



Viacoin Whitepaper

Đội phát triển Viacoin (Viacoin Dev Team)
Ngày 12 tháng 9 năm 2017

Lần cập nhật mới nhất vào ngày 17 tháng 3 năm 2018

Tóm tắt (Abstract)

Viacoin là 1 loại tiền mã hóa với nguồn mở được tạo ra vào năm 2014, bắt nguồn từ [bitcoin2008] giao thức của Bitcoin, nó hỗ trợ sự đồng thuận nhúng (embedded consensus) với một kịch bản lệnh được mở rộng 120 byte. Viacoin có tính năng (Scrypt Merged Mining) khai thác mỏ KẾT HỢP (cho phép người dùng khai thác nhiều loại tiền mã hóa cùng một lúc.), còn được gọi là khai thác bổ sung của bằng chứng của công việc viết tắt (AuxPoW - Auxiliary proof of work), Viacoin giao dịch nhanh hơn Bitcoin 25 lần. Việc khai thác số lượng phần thưởng Viacoin sẽ giảm đi một nửa diễn ra mỗi 6 tháng và có tổng cung 23.176.392.41459 Viacoin. Tỷ lệ lạm phát của Viacoin thấp do khai thác mỏ tối thiểu.

Khi phần thưởng khối lượng của Viacoin thấp, các thợ mỏ được khuyến khích đào Viacoin thông qua khai thác kết hợp (AuxPoW). Viacoin hiện đang được khai thác bởi một trong những bể khai thác mỏ lớn nhất (F2Pool) với hashrate rất cao. Các tính năng khác bao gồm một thuật toán điều chỉnh khó trong khai thác mỏ sẽ gửi các sai sót tới Gravity Well (Gravity Well là Một thuật toán điều chỉnh độ khó trong mining phổ biến là DarkGravity-Wave). Các phiên bản của Bit cho phép thay đổi Soft Fork 29 lần đồng thời được thực hiện tại một thời điểm, Segwit và Lightning Network

Lưu ý nhỏ: Các whitepaper, tài liệu, thiết kế đang trong quá trình nghiên cứu và phát triển có thể thay đổi theo giai đoạn.



Viacoin Whitepaper

1. Scrypt

Trong mật mã học, [scrypt] Scrypt là một hàm dẫn xuất (KDF - key derivation function) dựa trên mật khẩu được tạo ra bởi Colin Percival. Thuật toán được thiết kế đặc biệt để làm cho nó thật tốn kém khi bị thực hiện các cuộc tấn công phần cứng bất kỳ với quy mô lớn bằng cách đòi hỏi một dung lượng bộ nhớ thật lớn. Năm 2012, thuật toán được IETF (Internet Engineering Task Force - Lực lượng Chuyên trách về Kỹ thuật Liên mạng) xuất bản dưới dạng một bản thảo trên Internet nhằm trở thành một bản yêu cầu nhận xét (Request for Comments - RFC) của IETF cho thông tin, nhưng một phiên bản của Scrypt hiện được sử dụng như là một bản trình bày về chương trình bằng chứng công việc cho các loại tiền mã hóa như Viacoin.

Scrypt là một hàm dẫn xuất cho bộ nhớ chính, nó đòi hỏi một lượng lớn hợp lý của bộ nhớ ngẫu nhiên (RAM) để được đánh giá. Điều này làm cho việc thực hiện đặc biệt mục đích tùy chỉnh phần cứng (ASICs) đòi hỏi nhiều diện tích VLSI (Very-large-scale integration - tích hợp rất lớn) hơn, mà sẽ làm cho nó không có lợi cho việc xây dựng với mục đích khai thác Viacoin. Yêu cầu của Scrypt thuật toán là một mảng lớn của các bit giả ngẫu nhiên được tổ chức trong bộ nhớ và một chìa khóa đó là xuất phát từ điều này. Thuật toán dựa trên TMTO (Time-Memory Tradeoff). Lợi thế của ASIC (ASIC là mạch tích hợp dành riêng cho ứng dụng) trong Viacoin được giảm xuống 10op lần so với Bitcoin.

