BITSOAR

ĐI ĐẦU TRONG TIỀN TỆ ĐIỆN TỬ

2017.11.10

Mục lục

Blockchain trong cuộc cách mạng công nghiệp 4

Bitcoin là chuỗi khối tạo ra đồng tiền mã hóa.
Cơ sở hạ tầng này sử dụng công nghệ mã hóa và công nghệ mạng phân tán, đã chứng minh được thực tế rằng "Trong thời gian qua, các giao dịch trực tuyến an toàn và minh bạch đã có thể được vận hành"

Ngoài ra, nhiều chuyên gia cũng dự đoán rằng blockchain sẽ là một công nghệ có thể làm lung lay và phá hủy thị trường toàn cầu.
Ngay khi Internet xuất hiện, các doanh nghiệp như Netscape và Yahoo đã đưa ra các dịch vụ như công cụ tìm kiếm, thương mại điện tử và e-mail.

Cho dù dữ liệu của người khác có đáng tin hay không, bạn có thể sử dụng một mạng lưới phân phối được gọi là blockchain và tất cả những người tham gia giao dịch này sẽ được minh bạch. Do đó, có rất ít khả năng giả mạo và giả mạo, và chi tiết giao dịch có thể được chia sẻ minh bạch. Ngoài ra, nó rất hữu ích vì nó có thể sử dụng ít tài nguyên máy tính hơn so với hiện tại. Khi AI và IoT được kết nối với kinh doanh thực, dự kiến rằng cơ sở hạ tầng như block chain đóng một vai trò quan trọng khi trao đổi thông tin khác nhau giữa các đối tượng hoặc khi thanh toán được thực hiện tự động.

Hiện trạng của công nghệ Blockchain

Công nghệ Blockchain ban đầu được thiết kế như là một blockchain công cộng hoặc sổ cái phân phối công cộng mà bất cứ ai có thể tham gia. Tuy nhiên, như bitocin chứng minh, sổ cái phân phối công cộng có một số vấn đề kỹ thuật và thực nghiệm.

Vấn đề là phải đặt nhiều nguồn lực để duy trì một mạng lưới trong đó có số người tham gia không cố định. Có nhiều nhược điểm khác nhau như vấn đề thông tin nội bộ liên quan đến việc chuyển giao được tiết lộ minh bạch, tốc độ xử lý rất chậm và ẩn danh của thương nhân.

Vì lý do này, chỉ có một số lượng hạn chế người tham gia, chủ yếu là trong ngành tài chính toàn cầu, công nghệ blockchain được thành lập không công khai đã được nhấn mạnh. Điều này là bởi vì bạn có thể tận dụng lợi thế của một mạng lưới chuỗi khối tự động xử lý giao dịch thực hiện và giải quyết trong thời gian thực đồng thời đảm bảo tính ổn định của mạng mà không cần tận dụng sức mạnh tính toán khổng lồ của Bitcoin blockchain. Một chuỗi khối không được liệt kê, còn được gọi là phân nhánh được phân phối theo giấy phép, dự kiến sẽ cho phép hoạt động hiệu quả hơn đồng thời giải quyết được nhiều vấn đề mà các chuỗi chặn hiện có đã có.

BITCOIN LÀ GÌ?

Đây là đồng tiền mã hóa đầu tiên của thế giới do Nakamoto Satoshi phát triển vào ngày 3 tháng 1 năm 2009.
Đơn vị tiền tệ của đồng xu bit là BTC.
Không giống như đồng tiền thông thường, Bitcoin cho phép giao dịch nhanh chóng và an toàn giữa các cá nhân (P2P) mà không có chính phủ, ngân hàng trung ương hoặc tổ chức tài chính can thiệp, không giống như tiền tệ sẵn có, nó có thể được thực hiện nhiều hơn nếu chính phủ mong muốn, phân phối được giới hạn đến 21 triệu USD. Đồng xu bit được khai thác ở mức 50 BTC mỗi 10 phút và mức bồi thường khai thác mỏ giảm một nửa trong vòng 4 năm.

- Phát tiền xu bit ban đầu: Ngày 3 tháng 1 năm 2009 (Phần thưởng 50 BTC)
- Hạn bán nửa: 28 tháng 11 năm 2012 (Phần thưởng 25 BTC)
- Hạn bán nửa thứ hai: ngày 10 tháng 7 năm 2016 (Phần thưởng 12.5 BTC)
- Hạn bán nửa thứ ba: Dự kiến tháng 7 năm 2020 (Phần thưởng 6,25 BTC)

Và đồng xu bit mở đầu cho một hệ thống phân cấp được gọi là một cuốn sổ cái phân phối.
Một đặc trưng khác nữa, thay vì nặc danh, nó đang là một hệt thống minh bạch hơn bất kì một hệ thống tài chính nào trên thế giới.
Nghĩa là, thông qua cuốn sổ cái phân phối, không chỉ tôi, mà ai cũng có thể thấy được các chi tiết giao dịch của người khác

Tính đến ngày 5 tháng 11 năm 2017, nó được giao dịch với 8.35 triệu won cho mỗi 1BTC. Biến động về giá rất cao vào tháng 1 năm 2015, nó đã giảm xuống 290,000 won cho mỗi 1BTC, năm 2013, khi nó được giao dịch ở mức giá cao, nó đã có hơn 1 triệu won cho 1 BTC. Ngày 22 tháng 5 năm 2017 vượt quá 3 triệu won. Sự đột biến tăng vào ngày 25 tháng 5 năm 2017 khiến giá 1BTC tăng lên 4,22 triệu won, con số này đã giảm xuống còn 2,7 triệu won vào ngày 27 tháng 5 và ổn định ở mức 3,2 triệu won tính đến tháng 6 năm 2017. Sau đó vào ngày 16 tháng 7 năm 2017, vì cuộc khủng hoảng hard fork, con số này đã giảm xuống còn 2,2 triệu won. Sau đó, vào ngày 1 tháng 8, giá đã tăng lên đáng kể so với 3,2 triệu won trước đó. Sau đó, nó đã lên đến 5 triệu won, và từ ngày 5 đến ngày 6 tháng 5 năm 2017, giá đã tăng hơn 800.000 won trong một ngày, vượt quá giá trị tối đa là 6.500.000 won.

SỰ CẦN THIẾT CỦA BITSOAR

Bitcoin là một tiền tệ điện tử sáng tạo dựa trên chuỗi khối (block chain) nhưng do không có bộ máy pháp lý, đối tượng điều khiển thực sự làm cho tính an toàn bị giảm xuống, đây chính là điểm bất lợi nhất của nó.

