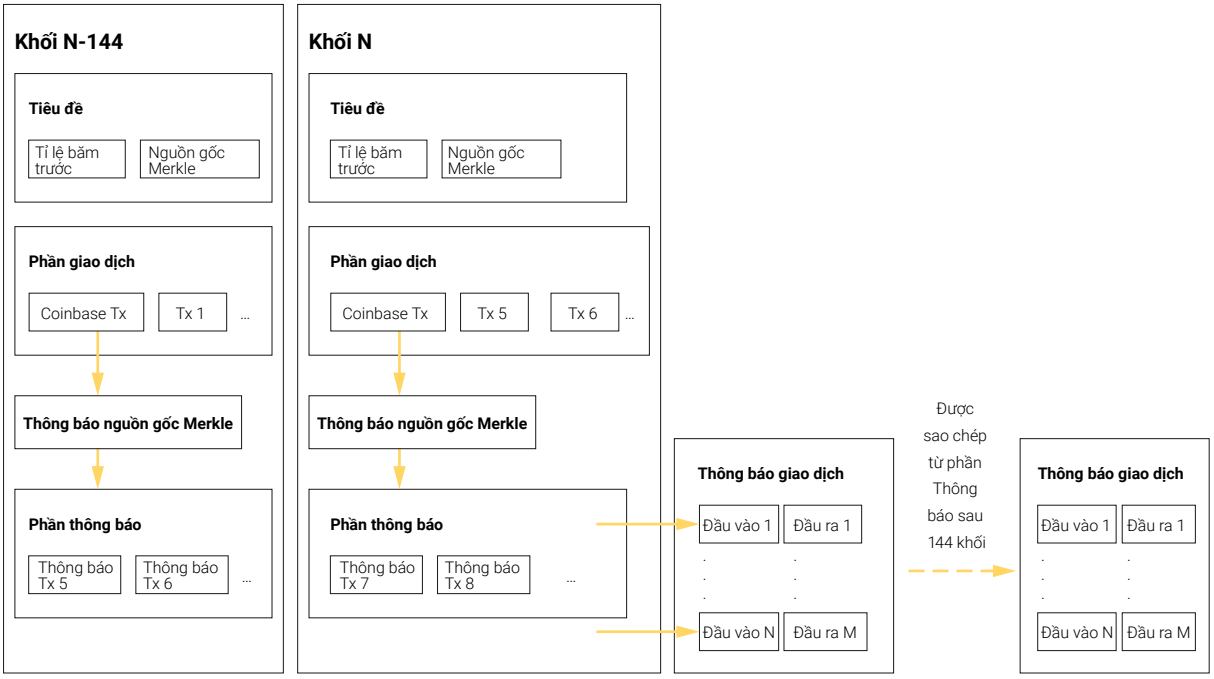


Tổng quan về kỹ thuật

Tập lệnh khóa, độ trễ mặc định là 144 khối, các giao dịch cảnh báo trên chuỗi:



Cấu trúc Khối BTCV với phần cảnh báo (cách nó được lưu trữ, điều gì sẽ xảy ra khi giao dịch thay đổi trạng thái từ cảnh báo sang xác nhận, cách thợ mỏ xác minh khi giao dịch thay đổi trạng thái).



Cảnh báo Giao dịch thay đổi vòng đời của UTXO.

Trong phiên bản tiêu chuẩn, UTXO có hai trạng thái: chưa chi tiêu và đã chi tiêu (về cơ bản có nghĩa là nó đã bị xóa). Một phiên bản mới của Bitcoin Vault giới thiệu một trạng thái mới – đã xác nhận. Điều này thay đổi cách UTXO được lưu trữ trong cơ sở dữ liệu. Từ bây giờ, trạng thái "đã xác nhận" là thời điểm UTXO bị xóa khỏi cơ sở dữ liệu và trạng thái đã chi tiêu khóa UTXO và lưu trữ thông tin về chiều cao khối mà nó đã được chi tiêu. Bằng cách này, hệ thống sẽ đợi Cảnh báo Giao dịch được xác nhận trước khi xóa UTXO.

