Technical White Paper

(Một số chi tiết có thể được thêm vào)

Hệ thống tài chính phi chính phủ

CREDITS

Version 1.5/12.09.2017

Mục Lục

Tóm Tắt 3

Lời Nói Đầu 3

1. Hồ Sơ Network 4

Định nghĩa 4

Network Nodes 4

Block cuối cùng

Đồng bộ hóa nodes

2. Đồng Bộ Network 5

So Sánh Đồng Bộ 5

Khái Niệm Chính Của Network Node 6

Thiết Bị Của Network Nodes 7

Đồng Bộ Xây Dựng 7

Xây Dựng và Bắt Đầu Hồ Sơ 7

Những Giao Dịch Không Có Trong Đăng Ký 8

3. Xử Lý Giao Dịch 8

Giao Dịch 8

Đồng Bộ Xây Dựng 8

Xử Lý Giao Dịch 8

Cấu Trúc Phần Đầu Hồ Sơ 8

Cấu Trúc Hồ Sơ của CREDITS 9

Khối Lượng Block 9

Tìm kiếm Người tham gia Giao dịch 9

Kênh truyền dữ liệu 9

Hành động trong Hệ thống 10

Thêm giao dịch để xác nhận 11

Chi phí giao dịch 11

4. Hợp đồng thông minh 11

Lời Nói Đầu 11

Các đơn vị 11

Phương thức hợp đồng thông minh 12

Máy ảo thực thi 12

Giới Hạn Giá Trị 12

Thực hiện các Điều khoản Hợp đồng Thông minh 13

Data Sources 13

5. Kế hoạch thực hiện 13

Kế hoạch kỹ thuật thực hiện dự án 13

CREDITS cryptocurrency 14

Tóm Tắt

Nền tảng CREDITS là một hệ thống tài chính phân cấp cho sự tương tác trực tiếp giữa những người tham gia về nguyên tắc peer-to-peer (P2P). Nền tảng này mở rộng tiềm năng sử dụng các dịch vụ tài chính trên cơ sở một sổ cái phân phối, hợp đồng thông minh tự thực hiện, và cryptocurrency của CREDITS. Hệ thống này kết hợp tất cả người tham gia vào một trang web, cung cấp cho họ một nền tảng để tạo và sử dụng các dịch vụ tài chính, nơi mọi người đều có thể cung cấp dịch vụ và sử dụng nó. Nhờ vào hệ thống công nghệ cân bằng và cân bằng, nền tảng CREDITS đưa ra một giải pháp kỹ thuật mới và một mô hình khái niệm mới cho sự tương tác của các bên tham gia mạng lưới để phát triển các dịch vụ tài chính hiện đại.

Lời Nói Đầu

Một thỏa thuận đầy đủ cho các hệ thống phân phối dịch vụ cho phép hình thành các dịch vụ tài chính: chuyển tiền, trao đổi tiền tệ và giá trị, tín dụng, tài trợ và các dịch vụ khác trực tiếp giữa các bên tham gia. Tất cả mọi thứ được cung cấp mà không có các trung gian bổ sung, theo một nguyên tắc - một trong những người tham gia bình đẳng - cho những người tham gia hệ thống khác. Kết quả là, mọi người đều nhận được dịch vụ rẻ hơn, nhanh hơn và tốt hơn.

Thế giới đang hướng tới sự tương tác trực tiếp giữa những người theo nguyên tắc ngang hàng - bằng nhau. Một cuộc cách mạng đã xảy ra! Điều này được thể hiện rõ qua sự đảo lộn trên các phương tiện thông tin đại chúng: cho đến những năm 1990, báo, tạp chí và truyền hình là những nhà cung cấp thông tin chính. Ngày nay, các nhà lãnh đạo ý kiến là các blogger, tìm kiếm trên các kênh Youtube và các mạng xã hội, tiền được đầu tư vào crowdfunding và ICO, và thông tin được lưu trữ trong các hệ thống điện toán phân quyền.

Ngành công nghiệp tài chính, có lẽ, là một trong số ít ngành công nghiệp tụt lại phía sau, chống lại việc đưa ra sự phân quyền và sự tương tác trực tiếp giữa các bên tham gia. Mặc dù về mặt kỹ thuật, việc tạo ra các dịch vụ tài chính phi tập trung dễ hơn là tạo ra các phương tiện không người lái.

Một môi trường công nghệ tương ứng được yêu cầu để tạo ra một hệ thống các sản phẩm và dịch vụ tài chính phân tán dựa trên phân loại phân phối:

1. Tốc độ thực hiện cao (tính bằng giây), cùng với khả năng xử lý một số lượng lớn các giao dịch cùng một lúc (hàng trăm nghìn mỗi giây) với chi phí thấp cho mỗi giao dịch (đối với thanh toán nhỏ và các giao dịch noncash).
2. Phát triển một hệ thống mà tất cả người tham gia và các mặt hàng cần thiết cho các dịch vụ phân cấp tài chính có chất lượng được kết hợp: cá nhân hóa người sử dụng, KYC, văn phòng lịch sử tín dụng, trung tâm thanh toán tiền fiat, thu hồi và tiền mặt của cryptokurrencies vv

Đây là hai nhiệm vụ lớn và cơ bản đang cản trở sự phát triển của sản phẩm tài chính.

Chúng tôi trình bày cho bạn một giải pháp cho những nhiệm vụ này, chúng tôi thực hiện với sự trợ giúp của hệ thống tài chính tín dụng.

CREDITS nền tảng phân cấp công nghệ đơn có thể kết hợp tất cả những người tham gia dịch vụ tài chính, thực hiện tất cả các giao dịch một cách an toàn và nhanh chóng bằng cách sử dụng các nguyên tắc của một sổ cái phân phối. Tự thực hiện hợp đồng thông minh và các nguyên tắc của một hệ thống bầu cử liên bang cung cấp cơ hội không giới hạn cho tất cả người tham gia để tạo ra sự tương tác độc đáo của các sản phẩm tài chính khác nhau. Nền tảng này mở ra một thị trường khổng lồ mới và tiềm năng mới cho việc sử dụng các dự án và dịch vụ blockchain trong các lĩnh vực tài chính và các ngành khác mà trước đây không thể sử dụng do tốc độ và chi phí giao dịch hạn chế.