Đặc biệt là đối với người dân bình thường nói chung để lưu trữ một cách an toàn và sử dụng tiền điện tử là một việc làm khá khó khăn và phức tạp

Vì vậy BITSOAR được thiết kế để giải quyết mức độ ổn định thấp của đồng xu bit và những nhược điểm của việc sử dụng tiền tệ phức tạp và khó khan. Đây là một loại tiền tệ tiên tiến được tạo ra. Thông qua điều này, BITSOAR sẽ tiếp tục cải thiện giá trị kỹ thuật và tiền tệ của đồng xu bit.

Chính sách Phát triển BITSOAR

BITSOAR là một loại tiền tệ điện tử được phát triển bằng cách kế thừa các đặc tính cấu trúc của đồng bitcoin vô cùng hoàn hảo và ổn định. Và chúng tôi sẽ phát triển nền BITSOAR để sử dụng BITSOAR một cách an toàn và thuận tiện ở đây.

Tổng số BITSOAR phát hành là 3.980.000.000 BSR.

Vì lượng BITSOAR ban hành đã được xác định trước nên việc giá trị đồng tiền này sẽ giảm sau khi lạm phát kết thúc là gần như không xảy ra

Những người tham gia của BITSOAR là các cơ sở, nhà điều hành, người đào coin và người sử dụng.

• Quỹ có trách nhiệm thiết lập và phổ biến các chính sách phát triển và hoạt động của BITSOAR. Mục đích của chính sách ở đây là một bộ quy tắc có thể kích thích giá trị của BITSOAR và kích hoạt giao dịch.

• Các nhà khai thác chịu trách nhiệm theo dõi và xác nhận việc tuân thủ các chính sách phát triển và hoạt động của BITSOAR. Đặc biệt, nó cũng đóng một vai trò lắng nghe các khiếu nại của khách hàng, xử lý các yêu cầu, và tạo ra và xuất bản các báo cáo về chúng.

• Người khai thác coin sẽ giữ vai trò duy trì hệ thống BITSOAR và nhận tiền xu như một khoản bồi thường.

• Bạn là người thực sự sử dụng hệ thống BITSOAR. Người sử dụng có thể mua một đồng xu thông qua hệ thống BITSOAR và gửi hoặc nhận đồng xu.

THÔNG SỐ BITSOAR

- Tên đồng xu: BITSOAR COIN
- Ký hiệu đồng xu (đơn vị): BSR
- Tổng cộng: 3.980.000.000 (đường khai thác 3,68 tỷ)
- Loại khai thác: 300 triệu
- Loại tiền xu: PoW
- Giải thuật Hashing: X11
- Tỷ lệ giao dịch: 10 TPS (600 Tốc độ / phút)
- Kích thước khối: biến (1MB đến 4MB)
- Thời gian chặn: 600 giây (10 phút)

- Số bộ bù: 50
- Số khối: 144
- Bán thời gian: 1 năm

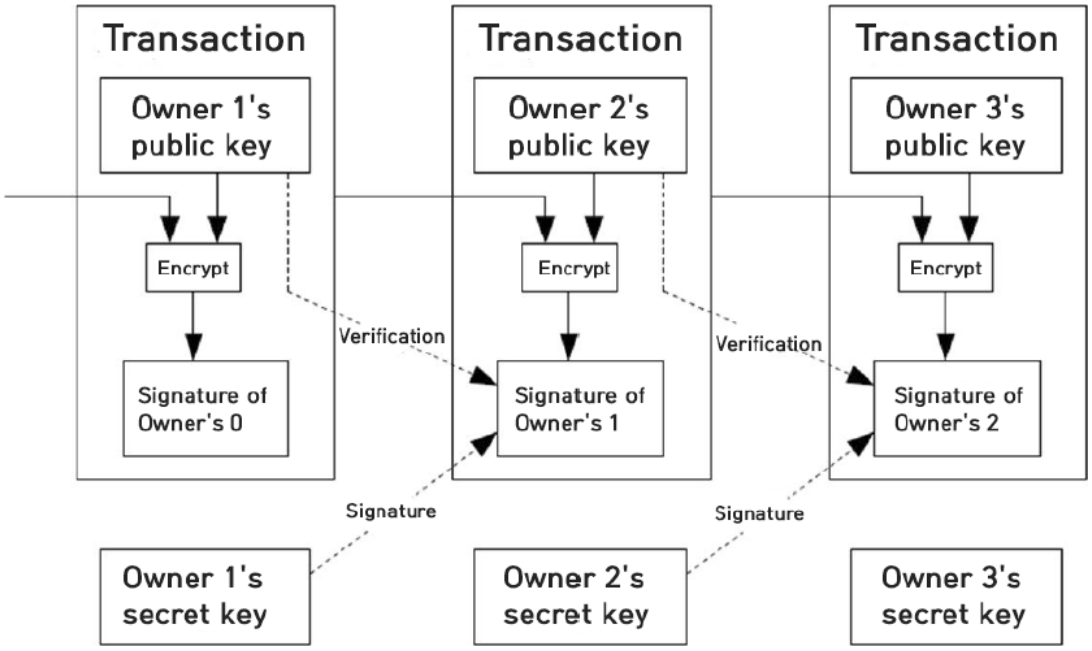
Thuật toán của BITSOAR

Thuật toán cho BITSOAR là X11.
X11 là một thuật toán phức tạp hơn nhiều so với SHA256, và nó ngăn ngừa sự tập trung của sức mạnh hàm băm bằng máy đào chuyên dụng.
X11 là một thuật toán hàm băm quay vòng thực hiện bằng cách tuần tự áp dụng 11 thuật toán hàm băm khác nhau.
11 thuật toán liên quan là blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, và echo.

Dưới đây là các loại đồng coin đại diện cho thuật toán X11

Giao dịch Bitsoar

Trong hệ thống BITSOAR, mỗi giao dịch chứa một chữ ký số cho mỗi giao dịch, nó cũng bao gồm luôn một khóa công khai để xác minh chữ ký số. Hình dưới minh họa việc sử dụng chữ ký số trong các giao dịch BITSOAR.