Scrypt sử dụng các tham số sau để tạo ra một khoá dẫn xuất:

- Cụm từ mật khẩu: Chuỗi ký tự để hàm băm
- Salt: Chuỗi ngẫu nhiên được cung cấp cho chức năng Scrypt
- N: Tham số chi phí bộ nhớ / CPU
- P: Thông số song song
- R: tham số khối
- dkLen: Chiều dài dự kiến khóa then chốt có nguồn gốc từ byte

kd = scrypt(P, S, N, P, R, dkLen)

Thông số Viacoin trong đó N = 1024, R = 1, P = 1 và S = ngẫu nhiên 80 byte tạo ra 256-bit output.



Viacoin Whitepaper

2. Khai thác mỏ kết hợp bổ sung bằng chứng công việc (Merged Mining AuxPoW)

Khai thác mỏ kết hợp của VIA nhằm tái sử dụng sức mạnh khai thác của bất kỳ hàm dẫn xuất Scrypt để tăng cường khả năng bảo mật cho Blockchain của Viacoin, điều này cho phép người thợ mỏ khai thác được nhiều hơn một blockchain cùng một lúc. Ví dụ, một thợ mỏ có thể khai thác Viacoin và Litecoin hoặc bất kỳ coin nào khác cùng với Viacoin với ít hoặc không có tác động nào lên hashrate của một trong hai.

Mỗi hash khai thác mỏ đóng góp cho tổng số hashrate của cryptocurrencies và kết quả là một blockchain an toàn hơn. Khối AuxPoW là một loại khối tương tự như khối Bitcoin chuẩn với hai sự khác nhau. Các băm tiêu đề khối không đáp ứng được mức độ khó khăn của blockchain. Thứ hai, nó có thêm các yếu tố dữ liệu chỉ ra rằng các thợ mỏ đã tạo ra một khối và đã khai thác mỏ trên blockchain gốc và làm việc đáp ứng mức độ khó của các blockchain aux.

Người thợ mỏ được khuyến khích để đào Viacoin ngay cả khi phần thưởng thấp vì họ có thể đào bất kỳ đồng coin nào đồng thời cùng với việc đào Viacoin một cách miễn phí. Do việc khai thác Viacoin không phải là phần thưởng lớn, điều này cho phép Viacoin có tỷ lệ lạm phát thấp hơn so với các loại tiền mặt mã khác không hỗ trợ khai thác Kết hợp.

3. Thuật toán điều chỉnh độ khó (Dark Gravity Wave)

Dark Gravity Wave (DGW) là một thuật toán điều chỉnh độ khó với mã nguồn mở. Evan Duffield là tác giả của DGW, nhà phát triển và người sáng tạo ra X11 / Darkcoin / Dash. Thuật toán được thiết kế để giải quyết các sai sót như cuộc tấn công Time Warp trong thuật toán Kimoto Gravity Wave.

Dark Gravity Wave được giới thiệu lần đầu tiên trong Dash (Darkcoin). DGW sử dụng cho nhiều đường trung bình di chuyển theo lũy thừa và đường trung bình di chuyển đơn giản để làm phẳng cơ chế điều chỉnh.

Công thức:

$$2222222 / (((\text{Difficulty} + 2600) / 9)^2)$$

Dark Gravity Wave phiên bản 3 là phiên bản mới nhất và cho phép cải thiện độ khó khi so sánh với thuật toán Kimo Gravity Well nổi tiếng.



Viacoin Whitepaper

4. Segwit

Viacoin đã kích hoạt [Segwit] Segwit (BIP 141). Segregated Witness giúp thu nhỏ kích cỡ của một giao dịch và đối phó với sự tăng trưởng của UTXO (UTXO là một đầu ra giao dịch không chủ ý). Segregated Witness là một định dạng giao dịch mà dữ liệu của nhân chứng (ở đây là chữ ký số) được tách biệt khỏi giao dịch. Nó cũng nhằm mục đích tăng khối lượng giao dịch mỗi block bằng 2 hoặc 3 lần, trong khi đó đồng thời làm cho khối đồng bộ hóa nhanh hơn cho các nút mới.

Mục đích chính của việc thực hiện Segwit trong Viacoin không phải là để nâng cao năng lực, tuy nhiên nó dùng để sửa chữa tính dẻo dai và làm cho kịch bản nâng cấp dễ dàng hơn.

Việc nâng cấp tính dẻo dai cho phép bổ sung các tính năng trong Viacoin như hoán đổi nguyên tử (Atomic swaps), sử dụng kênh thanh toán hai chiều và Lightning Network điều đó giúp tăng khả năng tương thích của Viacoin với Bitcoin.

