THIẾT KẾ MASTERNODE CỦA ANTCOIN NETWORK

GIỚI THIỆU TỔNG QUAN :

- Trong bài viết này, chúng tôi trình bày về một thiết kế kiến trúc tổng quan về công nghệ và giải pháp AntCoin, Ant Coin là một blockchain tương thích với EVN (Máy ảo Ethereum) với những ưu điểm sau :

+ giá trị giao dịch thấp chỉ với 2 số nhị phân

+ Thời gian xác thực nhannh chỉ với 2s

+ Xác thực kép ngẫu nhiên và đảm bảo an ninh.

+ Sự đồng thuận của Proof-of-Stake Voting (PoSV), đây là một giao thức blockchain dựa trên (PoS) với cơ chế bỏ phiếu cực kỳ công bằng, đảm bảo an ninh nghiêm ngặt và tính nhanh chóng.

+ Cơ chế phần thưởng mới,

+ Blockchain có xác suất fork thấp, thời gian chuyển đổi cực nhanh.

+ Masternode !

+ Ngành công nghiệp blockchain và sơ sở hạ tầng của Internet of Value đang được xây dựng nhanh chóng toàn cầu.

Vào những năm 2008,Satoshi Nakamoto - ”đã đề xuất“ giao thức blockchain BTC, còn được gọi là Blockchain 1.0

Sau đó, ETH tức là Etherum với Máy ảo Ethereum (EVM) đã đề xuất một số cải tiến đáng kể so với Bitcoin, ETH có hợp đồng thông minh.

Nhưng cả ETH và BTC đều có một số vấn đề chung, đó là hiệu suất xử lý giao dịch, và thời gian cũng như chi phí. Chính vì những vấn đề như thế, nên để xây dựng một giao thức đồng thuận an toàn và hiệu quả cho Antcoin, chúng tôi giải quyết các vấn đề chính sau đây của các blockchain cổ điển ngày trước.

Các vấn đề sau đây :

+ Tính hiệu quả: Các blockchain hiện tại được sử dụng bởi các loại tiền điện tử chính (ví dụ BTC và ETH) không mở rộng quy mô tốt để xử lý khối lượng giao dịch lớn,ETH hoặc BTC chỉ có thể xử lý khoảng 10 giao dịch / giây .

+ Về thời gian xác định : Thời gian để xác nhận 1 khối BTC cần khoản 10 phút để đạt được 1 xác nhận, nhưng phải cần xác định tổng cộng 6 khối thì mới được xác nhận hoàn thành, vậy thời gian ta cần phải ít nhất là 60 phút cho 6 khối.(với

tỷ lệ thấp) thời gian giao dịch nhanh hay chậm còn phụ thuộc vào số lượng phí trả khi giao dịch.

+ Còn riêng với ETH thì cần ít nhất cũng khoản 13 phút, và cũng tùy thuộc vào phí GAS trả cho từng giao dịch.

+ Fork : Vấn đề của Fork chain tiêu tốn năng lượng tính toán, thời gina và tạo ra các lỗ hổng tiềm ẩn cho hackker có thể xâm nhập.

Với những vấn đề đã đề cập ở trên .

Để bắt đầu giải quyết những vấn đề này, trong bài báo này, chúng tôi trình bày thiết kế kiến trúc tổng quan về các nút chính của Antcoin.

+ Đặc biệt, chúng tôi đề xuất sự đồng thuận Bỏ phiếu bằng chứng cổ phần (PoSV),

Vậy PoSV là gì ?

Đây là một giao thức blockchain dựa trên Bằng chứng cổ phần (PoS) với cơ chế bỏ phiếu công bằng, đảm bảo bảo mật nghiêm ngặt và tính nhanh chóng.

AntCoin là gì?

AntCoin là một blockchain công cộng có thể mở rộng được xây dựng trên một lớp hiệu suất giúp đạt được tốc độ giao dịch cao mà không ảnh hưởng đến sự phân quyền. AntCoin sử dụng một phương pháp đồng thuận sáng tạo được gọi là Proof of Stake Voting, khuyến khích tất cả chủ sở hữu mã thông báo AntCoin đóng một vai trò tích cực trong việc đặt cược trên mạng lưới gồm 150 Masternode chất lượng cao và để theo dõi hiệu suất và quản trị của họ một cách chủ động.