Đây là một cách tiếp cận cần thiết bởi vì, cho đến khi nhận được xác nhận, Cảnh báo Giao dịch có thể được khôi phục với Giao dịch Khôi phục (nó chỉ sử dụng UTXO bị khóa làm đầu vào). Cách tốt nhất để thay đổi vòng đời của UTXO trong ứng dụng là lưu trữ thông tin về độ cao mà chúng đã chi tiêu – độ cao đã chi tiêu. Thông tin mới này sẽ xác định UTXO ở trạng thái nào:

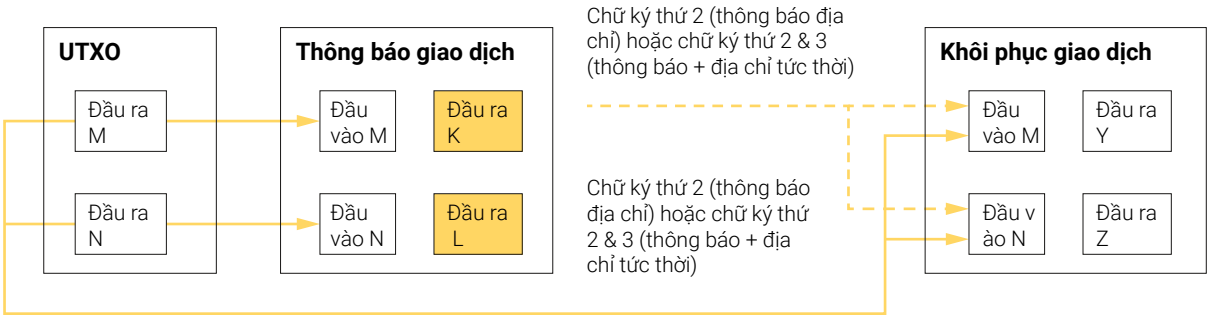
- 0 khi chưa chi tiêu,
- >0 khi đã chi tiêu.

Ngoài ra, cùng một thông tin cần được xem xét trong cấu trúc Hoàn tác. Danh sách Hoàn tác lưu trữ thông tin về các trạng thái trước đó của UTXO ở các độ cao khác nhau và sử dụng thông tin đó khi việc tổ chức lại chuỗi xảy ra.

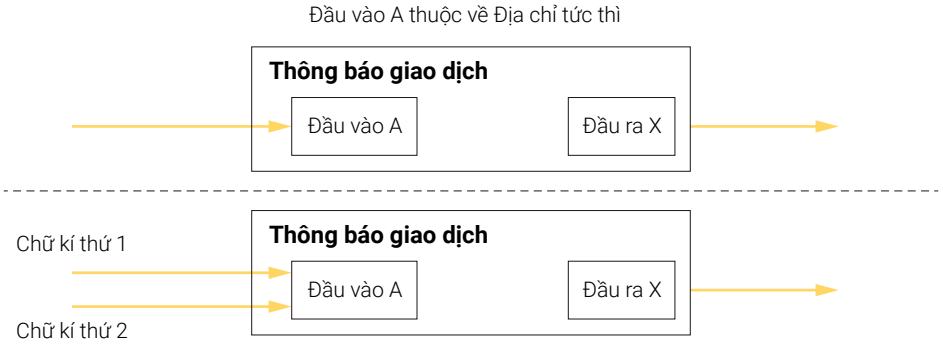
Các trạng thái UTXO mới và các loại giao dịch cũng có tác động đến số dư mà người dùng có thể nhìn thấy. UTXO ở trạng thái đã chi tiêu sẽ được tính là số dư mới và sẽ hiển thị trong số dư đã xác nhận. Nó không

thể được tính là số dư chưa xác nhận vì số dư đó liên quan đến các giao dịch chưa xác định và có thể chi tiêu. Ý tưởng là tạo ra số dư không thể chi tiêu nhưng có nhiều thông tin:

- cảnh báo gửi đi – được tính trong số UTXO ở trạng thái đã chi tiêu, bị khóa bởi Cảnh báo Giao dịch,
- cảnh báo gửi đến – được tính trong số UTXO sẽ khả dụng sau khi xác nhận Cảnh báo Giao dịch..