1. Hồ Sơ Network

Định nghĩa

1. Một hệ thống là một tập hợp các nút mạng phân tán đang thực hiện chế biến, lưu các giao dịch, thực hiện và xác nhận các điều khoản hợp đồng thông minh, xử lý các yêu cầu từ các hệ thống của bên thứ ba, cung cấp dữ liệu thông tin khi có yêu cầu.
2. Một nút mạng là một máy tính cài đặt một máy khách hoàn chỉnh, kết nối với một hệ thống chung, kiểm tra giao dịch và ghi chúng vào hồ sơ.
3. Sổ cái là danh sách các giao dịch được xác nhận bởi hệ thống và được lưu trữ trên tất cả các nút mạng.
4. Một giao dịch là mục hệ thống, biểu thị yêu cầu thực hiện một phương thức hợp đồng thông minh hoặc bất kỳ hành động nào trên mạng và ghi lại các kết quả trong một hệ thống blockchain.
5. Hợp đồng thông minh là mục hệ thống, các giao thức máy tính tạo thuận lợi, xác minh hoặc đảm bảo tuân thủ các điều khoản tương tác. Họ thường có một giao diện người dùng và thường mô phỏng logic của các mối quan hệ hợp đồng. Tài sản chính của một hợp đồng thông minh là sự phân quyền và sự độc lập của nó từ một nguồn trung tâm.
6. Phương thức hợp đồng thông minh là mã chương trình chịu trách nhiệm tính toán kết quả công việc của các điều khoản hợp đồng thông minh và ghi nó vào hồ sơ
7. Một bên ký kết là người tham gia mạng cuối cùng và người sử dụng hệ thống.

Network Nodes

Chúng tôi sử dụng một số loại nút, tùy thuộc vào mục đích của họ để xây dựng một mạng lưới phân cấp dựa trên truy cập miễn phí và kết nối nút:

1. Nodes phổ biến (ОУ) là nút tham gia xác minh giao dịch tính hợp lệ nhưng có một yếu tố tin cậy tối thiểu. Nó cũng là một ứng cử viên cho vai trò của một nút đáng tin cậy và nút của quá trình xử lý hiện tại trong chu kỳ tiếp theo của việc lựa chọn vai trò nút trong mạng.
2. Nodes đáng tin cậy (ДУ) là nút tham gia xác minh giao dịch và có hệ số tin cậy tối đa (1), là một ứng cử viên cho vai trò của nút của nút xử lý hiện tại và nút thông thường. Nút này không thể trở nên đáng tin cậy trong một số phép tính toán và vòng bỏ phiếu giữa các nút. Việc tính toán toán học phụ thuộc vào số nút và độ phức tạp của mạng.
3. Nodes chính (ГУ) của mạng là nút tham gia vào quá trình xác minh và chịu trách nhiệm cho việc thêm các giao dịch vào khối ngăn sổ giao dịch. Nút này không thể trở nên đáng tin cậy hoặc là nút của quá trình xử lý hiện tại trong một số các chu kỳ bỏ phiếu được tính toán về mặt toán học, tính toán đó phụ thuộc vào số nút và độ phức tạp của mạng.

Hệ thống sử dụng một yếu tố tin cậy - một giá trị số 0 tuyệt đối bằng 0, được biểu diễn dưới dạng số học của số nút đáng tin cậy +1 cho tổng số nút trong mạng. Số lượng nút đáng tin cậy tối đa không được vượt quá 50% nút mạng.

Block Cuối Cùng

Hồ Sơ Chung của Các Block (CRB) là trạng thái đồng bộ của toàn bộ sổ cái chung của các khối trong tất cả các nút hệ thống.

Theo nội dung khối sổ kế toán, chúng tôi muốn nói đến một đơn vị thông tin được lưu giữ có chứa mã băm của khối trước đó và một danh sách các dữ liệu liên quan đến sổ cái này với số liên kết của khối trước đó. Khi nhận được khối từ nút khác, nó mất vị trí của nó trong sổ cái chung của các khối theo số. Điều này giúp tiết kiệm băng thông mạng

Trong quá trình đồng bộ hóa, chỉ số khối mới được kiểm tra. Nếu khối này bị thiếu ở nút này, nó sẽ được tải xuống và lưu lại.

Do đó, hệ thống bất kỳ lúc nào cũng có bản sao bản sao lưu gần đây nhất của sổ cái. Chúng tôi đặt tên nó là hồ sơ cuối cùng (LR). Nó được tự động tạo ra bởi nodes chịu trách nhiệm cho sự hình thành hồ sơ khi đạt được sự đồng thuận. Block này được gửi đến tất cả các nodes hệ thống để duy trì độ đồng dạng cập nhật của trạng thái sổ cái trong tất cả các nodes hệ thống.

Mỗi node được kết hợp với tất cả các node khác trong mạng và liên tục trao đổi các block mới với những lệnh giao dịch với chúng, để luôn duy trì các thông tin có liên quan. Tất cả các block tạo thành một tập hợp các transactioncandidates đang chờ để được thêm vào hồ sơ. Đồng thời, mỗi máy chủ tạo ra các tập hợp giả định của các ứng cử viên cho các máy chủ khác và các bộ đề xuất của các giao dịch. Một quyết định được thực hiện khi kiểm tra, có nên thêm chúng vào hồ sơ.

Kết quả là, có thể lưu trữ dữ liệu hồ sơ nhiều lần trên nhiều máy chủ - các nodes hệ thống, và tất cả các thông tin đều được bảo vệ. Các nodes nhiều hơn trong hệ thống, nó đáng tin cậy và độc lập hơn.