Chuỗi khối AntCoin và hệ sinh thái sản phẩm của nó cho phép các doanh nhân, doanh nghiệp và tổ chức xây dựng các dự án blockchain giàu tính năng, hiệu suất cao trên nền tảng tương thích EVM nâng cao. Một loạt các tính năng và giao thức ban đầu được thiết kế để hỗ trợ tất cả các nhu cầu về tốc độ, quyền riêng tư, khả năng sử dụng và thanh khoản của người dùng trong một nền tảng.

+ AntCoin Hoạt Động Như Thế Nào?

AntCoin dựa trên hệ thống 150 Masternode có sự đồng thuận của Proof of Stake Voting (POSV) có thể hỗ trợ phí thấp (khoảng 1/100 của Ethereum) và thời gian xác nhận giao dịch trong 2 giây. Tính bảo mật, ổn định và tính cuối cùng của chuỗi được đảm bảo thông qua các kỹ thuật mới như Xác thực kép, đặt cược thông qua hợp đồng thông minh và quy trình ngẫu nhiên hóa thực sự.

THIẾT KẾ ANCOIN MASTERNODE

Hiểu một cách đơn giản, masternode là một máy chủ trên mạng phi tập trung. Nó được sử dụng để hoàn thành các chức năng duy nhất theo cách mà các nút thông thường không thể. Masternode có thể được sử dụng cho các tính năng như gửi trực tiếp / giao dịch tức thời hoặc giao dịch riêng tư.

Để đi vào chi tiết hơn về masternode, chúng ta hãy dạo qua một chút về Blockchain.

Blockchains, theo nghĩa rộng của cơ chế đồng thuận được chia thành 3 loại: POW (bằng chứng công việc), POS (bằng chứng cổ phần) và hỗn hợp cả 2 loại. Mỗi loại chuỗi khối phải có một cơ chế xử lý các giao dịch cho phép chuỗi khối hoạt động.

Các blockchain với cơ chế POW, chẳng hạn như Bitcoin, được hỗ trợ bởi các ‘thợ mỏ’ – những người xử lý các giao dịch bằng các khối ‘khai thác’ sau đó được thêm vào blockchain. Khi một khối được khai thác, thợ đào được thưởng, trong trường hợp này là Bitcoin. Tuy vậy, các hệ thống POW rất tốn năng lượng và ngành công nghiệp tiền điện tử đang dần chuyển sang một loại blockchain thay thế, tiết kiệm năng lượng hơn gọi là POS.

Việc chạy một masternode giống như PoS, theo nghĩa là bạn tạo thu nhập thụ động thông qua một masternode chỉ bằng cách giữ tiền của bạn, tương tự như cách mà bạn kiếm được trong các hệ thống PoS.

Do khả năng phát triển của chúng, các masternode thường cần một khoản đầu tư lớn để có thể chạy. Nhưng nó vẫn được khuyến khích sử dụng, vì các nhà

khai thác masternode sẽ được thưởng bằng cách kiếm được một phần thưởng khối trong bất kỳ loại tiền điện tử nào mà họ tham gia khai thác.

Các masternode không giống nhau vì mỗi mạng đều có ưu và nhược điểm riêng, nhưng cùng với điều đó, mỗi hệ thống lại có các khoản thanh toán theo những cách khác nhau. Một số loại tiền điện tử trả phần thưởng cho các nhà khai thác masternode nhiều lần trong một ngày, trong khi một số khác trả một lần mỗi ngày. Lợi ích của tính năng động này là các nhà khai thác vẫn có thể kiếm tiền và cung cấp dịch vụ cho mạng mà không phải đầu tư vào thiết bị khai thác Bitcoin & tiền điện tử đắt tiền.

Masternode hoạt động như thế nào?

Giống như các nút đầy đủ trong các loại tiền điện tử, Masternode có thể được điều hành bởi bất kỳ ai. Tuy nhiên, có một bước an ninh để đảm bảo rằng toàn bộ hệ thống không bị tấn công. Bước an ninh đó cụ thể là bạn cần phải cam kết hoặc thế chấp một số lượng nhất định loại tiền điện tử để có thể đủ điều kiện chạy Masternode.