Cách thức hoạt động của Giao dịch Nhanh (giải thích về thời gian trễ 24 giờ, điều gì khiến nó có thể thực hiện được – đa chữ ký):



Proof-of-Work

Bitcoin Vault là một đồng tiền Proof-of-Work dựa trên mã nguồn mở Bitcoin Royale. Với hardfork được thực hiện vào ngày 17 tháng 11 năm 2020, việc khai thác hợp nhất với Bitcoin (BTCV) đã được triển khai.

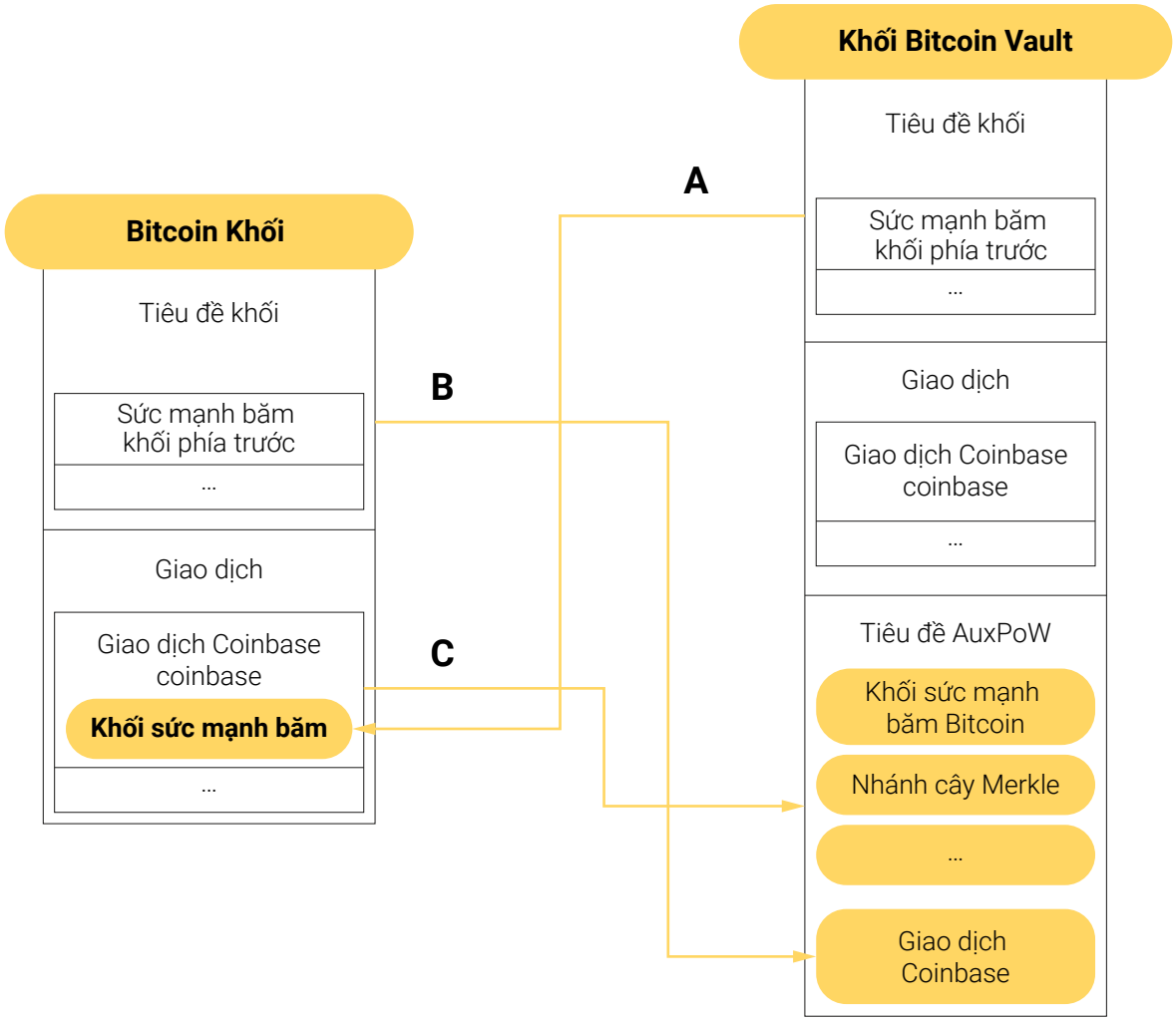
Khai thác hợp nhất

Cùng với bản cập nhật lớn của giao thức BTCV ở số khối 58.420, Bitcoin Vault cũng đã được điều chỉnh để chấp nhận khai thác hợp nhất. Khai thác hợp nhất, còn được gọi là Proof-of-Work Phụ trợ, là một quá trình mà các thợ mỏ đồng thời tìm kiếm PoW cho ít nhất hai loại tiền điện tử riêng biệt có cùng sức mạnh tính toán. Tuy nhiên, để xây dựng mối quan hệ như vậy giữa các blockchains – cha mẹ và phụ trợ – dễ dàng nhất là khi chuỗi phụ trợ được chuẩn bị cho sự thay đổi.

Trong Bitcoin Vault, khai thác hợp nhất đã được thực hiện với Bitcoin, vì cả hai loại tiền điện tử đều sử dụng hàm băm SHA-256. Trong trường hợp này, BTC là chuỗi mẹ và BTCV là chuỗi phụ.

Do đó, các giải pháp proof-of-work của Bitcoin (mẹ) có thể được sử dụng để xác thực Bitcoin Vault (chuỗi phụ) như một cơ chế đồng thuận phụ trợ proof-of-work (AuxPoW).