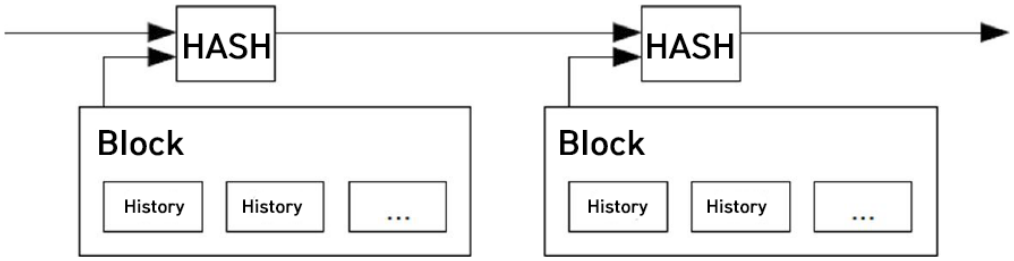
Các chuỗi khối trong hệ thống BITSOAR lưu trữ tất cả các giao dịch được thực hiện, mỗi giao dịch chứa một tập hợp chữ ký số và khóa công khai.
Kết quả là tất cả những người tham gia trong hệ thống BITSOAR đều có thể xác minh được tất cả các giao dịch xảy ra trước đó
Nếu bạn xác minh chữ ký điện tử của một giao dịch nào đó, bạn có thể thấy những điều dưới đây.

- Bên thứ ba đã giả mạo hoặc giả mạo nội dung giao dịch
- Bên thứ ba đã thực hiện giao dịch, chẳng hạn như ăn cắp
- Chủ sở hữu hợp pháp của đồng xu đã thực hiện giao dịch đúng

Để phát hành một giao dịch, bạn cần một cặp khóa chính và khóa riêng. Chiều dài khóa của cặp khóa BITSOAR là 256 bit trở lên sử dụng thuật toán mật mã elliptic đường cong (ECDSA).
Một lợi thế của việc sử dụng thuật toán mã hóa đường elliptic là nó có thể được thực hiện bằng cách sử dụng các phím ngắn hơn với mức độ mã hóa tương đương với các chương trình khác như RSA hoặc ElGamel, kết quả là, hiệu suất xử lý có thể được cải thiện.

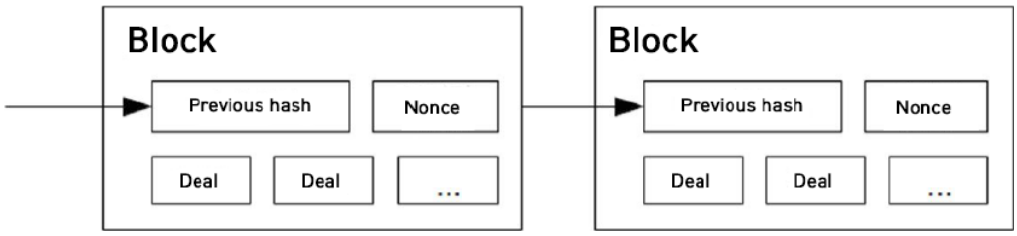
Máy chủ dấu thời gian (Time Stamp Server)

Hệ thống BITSOAR bắt đầu với một máy chủ dấu thời gian.
Máy chủ dấu thời gian hoạt động bằng cách băm một khối của mỗi mục cần được đánh dấu thời gian và sau đó xuất bản băm sang các nút khác. Nó giống như một tờ báo hay hệ thống thông tin Usenet Post.
Dấu thời gian chứng minh rằng dữ liệu đã nhập vào mã băm rõ ràng đã tồn tại vào thời điểm đó. Mỗi dấu thời gian có một băm chứa dấu thời gian trước đó và tạo thành một chuỗi để tăng cường bảo mật của các dấu thời gian trước đó.



Chứng nhận việc làm (Proof of Work)

Để triển khai một máy chủ phân phối thời gian mạng phân tán dựa trên P2P, bạn cần sử dụng một hệ thống chứng chỉ làm việc tương tự như của Adam Back`s Hashcash [6] thay vì các phương tiện truyền thông. SHA-SHIFT LÀM VIỆC CHUYÊN NGHIỆP
Một thuật toán như 256 chứa quá trình tìm giá trị băm mật mã bắt đầu bằng một số bit. Trung bình, số lượng thời gian dành cho các nhiệm vụ này tăng theo cấp số nhân dựa trên số bit liên tiếp của 0 bit, mã hóa.
Có thể khẳng định rằng bài thơ được thực hiện một lần.
Mạng Stamp thời gian thực hiện một quá trình để tăng giá trị tạm thời (nonce) cho khối cho đến khi khối hash kết quả trong một băm của khối băm kết quả trong phương pháp hoạt động. Khi kết quả của công việc CPU đã đạt đến điều kiện làm việc, khối được cố định trừ khi quá trình được đảo ngược lại. Sau đó các khối tạo thành một chuỗi, và để thay đổi một khối, khối sẽ cần phải được xây dựng lại và quá trình chứng nhận làm việc sẽ cần phải được hoàn thành cho tất cả các khối.



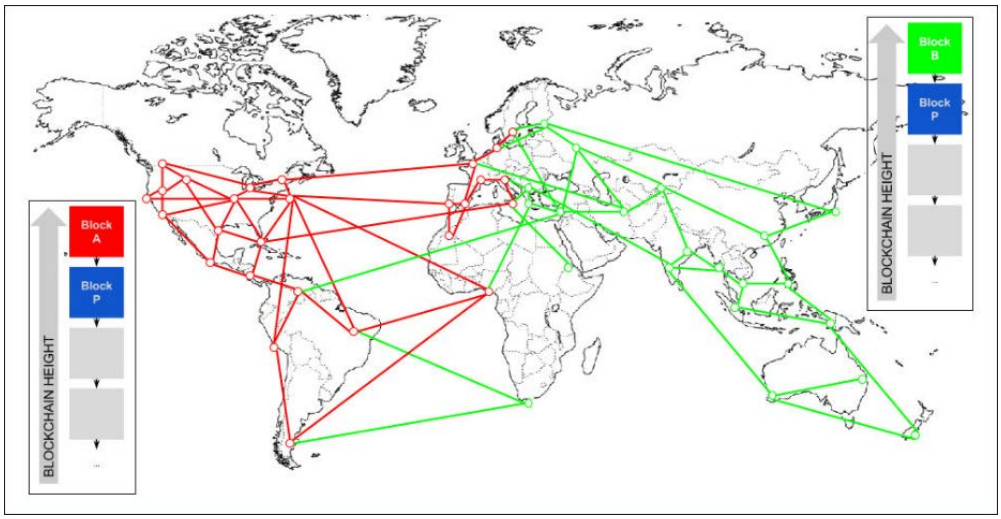
Bằng chứng công việc cũng giải quyết vấn đề xác định các quyết định ủy nhiệm trong quá trình ra quyết định. Nếu đa số hệ thống xác định một hệ thống dựa trên một hệ thống có thể chi trả một lần cho mỗi IP, bất cứ ai cũng có thể đảo ngược hệ thống bằng cách bảo đảm một số lượng lớn các địa chỉ IP. Nhưng bằng chứng về công việc chủ yếu là một cuộc bỏ phiếu cho mỗi CPU. Nó là một cấu trúc. Phần lớn các quyết định đại diện cho chuỗi dài nhất, làm cho nỗ lực để tận dụng tối đa công việc. Nếu phần lớn sức mạnh tính toán được kiểm soát bởi các nút trung thực, chuỗi trung thực sẽ là nhanh nhất, và dây chuyền cạnh tranh sẽ áp đảo đối thủ cạnh tranh.(Trong thực tế, nó chỉ ra rằng không nhiều hơn 50% tổng công suất tính toán, không quá 50% tổng công suất tính toán, không nhiều hơn 50% tổng công suất tính toán, nhưng toàn bộ số lượng toàn bộ máy tính lớn là Bây giờ lên đến 25%. Khả năng kẻ tấn công chậm được theo đuổi là để chỉ số giảm tiếp theo khi các khối được thêm vào. Để bù đắp cho tốc độ phần cứng tăng lên và sự tham gia của các nút trong nút, nhược điểm của nhiệm vụ là xác định Di chuyển trung bình dựa trên số lượng bình quân mỗi block mỗi giờ. Một khi khối được tạo ra quá nhanh, mức độ khó khăn tăng lên.