+ Số tiền yêu cầu tiền gửi cho vai trò masternode được đặt ở mức 50 000 $. Số tiền này bị khóa trong một hợp đồng thông minh bỏ phiếu.

+ Điều này được thực hiện để đảm bảo rằng chủ sở hữu masternode không gian lận hoặc làm hỏng hệ thống.

Vì vậy, rất ít sảy ra khả năng một người điều hành masternode sẽ gian lận vì người này có cổ phần trong việc điều hành toàn bộ hệ thống và ngay cả khi cố tình gian lận, người đó sẽ bị trừng phạt dưới hình thức phá giá HODL của chính họ

Bây giờ bạn đã hiểu khái niệm về masternode, hãy xem những yêu cầu để thiết lập nó:

Cần một lượng tối thiểu tiền điện tử:

Chẳng hạn đối với DASH MN, bạn cần 1000 đơn vị DASH và đối với PIVX MN, bạn cần 10.000 đơn vị PIVX. Vì vậy, số lượng tối thiểu này thay đổi phụ thuộc vào loại tiền điện tử bạn chọn.

Cần một máy chủ để lưu trữ ví đó

Cần một địa chỉ IP dành riêng cho máy chủ.

Cần một số không gian lưu trữ để lưu blockchain

Lợi ích Masternode đem lại với nhà đầu tư

Người sở hữu Masternode sẽ được chia phần thưởng khối vì đã cung cấp các dịch vụ đặc biệt cho mạng lưới. Phần thưởng chi trả dựa trên số lượng masternode trên hệ thống cũng như giá trị của đồng coin tại thời điểm đó. Chúng ta có thể nhận vài coin 1 ngày, 1 số masternode khác trả thưởng vài lần/ngày, điều này làm cho masternode trở thành 1 biểu mẫu “thu nhập tự động ” trong thế giới tiền kỹ thuật số mà không cần phải đầu tư quá nhiều tiền và máy móc.

Hệ thống quản trị phi tập trung này còn cho phép các Nút (Node) bỏ phiếu cho những phát triển quan trọng trong blockchain. Để bù đắp cho những rắc rối của mình, masternode thường chia sẻ 45% phần thưởng khối với các thợ mỏ của blockchain. 10% còn lại được chuyển đến quỹ kho bạc của blockchain, và các nhà khai thác chịu trách nhiệm bỏ phiếu về các đề xuất về cách thức các quỹ này sẽ được phân bổ để cải thiện mạng lưới.

Đối với hệ sinh thái tiền ảo

Tính bảo mật

Masternodes bảo vệ blockchain khỏi các cuộc tấn công mạng như PoS. Chi phí hoạt động cũng giữ cho các nhà khai thác hoàn toàn trung thực. Không giống như các thợ mỏ Bitcoin, những người dễ thay đổi quyết định nếu lợi nhuận không cao, các nhà khai thác được khuyến khích duy trì đúng các masternode.

Khoản đầu tư ban đầu được xem như tài sản thế chấp, và nếu các nhà khai thác muốn kiếm được lợi nhuận, họ phải tuân theo các quy tắc của blockchain. Giữa chi phí hoạt động cao và lợi tức đầu tư hứa hẹn, đó là lợi ích tốt nhất của nhà điều hành để vận hành nút chính xác và không có bất kỳ mục đích xấu nào.

Masternode thậm chí có thể giữ chân thợ mỏ. Trong mô hình của Dash, các masternode trên mạng lớp thứ 2 theo dõi mạng lưới PoW đầu tiên. Điều này cho phép masternode từ chối các khối nếu thợ mỏ cố gắng thao túng phần thưởng khối.