Giải thích kỹ thuật với ví dụ đồ họa về cấu trúc khối và mối quan hệ giữa khối BTC và BTCV:



Với việc triển khai khai thác hợp nhất với giao thức, các thợ mỏ BTCV được khuyến khích bởi khả năng nhận được hai phần thưởng khối từ cả hai blockchain BTC và BTCV. Một động lực bổ sung là nhờ sức mạnh băm bổ sung được thêm vào mạng bằng cách cõng mạng Bitcoin với tốc độ băm cao hơn, bảo mật mạng được tăng lên.

Phần thưởng khối

Bitcoin Vault có tổng nguồn cung là 21 triệu đồng tiền và thời gian khai thác một khối ước tính là 10 phút.

Phần thưởng khối Bitcoin Vault được thiết kế để loại bỏ một số vấn đề nhất định phát sinh ở giai đoạn đầu của quá trình phát triển tiền điện tử. Hai vấn đề chính đã được xác định:

Khoảng thời gian ban đầu để có được những người mới tham gia là quá ngắn để tiếp cận đúng số lượng thành viên cộng đồng cần thiết cho sự phát triển bền vững của dự án.

Phần thưởng khối sau giai đoạn đầu giảm mạnh. Điều này có thể dẫn đến việc không khuyến khích các thợ mỏ tham gia sâu hơn vào quá trình khai thác và dẫn đến giảm đáng kể sức mạnh băm.

Để ngăn chặn các mối đe dọa như vậy, Bitcoin Vault đã đề xuất các giải pháp sau:

- Để kéo dài thời gian với phần thưởng khối cao hơn đến 46 tháng.
- Chia giai đoạn này thành chín giai đoạn phụ ngắn hơn, cứ sau sáu tháng, với mức giảm phần thưởng khối dần dần.