Đồng bộ hóa nodes

Mỗi node mới được khởi chạy và đồng bộ hóa sau khi định nghĩa xác định và xác minh tin tưởng toàn diện. Để cải thiện tốc độ xử lý thông tin, tất cả các quy trình được xử lý đồng thời, độc lập với nhau. Nếu không có các biến đến, thì một cửa hàng bán hàng rỗng được tạo ra - một không gian được dành riêng trong RAM để tiếp tục đơn giản hóa truy cập. Trong trường hợp của hồ sơ yêu cầu không có sẵn, một yêu cầu được gửi đến các nodes đáng tin cậy để nhận tất cả các giao dịch được thực hiện cho tài khoản đồng bộ.

Nếu tham số đầu vào là một đối tượng mô tả giao dịch, thì tìm kiếm trong tất cả các luồng đồng bộ đang chạy đang bắt đầu. Kết quả hoạt động trong một mã số - số vị trí trong sổ lưu trữ điểm tin cậy cho luồng hiện tại hoặc số lỗi nếu giá trị nhỏ hơn không. Nếu phương pháp sợi kết thúc với một lỗi kết nối, sau đó sợi kết thúc hoàn toàn.

2. Đồng Bộ Network

Sự đồng thuận trong CREDITS là một phương pháp ra quyết định nhóm. Với mục đích phát triển các giải pháp cuối cùng có thể chấp nhận được cho tất cả các nodes network.

So Sánh Đồng Bộ

Định nghĩa các nguyên tắc của hồ sơ CREDITS phân quyền để so sánh các loại đồng thuận khác nhau:

- Sự sẵn có của sổ cái (các nút có thể ghi dữ liệu vào sổ cái và đọc chúng từ nó vào bất kỳ lúc nào);
- Khả năng điều chỉnh của tất cả các node network tham gia;
- Tính nhất quán của tất cả các nút hệ thống (tất cả các nút hiển thị một phiên bản hoàn toàn giống nhau của sổ cái, được cập nhật sau khi thay đổi);
- Khả năng chống phân tách (nếu một nút không hoạt động, điều này sẽ không ảnh hưởng đến hoạt động của toàn bộ sổ cái).

Tham số được so sánh	Credits cụ thể PoW và PoC	PoW	PoS
Nguyên tắc xác định node tạo ra block.	Tính toán các chức năng toán học. Xác nhận lưu trữ bản sao của hồ sơ cuối cùng.	Thực hiện tính lặp đi lặp lại của hàm toán học, với sự phức tạp khác nhau.	Tìm kiếm chồng tối đa giữa những người tham gia (các node cạnh tranh).

Attack 51%.	Không chắc bởi vì cần phải có hồ sơ đầy đủ trong tài nguyên và tính toán tính toán, và các node đáng tin cậy được chọn một cách năng động.	Có thể, nhưng sẽ rất tốn kém về việc sử dụng các nguồn lực.	Có thể, nhưng tốn kém, vì sự cần thiết phải tăng stack của riêng mình.
Bồi thường cho công việc được thực hiện tại địa điểm để thêm vào sổ cái / blockchain.	Tính toán tự động, phụ thuộc vào hoa hồng trên mỗi hoạt động.	Cung cấp sửa chữa cho việc mining block	Cung cấp sửa chữa cho việc mining block

Khái Niệm Chính Của Network Node

Tất cả các node network được phân cấp và không ai trong số chúng được ưu tiên. Nó được yêu cầu để xác định một node network sẽ xử lý hàng đợi của các giao dịch được lưu trữ tại các node network khác nhau. Sau đó, nó phải nhập một khối giao dịch mới được tạo ra vào hồ sơ.

Nền tảng CREDITS sử dụng giao thức kết hợp của riêng mình để tăng tốc độ xử lý giao dịch, cung cấp bảo mật hoàn chỉnh cho việc lưu trữ, xử lý và chuyển giao dữ liệu. Giao thức dựa trên việc tính toán các chức năng toán học của tất cả các giao dịch sổ cái, áp dụng nguyên tắc Proof của Thế Giới. Nó xác định một cách chính xác việc lưu trữ bản sao bản cập nhật mới nhất của sổ cái và phần mềm tại node này (Chứng minh năng lực), bằng cách tính checksum của các giá trị của toàn bộ nội dung - mã băm. Kích thước của tệp tin cũng được xác định, vì đây là bản sao bản mới nhất, bản sao lưu và mã băm của giao dịch mới nhất được ghi lại trong hệ thống.

Để trở thành node network chính, node tìm kiếm giá trị của hàm băm mà nó tính toán dựa trên hồ sơ được lưu trữ cuối cùng. Chúng tôi tổ chức một môi trường cạnh tranh lành mạnh giữa các node network để có cơ hội trở thành node chính, tạo ra và lưu trữ hồ sơ mới.

Sau khi tính hàm và nhận kết quả, nó sẽ được gửi đến tất cả các node network để xác minh. Kết quả chứa một dấu thời gian tính toán và một giá trị dựa trên việc tính toán các chức năng của các tập tin và phần mềm hồ sơ. Tất cả các node nhận được giá trị tính toán, so sánh thời gian tính toán được phân bổ cho việc tìm kiếm máy chủ mạng chính, xác minh nó và xác nhận yếu tố tin cậy của node, đồng thời xác nhận cơ hội tham gia vào cuộc thi - để trở thành node network chính.

Sau khi nhận được chấp thuận từ tất cả các node network, một danh sách được hình thành từ các nút chính xác tính giá trị của hàm và chứa một dấu thời gian. Node nhận được kết quả đúng và sẽ được phê duyệt trong thời gian nhanh nhất, trở thành node network chính của thời điểm này.

Thuật toán SHA2 được sử dụng để tính toán tổng băm của tệp tin.

Hash chức năng của gia đình SHA2 được xây dựng trên cơ sở cấu trúc MerkleDamgard.