Segwit bao gồm phiên bản cho các tập lệnh mà nó có thể sử dụng các mã thuật toán (opcode) bổ sung (thường đòi hỏi phải có hard fork trong các giao dịch không phải là segwit). Các thay đổi đối với các mã lệnh thuật toán sẽ làm cho Viacoin tiến triển tốt hơn. Điều này làm cho sự bổ sung của các tính năng khác như chữ ký Schnorr, sidechains, MAST được diễn ra hiệu quả và dễ dàng hơn.

5. The Lightning Network

Lightning Network là một mạng lưới truyền tải giao dịch ở một nhánh khác của blockchain Viacoin, nó sử dụng chức năng hợp đồng thông minh trong blockchain để cho phép thanh toán tức thời thông qua mạng lưới người tham gia. Điều này cho phép cải tiến số lượng lớn đơn đặt giao dịch cần xác nhận bằng cách di chuyển phần lớn các giao dịch ra bên ngoài các sổ cái đồng thuận bằng các kênh Thanh toán off-chain. Điều này cho phép thực hiện hàng triệu tỷ giao dịch mỗi giây qua mạng. Điều này có thể được thực hiện bằng cách hỗ trợ các kịch bản chuỗi trên mạng lưới on-chain, trong đó các bên tham gia vào các hợp đồng song phương, trong đó giao dịch có thể được cập nhật bằng cách chia sẻ thông tin chữ ký số và có thể đóng kenh giao dịch đưa bằng chứng giao dịch lên blockchain.



Viacoin Whitepaper

Lightning Network cho phép giao dịch với mức phí siêu thấp, và đối với cả một giao dịch có giá trị thấp, Lightning Network sẽ là viên đạn bạc. Nó cho phép các loại hình thương mại mới xuất hiện. Bằng cách mở một kênh thanh toán với nhiều bên, những người tham gia LN có thể trở thành đầu mối để định tuyến thanh toán của những người khác dẫn đến kênh thanh toán được kết nối hoàn toàn. Các khoản thanh toán được thực thi bằng cách sử dụng một tập lệnh thực hiện nguyên tử thông qua việc khóa thời gian time-locks.

Lợi ích khác là khả năng giao dịch hoán đổi chuỗi chéo nguyên tử, cho phép người sử dụng mua bán Viacoin, Bitcoin, Litecoin và các loại tiền Segwit khác ngay lập tức, và nó cho phép trao đổi phi tập trung rất hiệu quả, hoặc một hình thức phân cấp của 'Shape-shift.io'

6. Chữ Ký Schnorr

Chữ ký Schnorr cũng là một phần của sự phát triển sắp tới. Chức năng này cũng đã được đề xuất trong Bitcoin như là sự kế thừa của ECDSA vì nó là một thuật toán hiệu quả hơn. Trước đó, ở Viacoin và trong nhiều loại coin khác việc thực hiện chữ ký Schnorr là không thể khi không thực hiện hardfork. Nay với tính dẻo dai của Segwit, Chữ ký Schnorr đã có thể thực hiện. Tất cả dữ liệu chữ ký được chuyển đến người làm chứng. Viacoin hiện đang sử dụng chữ ký số (ECDSA) như một bằng chứng zk về quyền sở hữu để cho phép chuyển thông tin chữ ký từ một đầu ra sang kênh khác. Vào năm 2015, Daniel J. Bernstein đề xuất sử dụng một chữ ký giống như Schnorr trên một đường cong Elliptic.

Một số ưu điểm:

- Có thể đảm bảo an toàn theo các giả định chuẩn
- Miễn dịch đối với tính dẻo dai
- Chống va chạm hàm băm
- Xác nhận tính hợp lệ cho tăng tốc 2-3x
- Bản tự chữ hoa k-of-k...

Chữ ký Schnorr hỗ trợ xác nhận theo nhóm, có nghĩa là nếu bạn có một nhóm các cặp chữ ký công khai thay vì chỉ một chữ ký, bạn có thể xác minh tính xác thực của cả nhóm chữ ký đó như xác thực một chữ ký nhưng với tốc độ cao hơn từng chữ ký riêng lẻ. Phương pháp này là lý tưởng vì các khối là nhóm lớn của chữ ký để xác nhận.