Điều này cho phép đội ngũ đứng đằng sau dự án có đủ thời gian để phát triển. Cộng đồng có cơ hội phát triển lên số lượng đáng kể, các thợ mỏ được khuyến khích tham gia vào mạng lưới ngay từ những ngày đầu trong thời gian dài hơn và có đủ thời gian để số lượng đồng tiền bắt kịp với Bitcoin trong khi không làm giảm mạnh phần thưởng khối.

Trong khoảng thời gian đó, việc giảm phần thưởng khối được lên lịch theo cách như sau:

Ngày	Giảm Phần thưởng BTCV	Số Giai đoạn Phụ	Phần thưởng Khối	Thời gian Giai đoạn Phụ	Khối Giai đoạn Phụ
tháng 5 năm 2020	từ 175 xuống 150	1	175	6 months	29850
tháng 11 năm 2020	từ 150 xuống 125	2	150	6 months	26600
tháng 5 năm 2021	từ 125 xuống 100	3	125	6 months	26600
tháng 11 năm 2021	từ 100 xuống 75	4	100	6 months	26600
tháng 5 năm 2022	từ 75 xuống 50	5	75	6 months	26600
tháng 11 năm 2022	từ 50 xuống 25	6	50	6 months	26600
tháng 5 năm 2023	từ 25 xuống 12.5	7	25	6 months	26600
tháng 11 năm 2023	từ 12.5 xuống 6.25	8	12.5	6 months	26600
tháng 5 năm 2024	từ 6.25 xuống 3.125	9	6.25	6 months	26600

As a result, 19,687,500 coins are going to be distributed during this period, catching up and meeting the number of Bitcoins by its 4th halving (estimated in March 11, 2024). After that, the BTCV block reward will follow Bitcoin's halving schedule.

Sự phát triển của Bitcoin Vault

Các giai đoạn phát triển BTCV:

Tháng 5 2019 – Tháng 12 2019	Pre-Alpha
Tháng 12 2019 – Tháng 9 2020	Alpha
Tháng 9 2020 – Tháng 11 2020	Beta
Tháng 11 2020	Mainnet

Mainnet

Mainnet đã được khởi chạy thành công vào ngày 17 tháng 11 năm 2020 với số chiều cao khối là 58.420.

Lộ trình

Vào tháng 12 năm 2020, Đội ngũ Phát triển BTCV đã đưa ra lộ trình mới bao gồm các năm 2021-2022. Việc phát triển tiếp theo của BTCV được chia thành sáu workstream:

Workstream số 1 – Nâng cấp phát triển

Workstream phát triển liên quan đến tất cả các nâng cấp blockchain sẽ được thêm vào Bitcoin Vault. Mục tiêu chính của workstream này là tham gia vào hệ sinh thái Dapp xung quanh Ethereum 2.0 với Wrapped BTCV (wBTCV) cho đến cuối năm 2021.

- Qúy 1 năm 2021
  - wBTCV ERC-20 token – phân tích & tokenomics đằng sau wBTCV
- Qúy 2 năm 2021
  - Tích hợp sổ cái
- Qúy 3 năm 2021
  - wBTCV ERC-20 token giai đoạn thử nghiệm beta
- Qúy 4 năm 2021
  - Ra mắt wBTCV
  - Bắt đầu tích hợp với hệ sinh thái DeFI
- Qúy 1 năm 2022
  - Tích hợp hoàn toàn với hệ sinh thái DeFI
  - Phát triển Dapps
- Qúy 2 năm 2022+
  - Phát triển Dapps

Workstream số 2 – Nâng cấp bảo mật

Bitcoin Vault có một đội ngũ chuyên gia bảo mật blockchain nội bộ. Tính toàn vẹn của Mainnet blockchain đã được xác minh nhiều lần và vào năm 2021, mục tiêu chính của chúng tôi sẽ là củng cố mã và xác định bất kỳ lỗi và lỗ hổng nào còn lại với sự hỗ trợ của các đối tác bên ngoài. Sau các thử nghiệm thâm nhập nội bộ và bên ngoài, chúng tôi sẽ chạy một chương trình tiền thưởng mở cho các nhà phát triển và hợp tác chặt chẽ với cộng đồng 'mũ trắng'.