Mạng lưới (Network)

Các bước để vận hành mạng như sau.

1) Các giao dịch mới được phân phối đến tất cả các nút.
2) Mỗi nút tập hợp các giao dịch mới vào một khối.
3) Mỗi nút tiến hành chứng minh công việc để tạo ra một khối
4) Khi một nút tìm thấy một giải pháp cho chứng minh việc làm, thì khối đó sẽ chuyển đến tất cả các nút
5) Các nút có tất cả các thông tin giao dịch của khối trong đó bằng chứng của công việc là hợp lệ, nếu không có bản sao nào được sử dụng, khối này được chấp nhận.
6) Các nút hiển nhiên biểu thị rằng họ đã chấp nhận khối thông thường, bằng cách kết nối khối chấp nhận vào chuỗi và sau đó thực hiện nhiệm vụ tạo khối tiếp theo.

Hình dưới đây minh hoạ cho hai chuỗi khối riêng biệt. Việc này tự động được tổ chức thành một chuỗi đơn lẻ bằng thuật toán đồng thuận.



분리된 블록체인(https://mastanbtc.github.io/blockchainnotes/consensustypes)

Các nút luôn coi chuỗi dài nhất là đúng và thực hiện chuỗi để tiếp tục mở rộng.
Nếu hai nút được đồng thời thông báo về các phiên bản khác nhau của khối tiếp theo, một số nút sẽ nhận được một trong hai nút đầu tiên. Trong các trường hợp như vậy, mỗi nút thực hiện một công việc trên các khối mà họ nhận được, nhưng các chi nhánh khác của chuỗi được lưu trữ trong thời gian dài hơn thời gian. Nếu chiều dài của chuỗi được biết là dài hơn, chiều dài của chuỗi sẽ không còn bằng với chiều dài của chuỗi, và mỗi nút sẽ chuyển sang một thao tác ngắn hơn.
Chi tiết giao dịch mới không nhất thiết phải được chuyển đến tất cả các nút, và sớm hơn nó được chuyển đến nhiều nút, sớm hơn nó sẽ được bao gồm trong các khối. Cảnh báo chặn cũng không dễ bị tổn thương khi chúng bị thiếu. Nếu một nút không nhận được các khối, nó sẽ nhận các khối sau và nhận thấy rằng một nút bị thiếu.

Phần thưởng khai thác (Reward)

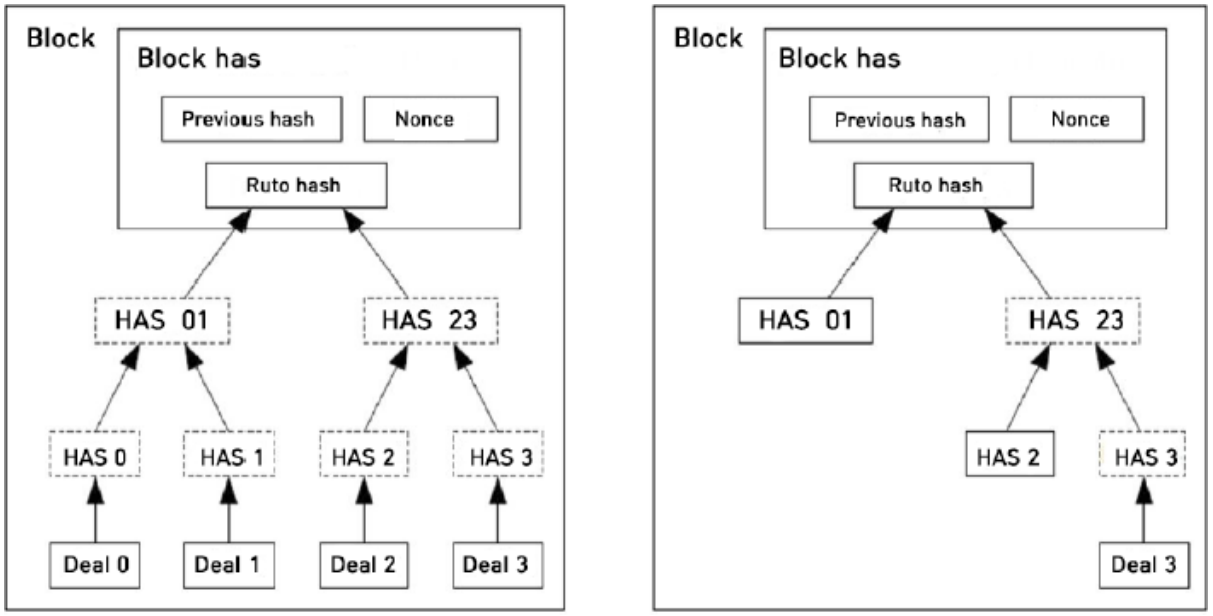
Theo quy ước, giao dịch ban đầu của một khối là một giao dịch đặc biệt mà tung ra một đồng xu mới thuộc sở hữu của người sáng tạo khối. Vì không có cơ quan trung ương phát hành đồng xu, giao dịch này bổ sung thêm một khoản tiền thưởng cho các nút hỗ trợ mạng, đồng thời cung cấp một cách để phân phối và phân phối tiền xu. Thêm vào đó, số tiền không đổi của đồng xu mới cũng tương tự như những thợ mỏ vàng chi tiêu tiền để thêm vàng vào lưu thông.