Viacoin Whitepaper

Kiểu chữ k-of-k thuần, ý tưởng của Schnorr là bạn có thể mua nhiều phím với nhau và có một chữ ký chứng minh rằng tất cả chúng đều được ký. Một nhóm có thể tạo một chữ ký hợp lệ cho tổng của các phím. U₁, U₂ và U₃ là những người sử dụng. Có một lược đồ tương tác 2 vòng, trong đó tất cả chúng xuất hiện với n-một lần k₁, k₂, k₃ và tất cả đều tính một điểm công cộng tương ứng R₁, R₂, R₃. Họ giao tiếp với nhau và thêm chúng với giá trị R tổng thể. Giá trị R tổng thể này ký hiệu nonce với chìa khóa của chính nó dẫn đến S₁, S₂, S₃ và sau đó bạn kết hợp tất cả các giá trị S vào một S. cuối cùng Một chữ ký sẽ hợp lệ cho tổng của các phím của chúng.

Điều này có lợi thế của multisig k-of-k.

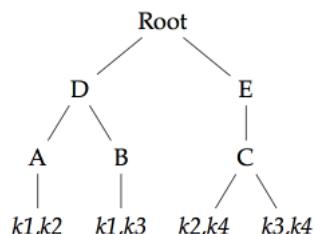
$$\begin{array}{c|c} U_1 \rightarrow k_1, R_1 & U_1 \rightarrow (R, s_1) \\ U_2 \rightarrow k_2, R_2 & U_2 \rightarrow (R, s_2) \\ U_3 \rightarrow k_3, R_3 & U_3 \rightarrow (R, s_3) \end{array} \longrightarrow R \longrightarrow \begin{array}{c} (R, s) \end{array} \quad (1)$$

Ngay cả khi không có tình huống k-of-k, bất kỳ chính sách nào khác của sự kết hợp của các phím có thể được ký kết. Tất cả các nhu cầu là một cây merkle cộng với khả năng cho Schnorr để thêm và xây dựng một cây nơi mà mỗi nút lá của cây là một sự kết hợp của các phím có thể được ký kết.

Sau đó chúng cần được băm cùng nhau và gốc là địa chỉ. OP_CHECKSIG & OP_CHECKMULTISIG sẽ được sửa đổi để chúng có thể xếp chồng các pubkeys, delin-earize và liên kết đầu vào đã được kiểm chứng và tạo ra một chữ ký kết hợp cho giao dịch dẫn đến giảm 20% kích thước khối.

2 trong 4 (k₁ ... k₄)
O (1) thời gian xác minh
Kích thước chữ O ($\log n$)
Thời gian ký hiệu O (n)

Có thể tổng hợp tất cả các chữ ký trong một giao dịch.
Ý tưởng phía sau nó là cho phép các trình xác nhận hệ thống như các nút Viacoin tính một phím đơn cho mọi đầu vào của tất cả các giao dịch.





Viacoin Whitepaper

7. Xử lý Non-atomic

Để làm cho hệ thống trở nên mạnh mẽ, trạng thái trên Disk phải liên tục với khối. Với việc tắt máy bất ngờ của ví, chúng tôi có thể khởi động và rollback hoặc roll phía trước của nó và có thể có được một tip thích hợp trên Disk. Thông thường bất cứ khi nào bộ nhớ cache sẽ đầy, việc xử lý sẽ là bắt buộc. Nếu nó xảy ra khi khởi động nó có nghĩa là chúng tôi đã Crash trong quá trình xử lý, và chúng tôi rollback / roll phía trước các khối bên trong của nó để có được một tip thích hợp trên Disk trước khi tiếp tục.

8. Colored coins

Ngôn ngữ bản thảo của Viacoin cho phép lưu trữ một lượng nhỏ siêu dữ liệu trên block-chain và có thể đại diện cho hướng dẫn thao tác tài sản. Một giao dịch Viacoin có thể được mã hóa rằng x đơn vị của một tài sản mới đã được phát hành và được ghi có vào một địa chỉ Viacoin. Thuật ngữ này bắt nguồn từ ý tưởng "tô màu" một lượng tiền xu danh nghĩa. Bằng cách tô màu một Viacoin, nó biến thành một mã thông báo có thể đại diện cho bất cứ điều gì người dùng muốn mua bán như cổ phần công ty hoặc hàng hoá vật chất.

Điều này có vẻ rất giống với tính năng của đồng (XCP) 'Counterparty' nhưng có một số điểm khác biệt chính. Nó sử dụng Blockchain Viacoin (ví dụ: NXT).