- Qúy 1 năm 2021
  - Kiểm tra toàn bộ mã (nội bộ & bên ngoài)
- Qúy 2 năm 2021
  - Kiểm tra thâm nhập (nội bộ)
- Qúy 3 năm 2021
  - Kiểm tra thâm nhập (bên ngoài)
- Qúy 4 năm 2021
  - Kiểm tra bảo mật CIS/20
  - Ma trận Bảo mật Mây
- 2022+
  - Cải tiến bảo mật tiếp theo & kiểm toán
  - Hackathons
  - Chương trình tiền thưởng

Workstream số 3 – Nâng cấp trải nghiệm người dùng

Trải nghiệm người dùng là một trong những yếu tố quan trọng nhất đằng sau việc sử dụng và tiếp nhận sản phẩm. Mục đích của chúng tôi là phát triển và nâng cấp hơn nữa các ứng dụng và điều chỉnh chúng theo nhu cầu của nhiều người dùng dựa trên phản hồi từ cộng đồng.

- Qúy 1 & Qúy 2 năm 2021
  - Ứng dụng di động GoldWallet cải tiến UX
  - Ứng dụng di động Electric Vault chuyển đổi chế độ đơn giản và chuyên gia
- Qúy 3 năm 2021
  - GoldWallet thông báo người dùng
- Qúy 4 năm 2021
  - Tích hợp GoldWallet với các ứng dụng bên thứ 3
- 2022+
  - Cải tiến thêm UX

Workstream số 4 – Sản phẩm

Cùng với việc phát triển Công nghệ Thông tin, chúng tôi đang tập trung mạnh mẽ vào việc tiếp nhận thị trường với các sản phẩm mới đang được triển khai. Vào năm 2021, chúng tôi muốn ra mắt sản phẩm đặt cược với sự hỗ trợ của các đối tác BTCV và kết nối hệ sinh thái BTCV với các loại tiền tệ FIAT.

- Qúy 1 năm 2021
  - Sản phẩm staking mới thông qua bên thứ 3
  - Sản phẩm giao dịch mới

- Qúy 2 năm 2021
  - Các cổng thanh toán mới
  - Tích hợp FIAT
- Qúy 3 năm 2021
  - Nền tảng phân tích dữ liệu (Big Data)
- Qúy 4 năm 2021
  - Sản phẩm liên quan tới wBTCV token
- 2022+
  - Các chức năng 3Keys mới
  - Sản phẩm dApps

Workstream số 5 – Hoạt động tiếp thị

Vào năm 2021, chúng tôi có kế hoạch khởi động chiến dịch nâng cao nhận thức và tương tác toàn cầu nhằm vào người dùng hiện tại và tương lai của BTCV cũng như toàn bộ cộng đồng tiền điện tử trên toàn thế giới. Chúng tôi sẽ tìm kiếm các mối quan hệ đối tác mới để tăng cường bảo mật của chuỗi khối BTCV cũng như cho phép BTCV đi trước nghiên cứu lượng tử.

- Qúy 1 năm 2021
  - Khởi chạy trang web mới
- Qúy 2 & Qúy 3 năm 2021
  - Chiến dịch tương tác và nâng cao nhận thức toàn cầu
- Qúy 4 năm 2021
  - Hợp tác an ninh chiến lược
- 2022+
  - Hợp tác khoa học chiến lược

Workstream số 6 – Những nâng cấp khác

Với một số nâng cấp bổ sung cho hệ sinh thái BTCV, chúng tôi muốn kết nối và tham gia với cộng đồng của mình và cung cấp các tùy chọn mới cho những người mới bắt đầu thông qua cơ chế airdrop mới sẽ ra mắt hoàn toàn vào đầu quý 2 năm 2021. Trọng tâm dài hạn của chúng tôi cũng sẽ xoay quanh điện toán lượng tử và tiềm năng của nó để ảnh hưởng đến tiền mã hóa của blockchain.