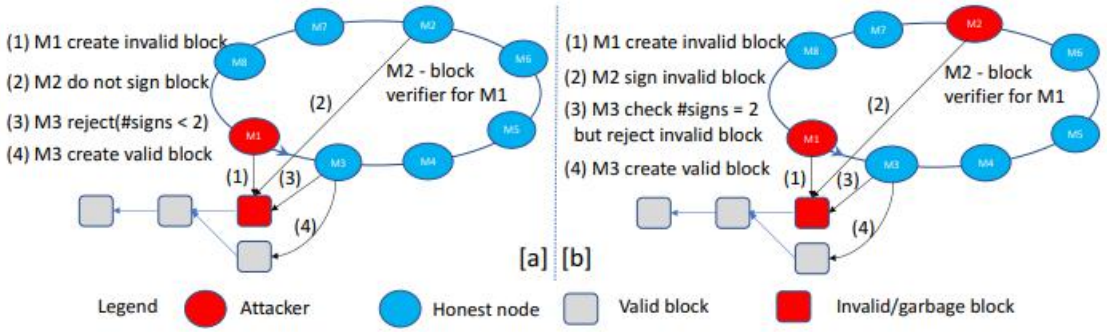


Fig. 3. Double Validation (DV): (a) DV with block creator as an attacker and (b) DV with both block creator and block verifier as attackers

• Xác thực đơn trong Xác thực đơn, trong một kỷ nguyên, mỗi biểu tượng chính, ví dụ: M1, tuần tự lấy

chuyển sang tạo một khối, ví dụ: khối100. Masternode tiếp theo, ví dụ: M2, trong trình tự sau đó xác nhận

đã tạo khối100. Nếu khối 100 không hợp lệ (điều đó có nghĩa là M1 là kẻ tấn công) và chứa

một giao dịch có lợi cho M1 một cách không hợp lệ, nếu M2 là trung thực (xem Hình 2 [a]), nó sẽ từ chối khối 100 và

tạo một khối khác 100 bên cạnh khối99. Tuy nhiên, nếu M2 là kẻ tấn công (xem Hình 2 [b])

với M1, M2 bỏ qua sự vô hiệu của khối 100, ký tên vào nó và tạo khối tiếp theo, cụ thể là khối101

điều đó là hợp lệ. Sau đó, nút chính tiếp theo M3 xác minh rằng khối101 là hợp lệ, M3 ký hiệu khối101 và

tạo ra một khối102. Bằng cách này, Xác thực một lần có khả năng khiến chuỗi khối có "rác"

hoặc các khối không hợp lệ yêu cầu "rebase" để khôi phục tính hợp lệ của blockchain.

• Xác thực kép Chúng tôi khẳng định rằng kỹ thuật DV của chúng tôi làm giảm đáng kể xác suất có

khối rác trong blockchain. Giả sử rằng M1 và M2 là trình tạo khối và xác minh khối,

tương ứng, đối với khối 100 trong DV của chúng tôi. Nếu khối 100 không hợp lệ và M2 là trung thực M2

sẽ không niêm phong khối này. Do đó, trình tạo khối tiếp theo M3 để tạo khối101 sẽ thấy rằng

block100 không có đủ 2 chữ ký, do đó hãy từ chối block100 và tạo block100 khác tiếp theo

tới khối99. Mặt khác, nếu M2 cũng là kẻ tấn công ghép nối / bắt tay với M1 (xem Hình 3 [b]),

M2 ký hiệu khối 100 mặc dù nó không hợp lệ (hãy nhớ rằng trình xác minh khối M2 được chọn ngẫu nhiên,

có rất ít cơ hội ghép nối thành công M1 và M2). Tiếp theo, mặc dù M3 sẽ xác minh rằng

block100 có hai chữ ký hợp lệ, M3 vẫn từ chối nó vì block100 không hợp lệ bởi M3

sẽ tạo một khối hợp lệ khác. Để phá vỡ sự ổn định và nhất quán của blockchain

trong trường hợp này, M3 nên là kẻ tấn công cùng với M1 và M2, tuy nhiên, có

xác suất. Nói cách khác, DV tăng cường tính nhất quán của blockchain

Tấn công DDOS

Masternode được khuyến khích chạy trong các nhà cung cấp đám mây công cộng nổi tiếng như AWS, Google Cloud hoặc Microsoft Azure cung cấp nhiều cơ chế ngăn chặn DDOS. Ngay cả trong trường hợp một số nút bị tấn công hoặc ngừng hoạt động, mạng vẫn hoạt động bình thường miễn là số lần bị lỗi và / hoặc bị tấn công các nút nhỏ hơn 1/4 số lượng nút chính.