Nó không phát hành một loại tiền phụ (ví dụ: Counterparty và Mastercoin). Medata mang ý nghĩa cho một giao dịch tiền xu màu có màu [colorCoins], thường được lưu trữ trong một trong các mã OP_RETURN. Đầu ra chứa OP_RETURN được gọi là đầu ra marker. Marketcut này có thể có giá trị bằng không hoặc không bằng không. Các đầu ra đánh dấu bắt đầu bằng OP_RETURN opcode và có thể được theo sau bởi bất kỳ chuỗi mã opcodes nào phải chứa một opcode PUSHDATA có chứa một phân tích cú pháp Mở tài sản Payload. Trường danh sách số lượng tài sản được sử dụng để xác định số lượng của mỗi đầu ra của nội dung và mỗi số nguyên đang sử dụng mã hoá LEB128. Nếu vượt quá 9 byte, đầu ra của thị trường sẽ bị coi là không hợp lệ. Số lượng tài sản tối đa cho sản lượng là 263 - 1. Các đồng tiền màu [openAsset] Open Asset Protocol nằm trên giao thức Viacoin. Nó không yêu cầu bất kỳ thay đổi nào đối với giao thức Viacoin.



Viacoin Whitepaper

9.MAST – màng chắn [Tóm tắt nhánh hàm dẫn xuất khóa trong bộ nhớ cứng Syntax Merkleized tree]

[MAST] Màng chắn cho phép các tập lệnh xác thực giao dịch Viacoin được lưu trữ dưới dạng phân chia một phần và cho phép các nút tương tác với Merkle Trees. "Khi chi tiêu, người dùng chỉ có thể cung cấp các chi nhánh mà họ đang thực hiện, và các bảng kết nối các chi nhánh với gốc Merkle có kích thước cố định. Điều này làm giảm kích thước của khối mua lại từ $O(n)$ thành $O(\log n)$ (n là số nhánh). Điều này cho phép điều kiện mua lại phức tạp mà hiện tại không thể thực hiện được vì kích thước tập lệnh và giới hạn về mã thuật toán, để cải thiện sự riêng tư bằng cách che giấu các nhánh không được thực hiện và cho phép đưa dữ liệu không có sự đồng thuận xuống với chi phí rất thấp hoặc không phát sinh thêm chi phí nào".

Điều quan trọng là vì MAST cho phép hợp đồng thông minh được tạo ra mà không làm tắc nghẽn blockchain. Thông thường tất cả các hợp đồng thông minh sẽ được hiển thị trên blockchain và chiếm không gian. Với MAST, chỉ có thể tiết lộ các hợp đồng thông minh đã được hoàn thành, tiết kiệm không gian khi các nút chỉ cần đọc lớp trên cùng của Merkle Tree là được. Điều này có vẻ quen thuộc với hệ thống hợp đồng thông minh của Ethereum nhưng có một sự khác biệt. Ethereum truy cập vào máy ảo trực tiếp nơi mà VIA sẽ truy cập vào máy ảo mặc dù RootStock (RSK). RSK hướng tới mục tiêu của Ethereum: một nền tảng hợp đồng thông minh được phân cấp, Turing hoàn chỉnh.

10. Viacoin - hợp đồng thông minh RSK

Rootstock là một nền tảng hợp đồng thông minh có một khóa hai chiều. Ý tưởng là để cho phép nó làm việc với các hợp đồng thông minh. Rootstock chạy một máy ảo hoàn chỉnh được gọi là máy ảo gốc (Rootstock Virtual Machine) (cũng tương thích với máy ảo Ethereum) và cho phép kết hợp các hợp đồng thông minh vững chắc để hoạt động. Nó có thể hoạt động bằng cách kết hợp khai thác với Viacoin, cho phép blockchain RSK có mức bảo mật giống như Viacoin. Nó cho phép khoảng 2000 giao dịch mỗi giây theo phương thức trực tiếp (on chain) và 20000 giao dịch mỗi giây theo phương thức không trực tiếp.



Viacoin Whitepaper

11. Giao dịch ẩn danh

[styx] Giao dịch thanh toán nguyên tử ẩn danh đối với Viacoin dựa trên nền tảng giao dịch ẩn danh của Bitcoin (Tumblebit).

<https://github.com/viacoin/documents/blob/master/whitepapers/styx/Viacoin-Styx-Whitepaper.pdf>