- Qúy 1 năm 2021
  - Phát triển & ra mắt cơ chế airdrop mới
  - Khóa ví Airdrops
- Qúy 2 năm 2021
  - Nền tảng / ứng dụng Airdrops
- Qúy 3 năm 2021
  - Nền tảng phân tích blockchain
- Qúy 4 năm 2021+
  - Nghiên cứu lượng tử
  - Chương trình tài trợ hợp tác khoa học

Máy tính lượng tử & DLT – Tầm nhìn của chúng tôi

Như nhiều nhà phát triển blockchain khác, chúng tôi thực sự quan tâm đến sự tiến bộ của công nghệ lượng tử. Các nhà nghiên cứu và nhà phát triển làm việc trên các công nghệ sổ cái phân tán (DLT) như blockchain phụ thuộc vào mật mã khóa công khai và các hàm băm, những thứ cần thiết cho tất cả các giải pháp blockchain.

Blockchain của Bitcoin Vault được bảo mật bằng các thuật toán mật mã mạnh mẽ như ECDSA và SHA-256, cũng được sử dụng trong Bitcoin cũng như nhiều loại tiền điện tử khác. Các thuật toán mã hóa hiện đang sử dụng đủ mạnh cho các phương pháp tính toán truyền thống.

Mối đe dọa máy tính lượng tử

Về lý thuyết, việc cải thiện sức mạnh tính toán theo cấp số nhân với công nghệ lượng tử có thể dẫn đến việc bẻ khóa khóa công khai để tính toán băm khóa riêng tư hoặc phá vỡ thuật toán SHA-256 để có được khối giá trị băm một lần được yêu cầu trên blockchain có thể xảy ra. Theo nhiều chuyên gia trong lĩnh vực này, chúng tôi vẫn đang nghiên cứu nhiều năm để phát triển máy tính lượng tử ổn định. Ngay cả khi đó, những máy tính đó sẽ cần được mã hóa thích hợp cho mục đích bẻ khóa các thuật toán mật mã nhất định.

Cơ hội máy tính lượng tử

Thay vì tập trung vào các mối đe dọa, chúng tôi muốn tập trung vào các cơ hội.

Một lần nữa, về lý thuyết, khi máy tính lượng tử có thể đạt đến độ ổn định đủ để thực hiện các phép tính đáng tin cậy, thì có thể sử dụng chúng để cải thiện các thuật toán mật mã. Đây là cơ hội mà chúng tôi nhìn thấy cho tương lai của blockchain.

Đối với ngày nay, chúng ta có thể xem xét các cách tiếp cận khác nhau để đạt được mục tiêu của một đồng tiền bằng chứng lượng tử, tức là:

- các hệ thống mật mã dựa trên mạng tinh thể,
- các hệ thống mật mã khóa công khai dựa trên đa biến,
- các hệ thống mật mã super-singular elliptic-curve isogenies,
- các hệ thống mật mã chữ ký số dựa trên băm
- các giải pháp kết hợp như những giải pháp được Google thử nghiệm (CECPQ1 và CECPQ2)
- và một số khách.

Để tìm ra giải pháp chống lượng tử phù hợp và chuẩn bị cho đồng BTCV cho kỷ nguyên hậu lượng tử, đội ngũ phát triển của chúng tôi cần nghiên cứu thêm về các kỹ thuật nén trên phím cần thiết và về việc sử dụng một số loại mã và kỹ thuật mã hóa nhất định.