Những thứ được tiêu thụ trong hệ thống BITSOAR là thời gian CPU và điện. Tiền thưởng cũng có thể bao gồm chi phí giao dịch. Nếu giá trị đầu ra của một giao dịch nhỏ hơn giá trị đầu vào, sự khác biệt về giá trị là chi phí giao dịch được cộng vào giá trị ưu đãi của khối có chứa giao dịch. Một khi số tiền xu đã xác định trước bắt đầu lưu thông, số tiền thưởng đó được hoàn toàn chuyển thành chi phí giao dịch. Số tiền thưởng đó cũng không liên quan đến lạm phát.

Tiền thưởng là động lực khuyến khích các nút phải thành thật
Nếu một kẻ tấn công vô cùng tham lam có thể huy động sức mạnh của CPU nhiều hơn tất cả các nút trung thực, kẻ đó có thể chọn một trong hai cách: dùng CPU đó lừa gạt mọi người để đánh cắp chi phí chi trả hoặc dùng CPU để tạo ra một đồng coin mới. Những kẻ tấn công hệ thống thích mình có nhiều đồng xu mới hơn là kết hợp đồng xu của mọi người, chứ không phải để làm suy yếu hệ thống hợp pháp của hệ thống và sự giàu có của chính nó,
Theo các quy tắc này, kẻ tấn công nên nhận ra rằng việc điều hành một hệ thống sẽ tạo nên nhiều lợi ích hơn

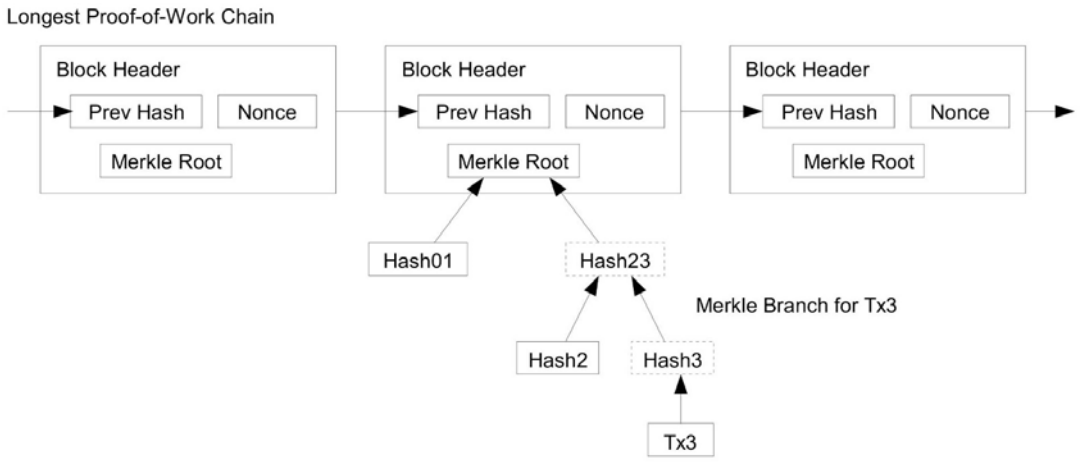
Mở rộng không gian lưu trữ (Increasing Disk Storage)

Một khi các giao dịch gần đây nhất của đồng xu được lưu trữ trong một khối có kích thước đầy đủ, các giao dịch được tiêu thụ trước khối đó có thể bị loại bỏ để tiết kiệm không gian lưu trữ. Để tiết kiệm không gian đĩa lưu trữ như vậy mà không phá hủy khối băm, người ta tạo ra Markle Tree là một giao dịch chỉ trên một khối hash chỉ bao gồm khối gốc. Markle Tree hợp nhất lặp lại quá trình tạo hai băm thấp thành một, cuối cùng tạo một băm.



Đơn giản hóa thanh toán (Simplified Payment Proof)

Có thể chứng minh thanh toán mà không sử dụng toàn bộ nút mạng. Người dùng chỉ cần có một bản sao của khối tiêu đề của chuỗi dài nhất. Bản sao của khối tiêu đề có chuỗi dài nhất của nó, có thể thu được bằng cách truy vấn các nút khác cho đến khi bạn chắc chắn rằng bạn đã có được các chi nhánh của cây Merkle liên kết với khối có chứa các giao dịch mong muốn. Người dùng không thể xác định chính xác các giao dịch, bằng cách đặt khối có chứa các giao dịch trong chuỗi dài nhất, nó có thể được gián tiếp xác nhận rằng khối đã được nhận trong chuỗi dài nhất, tiếp theo là các khối khác.



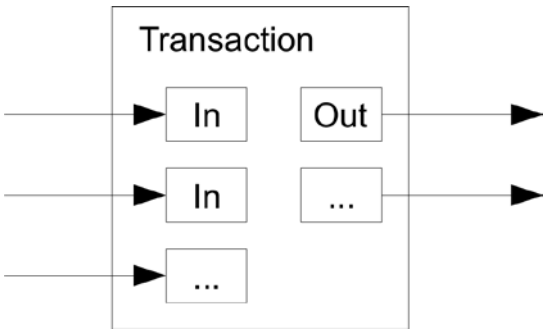
Nếu mạng được kiểm soát bởi các nút trung thực, đáng tin cậy, nếu kẻ tấn công có nhiều nguồn lực chiếm ưu thế hơn các nút trung thực trong mạng, mạng đó sẽ dễ bị suy yếu hơn. Các nút mạng có thể tự xác minh các chi tiết giao dịch, nhưng có thể được vô hiệu hoá bằng cách đơn giản thao tác và duy trì các giao dịch với một mạng lưới mà là một kẻ tấn công. Một chiến lược bảo vệ các phương pháp này là các nút mạng nhận được cảnh báo khi người dùng

tải các khối khối và tìm các khối khối mâu thuẫn với phần mềm của người dùng. Trong trường hợp thanh toán thường xuyên, có lẽ sẽ cần các hệ thống an ninh độc lập và phương pháp xác thực nhanh trên các nút riêng của họ.

Có thể xác minh rằng thanh toán được thanh toán ngay cả khi nó không ghi toàn bộ nút mạng. Nếu bạn chỉ có một bản sao của tiêu đề khối của chuỗi dài nhất chứng minh làm việc, bạn có thể yêu cầu nút mạng là chuỗi dài nhất và chỉ chấp nhận một phần của cây chặn được kết nối với khối đã ghi lại. Bạn không thể xác nhận Chi tiết giao dịch và có thể kết nối với chuỗi và xác nhận rằng nút mạng đã được chấp thuận bởi mạng và đã được xác nhận để xác nhận rằng khối đã được phê duyệt thêm.