Tấn công thư rác

AntCoin Network giữ cơ chế phí giao dịch giống như Ethereum được chỉ định thông qua gasPrice.

Tuy nhiên, AntCoin Network hỗ trợ phí giao dịch tối thiểu ,bằng cách nào đó cho phép gửi thư rác

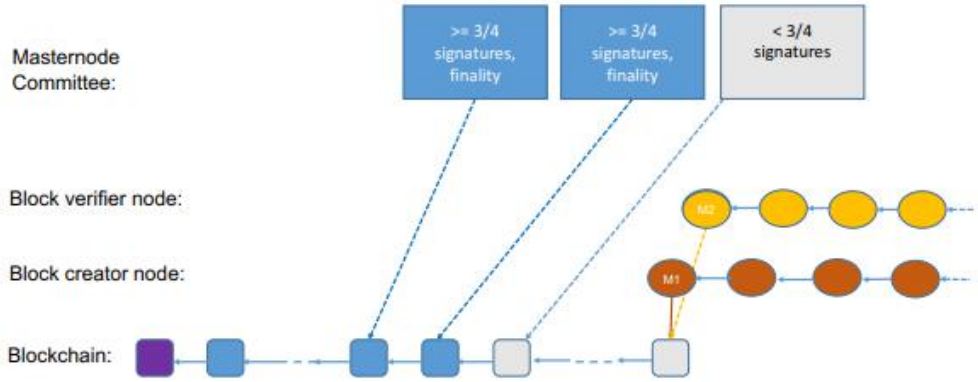
kẻ tấn công đó cố gắng phát một lượng lớn các giao dịch phí thấp vào hệ thống. Tuy nhiên, AntCoin Network masternode luôn sắp xếp các giao dịch và chỉ chọn các giao dịch có phí cao vào khối đề xuất. Vì vậy, những kẻ gửi thư rác có rất ít cơ hội làm hại hệ thống.

Phân tích tính cuối cùng

”Có một định nghĩa tiêu chuẩn về“ tổng kinh tế cuối cùng ”: nó diễn ra khi tất cả các masternode thực hiện các cược có tỷ lệ cược tối đa mà một khối hoặc trạng thái nhất định sẽ được kết thúc. Điều kiện này cung cấp rất mạnh mẽ

khuyến khích cho các masternode không bao giờ cố gắng thông đồng để hoàn nguyên khối: một khi các masternode đặt cược tỷ lệ cược tối đa như vậy, trong bất kỳ chuỗi khối nào không có khối hoặc trạng thái đó, các masternode sẽ mất toàn bộ tiền gửi của họ. "

AntCoin Network giữ tiêu chuẩn đó trong thiết kế để một khối được coi là không thể thay đổi nếu nó thu thập chữ ký của tất cả các ủy ban masternodes. Dòng thời gian của quá trình tạo blockchain, kiểm tra tính cuối cùng và đánh dấu khối là bất biến được mô tả như bên dưới



KẾT LUẬN VÀ KIỂM TRA

Trong bài viết này, chúng tôi đã đề xuất PoSV, một giao thức blockchain dựa trên PoS Voting với bỏ phiếu theo kinh nghiệm và công bằng cơ chế, đảm bảo an ninh nghiêm ngặt và hoàn tất nhanh chóng. Chúng tôi cũng đã trình bày một cơ chế phần thưởng mới và cho thấy rằng, với cơ chế này, blockchain có khả năng xảy ra fork thấp, xác nhận nhanh thời gian, cộng với những đóng góp và lợi

ích của các masternode là công bằng theo nghĩa là phân phối xác suất chức năng là đồng nhất cuối cùng.

Quan điểm

• Công việc trong tương lai Nhóm AntCoin Network hiện đang làm việc để thực hiện Bỏ phiếu Bằng chứng Cổ phần, sẽ được phát hành đúng tiến độ như đã nêu trong lộ trình của chúng tôi. Hơn nữa, song song với giao thức đồng thuận mới của chúng tôi, chúng tôi sẽ điều tra cơ chế Sharding để cung cấp thậm chí hiệu suất xử lý giao dịch tốt hơn. Chúng tôi tin rằng, kỹ thuật Sharding với số lượng masternode ổn định sẽ mang lại sự ổn định và hiệu quả tốt hơn cho blockchain. Tại đồng thời, chúng tôi cam kết duy trì các hợp đồng thông minh tương thích với EVM trong phạm vi chính của chúng tôi quy định.