Tuy nhiên, hiện nay, không có thuật toán blockchain hậu lượng tử nào cung cấp kích thước khóa nhỏ, kích thước chữ ký/băm ngắn, thực thi nhanh, độ phức tạp tính toán thấp và tiêu thụ năng lượng thấp, tất cả cùng một lúc. Những yếu tố này đặc biệt quan trọng đối với các thiết bị nhúng hạn chế tài nguyên như những thiết bị được sử dụng trong Internet of Things.

Trong vòng 3 đến 5 năm tới, các nhà phát triển BTCV của chúng tôi sẽ tập trung vào việc đạt được sự sẵn sàng hoạt động trong khả năng kháng lượng tử thông qua các mối quan hệ đối tác mới, đặc biệt là với các chuyên gia từ các doanh nghiệp, công ty khởi nghiệp và các trường đại học kỹ thuật khác nhau.

Người sáng lập Bitcoin Vault

Bitcoin Vault được thành lập bởi Eyal Avramovich, Giám đốc điều hành của Minebest, một trong những nhà điều hành hàng đầu thế giới về các cơ sở khai thác tiền điện tử ở Châu Á và Châu Âu.

Thêm thông tin về Minebest có thể được tìm thấy tại đây: https://minebest.com/

Thêm thông tin về đội ngũ đứng đằng sau Bitcoin Vault có thể được tìm thấy trên trang web chính thức: https://bitcoinvault.global/

Nguồn liên quan

Chúng tôi muốn ghi nhận công lao của những người tạo ra Bitcoin Royale cho ý tưởng khái niệm dẫn đến sự phát triển của Bitcoin Vault.

Sách trắng Bitcoin Royale: https://bitcoinroyale.org/bitcoinroyale.pdf

Nguồn BTCV:

Thông tin bổ sung về dự án có thể được tìm thấy::

https://bitcoinvault.global/
https://twitter.com/vaultbitcoin
https://medium.com/bitcoin-vault-btcv
https://t.me/Bitcoin_Vault
https://www.facebook.com/bitcoinvaultofficial
https://www.instagram.com/bitcoinvaultofficial
https://www.youtube.com/c/BitcoinVault

Tài liệu tham khảo:

1. Bitcoin Whitepaper, Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf
2. Bitcoin Royale: Peer-to-Peer No-Theft Electronic Gold, Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
3. Cryptocurrency Anti-Money Laundering and Crime Report, Spring 2020, https://ciphertrace.com/cryptocurrency-anti-money-laundering-and-crime-report-spring-2020/
4. The Chainalysis 2020 Crypto Crime Report, https://go.chainalysis.com/2020-Crypto-Crime-Report.html

5. Bitcoin, crypto-coins, and global anti-money laundering governance, Malcolm Campbell-Verduyn, https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance
6. Namecoin project, https://www.namecoin.org/
7. Bitcoin Wiki, Merged Mining Specifications, https://en.bitcoin.it/wiki/Merged_mining_specification
8. Adam Back, Hashcash – A Denial of Service Counter-Measure, http://www.hashcash.org/papers/hashcash.pdf
9. Phil Daian, Rafael Pass, Elaine Shi; Snow White: Robustly Reconfigurable Consensus and Applications, https://eprint.iacr.org/2016/919.pdf
10. Wrapped Tokens A multi-institutional framework for tokenizing any asset https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf
11. Smart Contract Extensibility with Wrapped Tokens https://yos.io/2019/07/13/smart-contract-extensibility-wrapped-tokens/#:~:text=Wrapped%20Tokens%20is%20a%20design,two%20versions%20at%20any%20time.
12. Aleksei Pupyshev, Ilya Sapranidi, Elshan Dzhafarov, Shamil Khalilov, Ilya Teterin, Graviton: interchain swaps and wrapped tokens liquidity incentivisation solution, https://arxiv.org/ftp/arxiv/papers/2009/2009.05540.pdf