Thông báo ban đầu sau khi bổ sung được chia thành các block, mỗi block được chia thành 16 từ. Thuật toán truyền từng block thông qua một chu kỳ với 64 hoặc 80 lần lặp (vòng). Tại mỗi lần lặp, 2 từ được chuyển đổi, và phần còn lại của các từ xác định chức năng chuyển đổi. Các kết quả của mỗi quá trình block được tóm tắt. Tổng là giá trị hàm băm. Tuy nhiên, trạng thái nội bộ được khởi tạo dựa trên kết quả của việc xử lý block trước đó. Vì vậy, không thể xử lý độc lập block và tổng kết các kết quả.

Thiết Bị của Network Nodes

Chúng tôi đang nỗ lực để xây dựng một nền tảng với các đặc điểm xử lý giao dịch nhanh nhất có thể, vì vậy chúng tôi đề xuất sử dụng ưu đãi vật chất để duy trì các node network trong điều kiện tốt nhất: thiết bị máy chủ hiệu suất cao và băng thông Internet cao.

Là một bồi thường vật chất, chủ sở hữu của node network chính sẽ nhận khoản tiền thù lao trong tiền tệ CREDITS từ một số tiền hoa hồng cho mỗi giao dịch của sổ cái được xử lý này. Phần còn lại (½) dành cho ngân sách phát triển dự án tổng thể để hỗ trợ người dùng, các tính năng hiện tại và phát triển sản phẩm mới. Tỷ lệ phần trăm có thể được thay đổi, cũng như được tách ra với hệ thống hình thành tỷ lệ thông qua các cuộc bầu cử liên bang bởi các node network, sau khi chào hàng coin offering ít nhất ba năm.

Do đó, chúng tôi khuyến khích chủ sở hữu máy chủ lưu giữ máy chủ này trên phần cứng có hiệu suất cao nhất và để duy trì một kênh truyền thông cao cấp.

Đồng Bộ Xây Dựng

Kết quả là, chúng ta có node network chính được chọn bởi tất cả các node. Các nhiệm vụ chính của node chính là: thu thập các giao dịch trong trạng thái ứng cử viên để thêm vào hồ sơ từ tất cả các node, xử lý chúng, xây dựng hồ sơ cuối cùng có liên quan và gửi hồ sơ mới được xây dựng cho tất cả các node network khác. Quá trình xử lý giao dịch và xây dựng hồ sơ có liên quan gần nhất chính là việc tìm kiếm giải pháp đồng thuận. Kết quả của việc xây dựng hồ sơ cuối cùng có liên quan là giải pháp đồng thuận.

Toàn bộ quá trình có thể được chia thành các giai đoạn sau:

1. Tìm kiếm network node chính;
2. Xây dựng node đáng tin cậy ;
3. Nhận danh sách các giao dịch và xây dựng một danh sách các ứng cử viên để bổ sung hồ sơ ;
4. Xử lý danh sách ứng cử viên, bỏ phiếu của node (các node tin cậy và phổ biến có các yếu tố trọng lượng khác nhau (yếu tố tin tưởng);
5. Loại bỏ khỏi danh sách ứng viên của các giao dịch chưa được xác nhận chưa được xác minh hoặc có xác nhận phủ định ;
6. Xây dựng một danh sách các giao dịch đã được xác nhận để thêm vào hồ sơ ;
7. Thêm giao dịch vào hồ sơ với dấu thời gian và mã băm của block chứa giao dịch ;
8. Gửi block với các giao dịch đến tất cả các node network. Khi nhận được, nó được thêm vào các đăng ký của tất cả các node.

Xây Dựng Và Bắt Đầu Hồ Sơ

Toàn bộ quá trình có thể được mô tả theo trình tự sau:

1. Người dùng cuối của mạng trong hệ thống tạo ra một giao dịch.
2. Khi tất cả các điều kiện của hợp đồng thông minh quy định trong đó được đáp ứng, người sử dụng sẽ khởi tạo hành động (giao dịch) thông qua việc gọi phương thức bắt buộc sử dụng phần mềm nền tảng.
3. Để làm theo các nguyên tắc cơ bản của blockchain, hạt nhân của các trình xác nhận sẽ theo dõi sự đồng bộ hóa và sự bất biến của phiên bản sổ cái mới nhất.
4. Vào thời điểm xây dựng sự đồng thuận, tất cả các giao dịch nhận được trong suốt chu kỳ được thu thập trong block.
5. Một số được gán cho block, bao gồm dấu thời gian và số nhận diện node được chuyển đổi thành mã băm, và sau đó khối được đặt trong mô đun đồng thuận.
6. Sau khi biên soạn danh sách trắng các ứng cử viên, không chỉ bảng băm của giao dịch được ghi vào hồ sơ, mà còn là bảng băm của block, để luôn xác nhận nguồn gốc dựa trên nó.

7. Băm này là một loại chữ ký của block và là người tạo ra block này với các giao dịch.
8. Sau khi xây dựng sự đồng thuận sử dụng một thuật toán tìm kiếm liên kết, các giao dịch được thêm vào block được chuyển đến hạt nhân của trình xác nhận để được ghi vào hồ sơ.

Những Giao Dịch Không Có Trong Đăng Ký

Các giao dịch không nằm trong danh sách các giao dịch đã sẵn sàng được đánh dấu là bị từ chối. Thông tin về việc này được hiển thị ngay tại người gửi (người khởi xướng) giao dịch.

Các giao dịch không bao gồm trong hồ sơ vẫn còn trong tập các ứng cử viên và được lưu trữ trong các node network. Tất cả các giao dịch mới nhận được bởi máy chủ tại thời điểm đồng thuận cũng đến đó, và sau đó quá trình tìm kiếm bắt đầu một lần nữa. Một hoạt động tuần hoàn liên tục của mạng cho phép thực hiện các giao dịch trong một khoảng thời gian khá ngắn trong khi vẫn duy trì độ tin cậy cao và sự liên quan của thông tin.

3. Xử Lý Giao Dịch

Giao Dịch

Giao dịch là đơn vị tối thiểu của hệ thống thông báo nền tảng của việc thực hiện các phương thức hợp đồng hoặc chuyển trực tiếp giữa các tài khoản mà không tạo ra một hợp đồng thông minh, tiếp theo là sắp xếp kết quả trong mạng ngang hàng.