Giá trị kết hợp và riêng biệt (Combination and Splitting Value)

Mặc dù có thể tự mình quản lý một đồng xu, sẽ rất rườm rà khi phân chia các khoản tiền vào các giao dịch của Cent và biến chúng thành các giao dịch riêng biệt. Để tách biệt và kết hợp các giá trị, một giao dịch sẽ bao gồm nhiều đầu vào và đầu ra. Thông thường sẽ có nhiều đầu vào và tối đa là hai đầu ra kết hợp một đầu vào đơn lẻ hoặc một lượng nhỏ tiền bởi một giao dịch lớn trước đó. Trong hai kết quả đầu ra này, một là thanh toán, và số kia, nếu có, là số tiền trả cho người gửi.

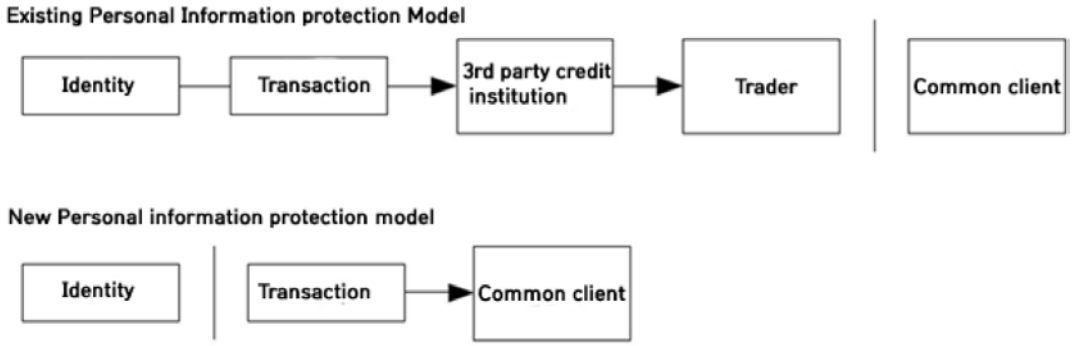


Nếu một giao dịch đơn lẻ phụ thuộc vào nhiều giao dịch hoặc các giao dịch của họ phải chịu nhiều giao dịch hơn, các hoạt động tách và phát triển những điều này (Fan-out) không phải là vấn đề. Nó không phải là cần thiết ở tất cả để trích xuất một bản sao của một người đọc hoàn thành chạy trên lịch sử giao dịch.

Bảo mật (Privacy)

Mô hình ngân hàng truyền thống đạt được xếp hạng về quyền riêng tư bằng cách hạn chế quyền truy cập vào các bên có liên quan và thông tin bên thứ ba đáng tin cậy. Mô hình này bị loại trừ vì cần công bố công khai tất cả các giao dịch, Tuy nhiên, sự riêng tư vẫn có thể được duy trì bằng cách chặn luồng thông tin ở những nơi khác. Điều này có thể bằng cách giữ cho khóa công khai vô danh.

Ai cũng có thể biết rằng ai đó đang gửi tiền cho người khác, tuy nhiên, không có thông tin về ai liên kết giao dịch. Điều này cũng tương tự như đánh giá thông tin được công bố bởi sở giao dịch chứng khoán, trên sàn chứng khoán, băng ghi thời gian và kích thước của mỗi giao dịch được tiết lộ, nhưng họ không nói họ là ai.



Là một tường lửa bổ sung, để ngăn chặn các bên liên kết với chủ sở hữu chung, một cặp khóa bí mật mới phải được sử dụng cho mỗi giao dịch. Trong giao dịch nhiều đầu vào, một số liên kết vẫn không thể tránh khỏi, điều này chắc chắn thể hiện một thực tế là đầu vào của họ là thuộc sở hữu của cùng một người. Nếu chủ sở hữu của khóa được biết đến, có nguy cơ liên kết sẽ làm cho các giao dịch khác thuộc cùng một chủ sở hữu được biết.

Tính toán (Calculation)

Hãy xem xét kịch bản của một kẻ tấn công cố gắng tạo ra một chuỗi thay thế nhanh hơn so với chuỗi máy chủ lưu trữ. Ngay cả khi điều này xảy ra, hệ thống BITSOAR sẽ an toàn trước những thay đổi, chẳng hạn như việc tạo ra đồng xu bất hợp pháp hoặc đánh cắp đồng xu.
Các nút sẽ không chấp nhận thanh toán cho các giao dịch không hợp lệ,
Các nút trung thực sẽ không bao giờ thừa nhận các khối có chứa chúng.

Kẻ tấn công có thể cố gắng thay đổi một trong những giao dịch của mình để nhận tiền gần nhất. Cuộc chạy đua giữa chuỗi trung thực và kẻ tấn công có thể được xác định bởi Cuộc đi bộ ngẫu nhiên nhị phân. Sự kiện thành công là một chuỗi trung thực có thể được mở rộng bằng một khối bằng cách tăng dần đầu của nó bằng +1, sự kiện thất bại cũng là một chuỗi các kẻ tấn công có thể được mở rộng bởi một khối bằng cách giảm khoảng cách bằng -1.

Xác suất bắt kịp kẻ tấn công từ bất kỳ mức thâm hụt cụ thể nào cũng tương tự như một người đánh bạc bị phá sản.
Giả sử một con bạc với tín dụng không hạn chế bắt đầu từ thâm hụt và cố gắng đạt được một thách thức vô hạn để đạt được một điểm hòa vốn.
Chúng ta có thể thấy rằng kẻ tấn công đã đạt đến một điểm hòa vốn
Ngoài ra, xác suất kẻ tấn công bắt kịp chuỗi trung thực có thể được tính như sau.

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

Trong phương trình trên, p là một nút trung bình, q là nút kẻ tấn công, và qz là xác suất tìm một nút trung bình. Nếu giả thiết p> q được đưa ra, xác suất giảm theo cấp số nhân với số khối người tấn công phải bắt kịp. Ngược lại, nếu kẻ tấn công không có may mắn sớm, cơ hội của hắn sẽ trở nên nhỏ bé và biến mất.

Bây giờ, cho đến khi chúng tôi hoàn toàn chắc chắn rằng người gửi sẽ không thể thay đổi giao dịch, chúng ta hãy kiểm tra xem người nhận giao dịch mới cần chờ đợi bao lâu.
Chúng tôi giả định rằng kẻ tấn công là người gửi muốn người nhận tin rằng kẻ tấn công đã tự trả tiền cho một thời gian, sau đó trả lại khoản thanh toán cho chính bạn sau một thời gian đã trôi qua. Khi điều này xảy ra, người nhận sẽ nhận được một cảnh báo, tuy nhiên, người gửi hy vọng rằng sẽ xảy ra rất muộn.