• Tính bền vững về kinh tế cũng là một khái niệm quan trọng đối với mạng phi tập trung dựa trên blockchain.

Điều đó có nghĩa là để duy trì mạng ở một điều kiện bền vững, cần phải đạt được trạng thái cân bằng,trong đó chi phí vận hành cơ sở hạ tầng mạng có thể được bù đắp bằng doanh thu được tạo ra.

Trong bối cảnh này, chi phí của cơ sở hạ tầng mạng bao gồm hai phần: chi phí vật lý để có phần cứng như máy chủ, bộ nhớ vượt qua các yêu cầu kỹ thuật mạng; và thủ đô chi phí của việc AntCoin bị khóa vào các hợp đồng thông minh. Doanh thu cho Masternodes chủ yếu sẽ đến từ việc phát ra Reward Engine và sau đó là từ doanh thu dịch vụ như phí trao đổi mã thông báo được cung cấp bởi các ứng dụng chạy trên TomoChain. Chúng tôi sẽ xuất bản một TomoChain kinh tế phân tích và đề xuất, tách biệt khỏi tài liệu kỹ thuật này trong một ngày sau đó

Người giới thiệu :

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronics cash system. 2008.

[2] Ethereum Foundation. Ethereum’s White Paper. http://github.com/ethereum/wiki/white-paper, 2014. Online available 25/05/2018.

[3] D. Larimer. Delegated Proof-of-Stake (DPOS). BitShare White Paper 2014.

[4] S. King and S. Nadal. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. Self-Published, 2012.
[5] V. Buterin. On public and private blockchains. Ethereum Blog, 2015.

[6] A. Kiayias, A. Russell, B. David, and R. Oliynykov: Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. IACRCRYPTO-2017.

[7] D. Mingxiao, et al. A Review on Consensus Algorithms of Blockchain. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) Banff Center, Banff, Canada, October 5-8, 2017

[8] R. Pass and E. Shi. Rethinking Large-Scale Consensus. In the Proceedings of the IEEE 30th Computer Security Foundations Symposium, 2017.

[9] Thunder Token Foundation: Thunder Consensus White Paper, Janurary, 2018.

[10] R. Pass, L. Seeman, and A. Shelat. Analysis of the Blockchain Protocol in Asynchronous Networks. In EUROCRYPTO 2017.

[11] Juan A. Garay, A. Kiayias, and N. Leonardos. The bitcoin backbone protocol: Analysis and applications. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology - EUROCRYPT 2015, Volume 9057 of Lecture Notes in Computer Science, pages 281–310. Springer, 2015.

[12] Tendermint Team. Understanding the Basics of a Proof-of-Stake Security Model. https://blog.cosmos.network/understanding-the-basicsof-a-proof-of-stake-security-model-de3b3e160710. Online available 25/05/2018.

[13] V. Buterin. On Settlement Finality. https://blog.ethereum.org/2016/05/09/on-settlement-finality/. Online available 25/05/2018.

[14] EOS Team. EOS.IO Technical White Paper v2. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md. Online available 25/05/2018. 18

[15] Bitshares Team. Delegated Proof-of-Stake Consensus. https://bitshares.org/technology/delegated-proof-of-stake-consensus/. Online available 25/05/2018. [16] R. Pass, and E. Shi. (2017). Hybrid consensus: Efficient consensus in the permissionless model. In LIPIcs-Leibniz International Proceedings in Informatics (Vol. 91). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. [17] V. Buterin, and V. Griffith. (2017). Casper the Friendly Finality Gadget. arXiv preprint arXiv:1710.09437. [18] H. McCook. Under the Microscope: Economic and Environmental Costs of Bitcoin Mining. https://www.coindesk.com/ microscope-economic-environmental-costs-bitcoin-mining/. Online available 25/05/2018.

[16] Whitepaper Technical Tomochain

https://docs.tomochain.com/whitepaper-and-research