Đồng Bộ Xây Dựng

Hệ thống sử dụng một mô hình liên bang để xây dựng một sự đồng thuận bỏ phiếu của các node xác nhận đáng tin cậy, và cũng là thuật toán xây dựng sự đồng thuận - một thuật toán để thông qua một automat finitestate. Sự đồng thuận theo chu kỳ (bước thời gian), mỗi bước thời gian, các giao dịch được trích xuất và đặt trong một nhóm (mảng theo chiều dọc). Sau khi được đặt trong pool, tất cả các giao dịch được gửi đến các node đáng tin cậy để nhận được phản hồi. Nếu nhận được phản hồi, thì giao dịch mà yêu cầu thêm đã được gửi, có thể được thêm vào hồ sơ của trình xác nhận này. Sau đó, nó được gửi tới trình xác nhận kế tiếp trong mạng. Khi sự đồng thuận được xây dựng - vào cuối chuỗi mà tính pháp lý chuyển nhượng đã được xác nhận đầy đủ, giao dịch sẽ được gửi đến xác nhận với một dấu để viết và lưu vào hồ sơ.

Xử Lý Giao Dịch

Để đạt được bản chất phi tập trung của hệ thống, mỗi máy chủ phải có cả hai lưu trữ sổ cái và cũng là một xử lý đầy đủ điều khiển của tất cả các giao dịch.

Hệ thống sử dụng khái niệm hạt nhân hệ thống. Bằng hạt nhân, chúng tôi muốn nói đến một trình xử lý dữ liệu thực hiện một nhiệm vụ sản xuất cụ thể, bất kể tính khả dụng và khả năng hoạt động của các thành phần hệ thống còn lại. Mỗi hạt nhân, tại đầu vào, tại thời điểm tác vụ được thực hiện, nhận được một danh sách các biến để xử lý. Và luôn luôn có được một kết quả ở đầu ra - tích cực, bất kỳ khác hoặc một lỗi. Kết quả là, hạt nhân hệ thống luôn chứa mã phản ứng, ngoài các bộ dữ liệu chính. Cấu trúc này là cần thiết cho tốc độ cao nhất có thể của mỗi quá trình, mà phải làm việc độc lập với nhau.

Cấu Trúc Phần Đầu của Hồ Sơ

Để đạt được hiệu suất sổ sách đáng kể, nhưng đồng thời, mà không ảnh hưởng đến an ninh, chúng tôi đề xuất sử dụng một cơ sở dữ liệu sổ cái mà không cần xây dựng Merkle tree từ mã băm của block trước đó và kết quả giao dịch.

Merkle tree (TTH – Tiger Tree Hashing) là một loại hàm băm được sử dụng để kiểm tra tính toàn vẹn của dữ liệu, để có được một nhận dạng duy nhất của chuỗi, và để khôi phục chuỗi. Dữ liệu được chia thành các phần nhỏ - các block được băm riêng bằng Leaf Tiger Hash, sau đó là Internal Tiger Hash được tính từ mỗi cặp hashes onebyone. Nếu băm không có một cặp, sau đó nó được chuyển giao cho chuỗi mới không thay đổi. Tiếp theo, Internal Tiger Hash được tính lại trong chuỗi cho mỗi cặp. Thủ tục này được lặp lại cho đến khi có một hash còn lại.

Khi hồ sơ được vận hành bằng Merkle tree, tốc độ xử lý giao dịch rất thấp và tải trên các tài nguyên máy tính rất cao. Theo chúng tôi, đây không phải là sử dụng hợp lý lưu trữ dữ liệu

Cấu Trúc Hồ Sơ của CREDITS

Chúng tôi cung cấp để bỏ Merkle tree và sử dụng hồ sơ giao dịch trong hệ thống CREDITS, với mỗi mục bao gồm một mã băm của block giao dịch để thêm vào danh sách các ứng cử viên bổ sung cho hồ sơ. Ngoài ra, mục nhập có định danh node và dấu thời gian khi nó được tạo ra. Mục nhập hồ sơ bao gồm hướng giao dịch, tài khoản ban đầu và cuối cùng của nó, loại khoản nợ, số đơn rút vốn, loại tiền gửi, và số đơn vị gửi tiền. Nguyên tắc này làm tăng tốc độ xử lý giao dịch, làm tăng sự phức tạp của thay đổi sổ cái kế toán bất hợp pháp và loại trừ những thay đổi có thể có trong mục hồ sơ với sự lơ là.

Khối Lượng Block

Đơn vị thời gian là chu kỳ tìm kiếm các node chính và đáng tin cậy, và thời gian chu kỳ được tính toán tùy thuộc vào sự phức tạp của mạng. Mỗi đơn vị thời gian, mạng có chứa N các giao dịch được tạo ra và chuyển giao để xử lý vào mạng từ khi kết thúc chu kỳ trước, cho đến khi bắt đầu chu kỳ tiếp theo, để có được trạng thái của "Ứng cử viên được thêm vào hồ sơ." Các giao dịch được lựa chọn từ mạng N được đặt trên khối. Kích thước khối phụ thuộc vào số lượng các giao dịch trong đó.

Tìm kiếm Người tham gia Giao dịch

CREDITS mạng peer-to-peer có thể được biểu diễn dưới dạng một đồ thị, với các tài khoản người dùng dưới dạng các đỉnh và vô số các giao dịch có thể dưới dạng các cạnh trực tiếp kết nối hai đỉnh (tài khoản). Vì tất cả các cạnh có đầu tiên và đỉnh đầu cuối, bạn luôn có thể xây dựng một đồ thị định hướng (orgraph).

Nếu chúng ta có các điều kiện sau để nhận dạng:

- Bất kỳ giao dịch nào cũng có người gửi và người nhận;
- Bất kỳ đỉnh nào (tài khoản) luôn có thể được kết nối với một đỉnh với cạnh có hướng (giao dịch);
- Bất kỳ đỉnh của biểu đồ (tài khoản) có một số hữu hạn của các cạnh trực tiếp (giao dịch đến và đi).