Người nhận tạo một cặp khóa bí mật mới và cũng gửi khoá công khai đến người gửi ngay trước khi ký. Điều này ngăn cản người gửi chuẩn bị một chuỗi khối trước khi tiếp tục làm công việc đó, cho đến khi kẻ tấn công được may mắn có được chuỗi phía trước của anh ta và tại thời điểm đó có dây chuyền. Khi một giao dịch được gửi đi, người gửi không trung thực sẽ bí mật bắt đầu nhiệm vụ tính toán trong một chuỗi nối có chứa một phiên bản thay thế của giao dịch của mình.

Người nhận chờ đợi cho đến khi giao dịch được thêm vào khối và các khối z được liên kết với khối sau đó. Người đó sẽ không biết số lượng chính xác mà kẻ tấn công đã thực hiện. Tuy nhiên, giả sử rằng khối trung bình có một thời gian ước tính trung bình cho mỗi block, đường cong hồi quy tiềm năng của kẻ tấn công có thể là một phân bố Poisson với các giá trị mong đợi sau:

$$\lambda = z\frac{q}{p}$$

Bây giờ, để xác định xác suất mà kẻ tấn công vẫn đang bắt kịp, chúng ta nhân hàm Poisson Density bằng số lượng tiến trình có thể được thực hiện bởi xác suất mà kẻ tấn công có thể bắt kịp tại thời điểm đó.

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{cases}(q/p)^{(z-k)} & if\ k\le z\\ 1 & if\ k>z\end{cases}$$

Công thức để ngăn chặn biểu thức được tính là vô hạn như sau.

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

Nếu bạn thực hiện phần này trong ngôn ngữ C như sau.

```
#include <math.h>

double AttackerSuccessProbability(double q, int z)
{
  double p = 1.0 - q;
  double lambda = z * (q / p);
  double sum = 1.0;
  int i, k;
  for (k = 0; k <= z; k++)
  {
        double poisson = exp(-lambda);
    for (i = 1; i <= k; i++)
    poisson *= lambda / i;
    sum -= poisson * (1 - pow(q / p, z - k));
  }
return sum;
}

```

Nếu bạn chạy một số kết quả, bạn có thể thấy rằng xác suất giảm theo số mũ với z.

Chiến lược tăng giá trị BITSOAR

Tổ chức BITSOAR nên tiết lộ và thực hiện các chiến lược để hỗ trợ, ổn định, hoặc ngăn chặn sự suy giảm hơn nữa giá trị của BITSOAR.

Thứ nhất, chiến lược bình ổn của BITSOAR như sau.

- Quỹ nhận được một phần của BITSOAR
- Tăng cường các hoạt động tiết lộ tích cực (+) để ổn định

Thứ hai, chiến lược Tăng cường của BITSOAR như sau.

- Thực hiện tăng vốn tự do
- Tăng cường các hoạt động tuyên truyền tích cực (+) để hỗ trợ

Thứ ba, chiến lược đầu tư của BITSOAR như sau.

- Đầu tư phát triển đồng xu
- Đầu tư vào các tổ chức phúc lợi công cộng và phúc lợi xã hội
- Đầu tư mở chi nhánh và thương nhân
- Đầu tư vào hoạt động tiền xu

Quỹ BITSOAR sẽ tiếp tục phấn đấu để tăng giá trị đồng tiền và mở rộng chiến lược.

Chiến lược Mở rộng của BITSOAR

BITSOAR là một đồng tiền được thiết kế để đáp ứng cuộc cách mạng công nghiệp kỹ thuật số và có thể tích cực kết hợp kinh doanh hợp nhất thế kỷ 21 với trí thông minh nhân tạo, số liệu lớn, Internet của sự vật và nền kinh tế chia sẻ. Lợi thế nền tảng của BITSOAR sẽ làm tăng thêm giá trị của BITSOAR. Sau đây là các API được cung cấp để hỗ trợ kinh doanh CNTT trong BITSOAR.

- Coin API để chuyển điểm sang BITSOAR
- Cung cấp 'API tương tác DB' có thể liên kết các DBS khác nhau
- Cung cấp 'Exchange API' cho hoạt động trao đổi riêng
- Cung cấp 'API quản lý hoạt động' hỗ trợ hoạt động độc lập
- Cung cấp 'Wallet API' cho việc phát triển ứng dụng ví
- Cung cấp 'máy chủ kiểm tra' cho các mục đích thử nghiệm

BITSOAR được thiết kế dựa trên cơ sở kiến trúc linh hoạt và cảnh báo,đồng thời, nó được thực hiện bằng ngôn ngữ hiện đại và có khả năng chi tiêu rất tốt. Tính năng này rất hữu ích để dễ dàng tích hợp BITSOAR vào các lĩnh vực khác nhau, cuối cùng sẽ dẫn đến kinh doanh tiền xu thành công

Lộ trình BITSOAR

Nhóm BITSOAR được thành lập vào ngày 15 tháng 10 năm 2015 và là một đội mạnh dẫn nhiều dự án.

I. Thiết lập team coin	**II. Định nghĩa thông số của coin**
- Cấu trúc member coin - Khảo xác thị trường Coin - Tổ chức hội thảo Coin - Chuẩn bị bản thảo …	- Định nghĩa coin - Logo coin - Thiết kế coin - Thiết kế Blockchain
III. Nghiên cứu máy coin	**IV. Chuẩn bị và tiến hành ICO**
- Nghiên cứu mô dun đào coin - Nghiên cứu mô dun chuyển coin - Nghiên cứu mô dun Ví Coin - Nghiên cứu mô-đun xác thực Coin - Nghiên cứu mô-đun quản lý Coin	- Bản lộ trình ICO - Khảo sát tính hợp pháp của ICO - Chuẩn bị trình bày ICO - Phát triển hệ thống phát hành token ICO - Phát triển hệ thống đăng nhập ICO
V. Phát triển máy coin	**VI. Phát triển nền tảng Coin**
- Phát triển mô dun đào coin - Phát triển mô dun chuyển coin - Phát triển mô dun Ví Coin - Phát triển mô-đun xác thực Coin - Phát triển mô-đun quản lý Coin	- Phát triển server giao dịch - Phát triển server Blockchain - Phát triển ví Coin - Phát triển hệ thống đào Phát triển hệ thống ứng dụng
VII. Đăng kí sàn giao dịch Coin	**VIII. Thành lập quỹ coin**

- Đăng ký nguồn GitHub - Đăng kí dịch vụ khai thác coin - Đăng kí dịch vụ tìm kiếm blockchain - Đăng kí dịch vụ API	- Mục đích của Quỹ - Định nghĩa hoạt động chính - Bản dự thảo ngân sách - Xây dựng chính sách

Thành lập Quỹ BITSOAR

Tổ chức BITSOAR là một tổ chức phi lợi nhuận quản lý tất cả các thông tin liên quan đến BITSOAR. Tổ chức BITSOAR làm theo các bước sau đây.