Liên quan đến những điều đã nói ở trên, chúng ta có thể nói rằng orgraph chứa đường đi cần thiết để hoàn thành các điều kiện giao dịch cần thiết và xây dựng một chuỗi đơn giản. Bởi vì nó là một dãy hữu hạn các đỉnh, nơi mà mỗi đỉnh (ngoại trừ cuối cùng) được nối với đỉnh tiếp theo trong dãy bởi một cạnh.

Kênh truyền dữ liệu

Mỗi kênh truyền thông giữa node network chính và node chung của mạng tín chỉ là một luồng riêng biệt (đa luồng), trong đó dữ liệu được gửi ở dạng mật mã khi giao dịch được thực hiện.

Để đảm bảo an ninh mạng, tất cả dữ liệu giữa các node xác thực được truyền đi dưới dạng mã hoá, và mỗi kết nối giữa các node là thấp hơn dựa trên thư viện mạng. Nếu quá trình truyền dữ liệu diễn ra với lỗi, luồng sẽ tự động bị gián đoạn, mục nhập tương ứng được đặt để ghi vào hệ thống ghi nhật ký và sau đó đến tệp nhật ký. Dữ liệu được truyền qua các biến điển hình. Dữ liệu đã truyền được mã hóa sử dụng thuật toán RC4 đối xứng. Vì thuật toán này hoạt động dưới khóa bí mật thông thường, khóa này được truyền khi một kết nối được tạo ra giữa các node và được truyền đi dưới dạng mã hoá theo thuật toán DiffieHellman.

Thuật toán RC4, giống như bất kỳ mật mã luồng nào, được xây dựng trên cơ sở một máy phát bit giả ngẫu nhiên. Khóa được ghi vào đầu vào máy phát, và các bit giả ngẫu nhiên được đọc ở đầu ra. Chiều dài khóa có thể từ 40 đến 2048 bit. Các bit được tạo ra có sự phân bố đồng đều.

Thuật toán DiffieHellman cho phép hai bên nhận được khóa bí mật chung sử dụng một kênh không được bảo vệ từ nghe qua nhưng được bảo vệ khỏi sự thay đổi kênh truyền thông. Khóa nhận được có thể được sử dụng để trao đổi các tin nhắn sử dụng mã hóa đối xứng. Thuật toán dựa trên sự phức tạp của việc tính logarithms rời rạc. Trong đó, như trong các thuật toán khác với khoá công khai, các phép tính được thực hiện theo modulo đến một số nguyên tố lớn P.

Thứ nhất, một số tự nhiên nhất định A, nhỏ hơn P, được chọn theo cách đặc biệt. Nếu chúng ta muốn mã hóa giá trị X, thì chúng ta tính

$$Y = AX \bmod P.$$

Và dễ dàng tính Y có X. Vấn đề đảo ngược khi tính X từ Y khá phức tạp. Số X được gọi chính xác là logarithm rời rẽ Y. Do đó, biết được tính phức tạp của việc tính logarithm rời rạc, số Y có thể được truyền công khai vào bất kỳ kênh truyền thông nào, vì với một mô đun lớn P thì giá trị ban đầu X sẽ gần như không thể chọn được. Thuật toán DiffieHellman để tạo ra một khoá dựa trên sự kiện toán học này.

Mọi hành động trong hệ thống được gắn với dấu thời gian, số khối trước, đăng nhập của người dùng và ID hợp đồng thông minh. Điều này cho phép tìm kiếm các bản sao khi thực hiện. Nếu một bản sao được tìm thấy, sau đó chúng tôi thực hiện giao dịch đầu tiên từ hồ bơi, phần còn lại được coi là bất hợp pháp.

Hành Động Trong Hệ Thống

Hành động trong hệ thống là một giao dịch mô tả sự chuyển giá trị đơn giản nhất từ tài khoản sang tài khoản hoặc chuyển kết quả phương pháp hợp đồng sang trình xác nhận cho việc tìm kiếm một giải pháp trong hệ thống con.

Để tránh sự trùng lặp của giao tác trong cùng một khối với cùng một định danh, hệ thống chấp nhận một thỏa thuận rằng giao dịch thật sự và chính xác là lần đầu tiên đến hệ thống con của trình duyệt tính hợp lệ để xử lý. Vì nó đã được ghi lại trong hệ thống kiểm chứng mà một giao dịch đã được thực hiện từ tài khoản hiện tại và không có giá trị còn lại trong tài khoản để tiến hành giao dịch, không thể tìm thấy sự đồng thuận. Do đó, vấn đề chất thải kép được giải quyết.

Khi giao dịch được thực hiện, thông tin được nhận đến người kiểm chứng và xác nhận, thông tin về thay đổi trạng thái sổ cái được tự động phân phối cho tất cả các nút từ danh sách đáng tin cậy, sau đó sổ cái được đồng bộ hóa.

Để luôn luôn có một sổ cái giao dịch nâng cấp giữa tất cả các node đáng tin cậy cho node validator hiện tại, cần phải đồng bộ hóa giao dịch mới đến trong sổ cái của tất cả các node mỗi lần. Để giải quyết vấn đề này, cần sử dụng một cổng riêng để đồng bộ hóa (nếu có cơ hội như vậy). Cơ hội này sẽ làm tăng tốc độ xử lý thông tin đến hạt nhân của trình xác nhận do phân bố tải trên cổng. Chuỗi đồng bộ luôn được thực hiện, nó là chu kỳ. Ưu tiên phân bổ RAM và tải CPU (sử dụng chu kỳ CPU) thấp hơn mức trung bình. Bộ nhớ lưu trữ 1.000 thao tác cuối cùng và trạng thái của các tài khoản cho chúng (trong một mẫu mật mã sử dụng thuật toán đồng bộ), điều này làm tăng tốc độ đáp ứng các yêu cầu từ các nút xác thực khác.

Thêm giao dịch để xác nhận

Thêm các giao dịch vào sổ cái được gọi là chỉ từ hệ thống phụ validator ngay sau khi xây dựng sự đồng thuận và biên soạn một danh sách trắng với kết quả của các giao dịch tiết kiệm trong sổ cái. Gọi từ các hệ thống của bên thứ ba là không thể, để cải thiện an ninh.

Tham số đến - đối tượng mô tả giao dịch. Giá trị kết quả ResultValue <0 – thực hiện bị hủy bỏ với một lỗi, giá trị kết quả là một mã lỗi có thể / 0 <ResultValue - chức năng đã được thực hiện mà không có lỗi, kết quả là số mục nhập trong sổ cái.

Tham số đến - đối tượng chứa nhãn duy nhất của giao dịch, người gửi, người nhận, giá trị được chuyển giao, giá trị tương ứng, giá trị mong muốn, số tiền của giá trị được chuyển nhượng, giá trị mong muốn và thông tin hệ thống khác có thể được thay đổi nếu cần thiết.

Chi Phí Giao Dịch

Hệ thống sử dụng tiền tệ CREDITS, phục vụ:

- Là phương tiện thanh toán nội bộ cho việc sử dụng hệ thống ;
- Để đổi tiền tệ khác nhau trong hệ thống ;
- Trao đổi các giá trị trong hệ thống;
- Tạo và xử lý các hoạt động theo hợp đồng thông minh;
- Để mua thông tin từ các nguồn bên thứ ba cho các dịch vụ trong hệ thống.

Chi phí của một giao dịch có thể thay đổi tùy thuộc vào tải mạng, trên một người sử dụng cụ thể của hệ thống, về mặt lý thuyết có thể hướng một luồng giao dịch khổng lồ vào thời điểm cao điểm nhất định. Chúng tôi đề nghị sử dụng phương pháp vật liệu và tác động đến người dùng hệ thống để kiểm soát tải mạng.

Chi phí thực hiện giao dịch trong ba năm đầu tiên của hoạt động hệ thống sẽ được đặt riêng cho các loại giao dịch và hoạt động khác nhau. Trong tương lai, sẽ phát triển một thuật toán để tự động tạo ra chi phí giao dịch.

4. Hợp Đồng Thông Minh

Lời Nói Đầu

Hợp đồng thông minh trong hệ thống CREDITS là một thuật toán điện tử mô tả một tập hợp các điều kiện theo đó hành động và sự kiện trong thế giới thực hoặc các hệ thống số có thể được liên kết.

Để thực hiện các hợp đồng tự kiểm soát, một môi trường phân cấp hoàn toàn loại trừ yếu tố con người là cần thiết, và để sử dụng việc chuyển giao chi phí của một hợp đồng thông minh, cần phải có một ngân hàng mã độc lập với cơ quan trung ương.

Các đơn vị

Một hợp đồng thông minh trong CREDITS bao gồm các đơn vị sau đây:

1. Tài sản (các biến công cộng) - thực thể hệ thống lưu trữ dữ liệu công cộng cần thiết cho công việc của hợp đồng trong hệ thống Tín dụng.
2. Phương pháp là cơ quan hệ thống tín dụng chịu trách nhiệm theo dõi logic và trình tự của hành động khi tiến hành giao dịch (các hành động theo hợp đồng).

Những người tham gia vào hệ thống CREDITS ký các hợp đồng thông minh sử dụng phương thức gọi để sửa đổi các đặc tính của hợp đồng, bằng cách khởi động các quy trình để kiểm tra sự tuân thủ các điều kiện và phối hợp.

Một hợp đồng thông minh có hiệu lực sau khi các bên ký kết. Để đảm bảo tự động thực hiện các nghĩa vụ, cần có một môi trường sống tự động hóa hoàn toàn việc thực hiện các điều khoản hợp đồng. Điều này có nghĩa là các hợp đồng thông minh chỉ có thể tồn tại bên trong một môi trường mà không bị cản trở truy cập vào mã thực thi đối với các hợp đồng thông minh.

Tất cả các điều khoản hợp đồng phải có một mô tả toán học và logic rõ ràng về thực hiện. Do đó, nguyên tắc chính của một hợp đồng thông minh là tự động hóa hoàn chỉnh và độ tin cậy của quan hệ hợp đồng giữa các bên.

Phương thức hợp đồng thông minh

Phương thức hợp đồng thông minh CREDITS là đơn vị hệ thống chịu trách nhiệm tuân thủ logic và trình tự của các hành động trong quá trình giao dịch (các hành động theo hợp đồng).

Các logic và trình tự của các hành động được mô tả bởi một mã chương trình (module) chứa các lệnh, việc thực hiện tuần tự của chúng cho phép đạt được kết quả mong muốn. Mã này có thể xử lý các lệnh hệ thống (ví dụ lệnh chuyển nhượng), lệnh người dùng (các chức năng được viết riêng), các thuộc tính hợp đồng (các biến khởi tạo tĩnh hoặc tự động có sẵn từ bất kỳ phương thức hợp đồng nào) và các phương pháp từ bất kỳ hợp đồng bên thứ ba nào chỉ dành cho chủ sở hữu của hợp đồng kết nối (bên thứ ba). Để phổ biến hơn, sự phát triển được cung cấp bằng các ngôn ngữ kịch bản (ví dụ như, JavaScript).

Phương pháp (mã chương trình) cho phép sử dụng tất cả các toán tử ngôn ngữ kịch bản lệnh (lệnh) (lệnh, nhảy có điều kiện và không điều kiện), tạo các hàm và thủ tục (các thủ tục con), kết nối các thư viện của bên thứ ba.

Máy ảo thực thi

Phương pháp hợp đồng của hệ thống CREDITS được thực hiện trong môi trường ảo của hệ thống (Máy ảo, sau đây gọi là VM). Khi một phương thức được gọi cho một hợp đồng cụ thể, VM sẽ phân bổ một vùng bộ nhớ và tải bytecode hợp đồng trong đó chứa các phương thức và các biến được khởi tạo (hoặc được xác định lại khi gọi các phương thức hợp đồng khác). VM bắt đầu xử lý bytecode phương pháp, khi chạy, các biến và mã được nạp vào vùng nhớ, và các lệnh được thực hiện liên tiếp, kết quả của chúng được truyền đến mạng peer-to-peer để sắp xếp theo thứ tự trong hồ sơ.