① Thông tin đại diện ④ Thông tin về tiền tệ và phát hành trái phiếu / cổ phiếu ⑤ Chính sách và quy định ⑥ Các cuộc họp và hướng dẫn của Hội đồng ⑦ Các thành viên và chính sách của hội đồng ⑧ Tài chính và kế toán ⑨ Các điều khoản bổ sung

Nhiệm vụ của Quỹ BITSOAR

Quỹ BITSOAR cam kết tăng cường giá trị thực chất của coin.
Chúng tôi muốn thiết lập một chiến lược có hệ thống. Cụ thể như sau

- Thành lập chi nhánh Bitsoar Việt Nam ở TP HCM
- Nhanh chóng lên sàn ở sàn giao dịch quốc tế
- Lên sàn ở nhiều sàn giao dịch quốc tế khác nhau
- Triển khai ví trên điện thoại di động toàn cầu (hỗ trợ đa ngôn ngữ)
- Thiết lập cơ sở hạ tầng toàn cầu (Nga, Anh, Nhật, Trung Quốc, Việt Nam, Brazil, Mông Cổ, Paraguay, Thái Lan)
- Thẻ VISA có sẵn để thanh toán toàn cầu
- Mở 1000 chi nhánh ở Trung Quốc và Việt Nam
- Lắp đặt máy ATM ở Trung Quốc và Việt Nam

Nhóm Bitsoar

Các thành viên ở bộ phận kế hoạch và quảng bá BITSOAR như sau

	**Sangdong Kim, CEO**: Korea, Inha Univ. Sangdong Kim, CEO của trường đại học tư thục Inha Hàn Quốc. Ông đã từng đảm nhiệm chức vụ giám đốc của một công ty IT hàng đầu, chuyên về tính toán điện tử (khoa học máy tính). Ông nhận được bằng khen từ Bộ trưởng Bộ Ngoại giao và Bộ trưởng Bộ Khoa học Sáng tạo Tương lai
	**Attila Ferencz, Rumania, CIO**: Rumania, Cluj-Napoca Univ. Rumania, Cluj-Napoca Univ. Ông đã giữ chức vụ giáo sư trong nhiều năm liền sau khi ông nhận được bằng tiến sĩ tin học, Ông đã làm việc với tư cách là một nhà nghiên cứu tiền nhiệm của viện nghiên cứu KT và viện nghiên cứu phát triển của tập đoàn điện tử Sam Sung từ năm 1999. Hiện tại ông đang hoạt động với tư cách là một chuyên gia tiền tệ mã hóa.
	**Sergei Kuratov, Russia, CTO**: Ông là một chuyên gia IT có 20 năm kinh nghiệm, ông đang hoạt động với tư cách là một chuyên gia thiết kế phần cứng và phần mềm máy tính cho các trang web dịch vụ có quy mô lớn ở Mỹ, Israel, Nhật Bản, Hàn Quốc, Trung Quốc và Tây Ban Nha vv…

Kết luận

BITOAR không chỉ có thể trao đổi trong và ngoài nước, mà nó còn có thể được sử dụng chỉ cho mục đích kinh doanh. Ngoài ra, khi đăng ký trong giao dịch tiền tệ điện tử, người dùng chung có thể chủ động mua và bán đồng xu. Nó cung cấp cơ hội để đồng bộ với các doanh nghiệp khác nhau và có thể mang lại những lợi ích hợp lý.
Quỹ BITSOAR và các thành viên của nó cũng sẽ cố gắng hết sức để giúp các nhà đầu tư đạt được lợi nhuận đáng kể và ổn định.

Tài liệu tham khảo

01. Alt chains and atomic transfers: https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949
02. B-money: http://www.weidai.com/bmoney.txt
03. Bitcoin, A Peer-to-peer Electronic Cash System: https://bitcoin.org/bitcoin.pdf
04. Colored coins whitepaper: https://tinyurl.com/coloredcoin-whitepaper
05. Decentralized autonomous corporations, Bitcoin Magazine: https://tinyurl.com/Bootstrapping-DACs
06. Ethereum: https://ethereum.org.
07. Ethereum Merkle Patricia trees: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-Patricia-Tree
08. Ethereum RLP: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-RLP
09. GHOST: http://www.cs.huji.ac.il/~avivz/pubs/13/btc_scalability_full.pdf

10. Intrinsic value: https://tinyurl.com/BitcoinMag-IntrinsicValue
11. Jae Kwon. Cosmos, A Network of Distributed Ledgers: https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md
12. Joseph Poon and Tadge Dryja, Lightning Network: https://lightning.network/lightning-network-paper.pdf
13. Mastercoin whitepaper: https://github.com/mastercoin-MSC/spec
14. Merkle trees: http://en.wikipedia.org/wiki/Merkle_tree
15. Mike Hearn on Smart Property at Turing Festival: http://www.youtube.com/watch?v=Pu4PAMFPo5Y
16. Namecoin: https://namecoin.org/
17. Patricia trees: http://en.wikipedia.org/wiki/Patricia_tree
18. Paul Sztorc. Drivechain - The Simple Two Way Peg: http://www.truthcoin.info/blog/drivechain/
19. Peter Todd. Tree Chains: https://github.com/petertodd/tree-chains-paper
20. Peter Todd on Merkle sum trees: http://sourceforge.net/p/bitcoin/mailman/message/31709140/
21. Raiden. Raiden Network: https://raiden.network/
22. Reusable proofs of work: http://www.finney.org/~hal/rpow/
23. Secure property titles with owner authority: http://szabo.best.vwh.net/securetitle.html
24. Golden Master and Branch whitepaper: http:/www.gmbcoin.org/gmb-whitepaper.pdf/
25. Simplified payment verification: https://en.bitcoin.it/wiki/Scalability#Simplifiedpaymentverification
26. Smart contracts: https://en.bitcoin.it/wiki/Contracts
27. Smart property: https://en.bitcoin.it/wiki/Smart_Property
28. StorJ and Autonomous Agents, Jeff Garzik: https://tinyurl.com/storj-agents
29. The Bitcoin Model for Crowdfunding: https://startupboy.com/2014/03/09/the-bitcoin-model-for-crowdfunding/
30. Vitalik Buterin. Ethereum Sharding FAQ: https://github.com/ethereum/wiki/wiki/Sharding-FAQ
31. Zooko's triangle: http://en.wikipedia.org/wiki/Zooko's_triangle