Người khởi xướng phương thức thực hiện là người sử dụng hệ thống, thay mặt cho phương pháp này được khởi chạy.

Giới Hạn Giá Trị

CREDITS cryptocurrency cũng là một chỉ số về thời hạn giá trị của một đơn vị hợp đồng để so sánh hai đơn vị hoàn toàn khác nhau và xây dựng sự đồng thuận khi thực hiện hoặc chấp nhận hợp đồng bởi các bên. Thay vì đăng ký mỗi kết hợp giá trị / cổng riêng biệt, tín hiệu cryptocurrency của CREDITS đóng vai trò như một bó để thực hiện việc chuyển giá trị. Điều này là có thể bởi vì bất kỳ giá trị nào là lỏng đối với loại tiền tệ của tín dụng, có nghĩa là bất kỳ giá trị nào cũng có thể chất lỏng với bất kỳ giá trị nào khác.

Thực hiện các Điều khoản Hợp đồng Thông minh

Thời hạn hợp đồng trong hệ thống CREDITS là các giá trị của các trường kích hoạt (kiểm tra) bắt buộc phải đóng (hoàn thành) hợp đồng.

Thực hiện các điều khoản hợp đồng thông minh là một thủ tục khi các trường kích hoạt (mong muốn) được kiểm tra cho một giá trị tương đương mong muốn. Có ba cách để tìm ra giải pháp để thực hiện các điều khoản hợp đồng:

1. Hợp đồng được ký kết giữa hai hoặc nhiều bên để chuyển nhượng giá trị. Trong trường hợp này, việc thực hiện hợp đồng là việc cung cấp chi phí tương đương với giá trị cho bên chuyển giao từ bên nhận.
2. Hợp đồng được ký kết giữa các bên để chuyển giá trị, nhưng phải thanh toán khi thực hiện một số điều kiện nhất định (ví dụ như giao hàng cho bên nhận).
3. Một hợp đồng chuyển đổi một giá trị sang một loại khác có chi phí tương đương dưới dạng tín chỉ tiền gửi được đặt trong hệ thống. Trong trường hợp này, nền tảng này bắt đầu tìm kiếm con đường ngắn nhất có thể trao đổi một giá trị cho một người khác thông qua chuyển đổi trong các hợp đồng khác. Bất kỳ việc thực hiện hợp đồng nào có thể được cung cấp cho mỗi giao dịch, hoặc cho một số giao dịch, sẽ tạo cơ hội để thu thập số lượng yêu cầu của các đơn vị giá trị để hoàn thành hợp đồng.

Data Sources

Để làm việc chính xác và đầy đủ, kiểm tra và cung cấp thêm thông tin, để tạo ra một giải pháp cân bằng và tối ưu hơn, CREDITS sử dụng các nhà cung cấp dữ liệu bên thứ ba. Sự cần thiết phải đưa thêm các nguồn dữ liệu vào hệ thống là do sự không đầy đủ của thông tin công khai về một hoặc nhiều bên hợp đồng (ví dụ như có được tình trạng tín dụng của bên vay để đưa ra quyết định phát hành tín dụng).

Để làm việc với các hệ thống thông tin của bên thứ ba, nền tảng này có thể gọi một xe buýt hội nhập, mà bằng cách truy cập từ xa tạo yêu cầu tới hệ thống của bên thứ ba (trang web) theo định dạng để trình bày dữ liệu trên cơ sở trả tiền cho người tham gia hệ thống thanh toán bằng tín dụng CREDITS.

Yêu cầu được gửi dưới dạng mã hoá tới các cổng và địa chỉ được cung cấp bởi các hệ thống thông tin khác với các cổng thông tin chuẩn. Kết quả của yêu cầu có thể là bất kỳ phản ứng nào đối với dịch vụ có chứa thông tin cần thiết để đưa ra quyết định hoặc mã lỗi mô tả tính không thể nhận được phản hồi yêu cầu và các bước có thể để loại bỏ sai sót.

5. Kế hoạch thực hiện

Kế hoạch kỹ thuật thực hiện dự án

	S1	S2	S3	S4	S5
	Pre-Alpha	Alpha	Beta	Release candidate	Release
Lưu trữ, đồng thuận đồng thuận mFA	FA : Key Thực hiện Thiết kế	mFA : Key Thiết kế Thực hiện PoW (ProofofWork) và PoC (ProofofCapacity)	mFA Tối ưu hóa	–	–

Data Store	Phân cấp, Ledger, NoSQL Store hoàn thành	Lịch sử tin nhắn	–	Blockchain lưu trữ	–
CVM (Credits virtual machine)	Thiết kế và thực hiện	Tích hợp với hệ sinh thái	Tối ưu hóa	Kiểm tra lỗi	–
Hệ thống của bên thứ ba	–	Thiết kế và thực hiện	tích hợp với toàn bộ hệ thống	–	tối ưu hóa
Động cơ suy diễn	Quy cách chính thức và các yếu tố thiết kế chính	tích hợp với Blockchain	Tối ưu hoá	–	–
Giao diện người dùng	Thực hiện	Thiết kế web UX	–	–	–
Ví	Thông số chính thức của Wallet		Thử nghiệm ứng dụng thiết kế UX	–	Android, iOS, ví của bạn
RPC & REST API	Đặc điểm chính thức	Blockchain Explorer	–	Thám hiểm của bên thứ ba	–

CREDITS cryptocurrency

Sau khi phát hành phiên bản phát hành của hệ thống, một khoản tiền cố định là 1.000.000.000 tín dụng sẽ được phát hành. Họ sẽ được trao đổi với các thẻ tiêu chuẩn ERC20, được ban hành trong lần bán thẻ đầu tiên. Chúng sẽ được trao đổi với tỷ giá cố định: 1 mã thông báo chuẩn ERC20 = 1 đơn vị tiền tệ tín dụng.