Bitcoin Krypton

BTC Eternity - Bitcoin Krypton

Sustainable in the future without updating P2P (Peer to peer) Electronic Currency System

Satoshi.K satoshi.k@bitcoinkrypton.org

https://bitcoinkrypton.org

Tóm lược:

“Giao dịch P2P là hoạt động mua và bán tiền mã hóa trực tiếp giữa những người dùng mà không qua trung gian. Trong đó, chữ ký số cung cấp một phần giải pháp, nhưng những lợi ích quan trọng sẽ bị mất đi nếu chúng ta vẫn cần một bên thứ ba đáng tin cậy để ngăn chặn việc chi tiêu kép. Do đó, chúng tôi đề xuất một giải pháp cho vấn đề chi tiêu kép bằng cách sử dụng giao dịch ngang hàng (peer-to-peer). Mạng lưới này đánh dấu thời gian giao dịch dựa trên cơ sở hàm băm (hashing algorithm) của bằng chứng công việc (POW: proof of work), tạo thành bản ghi không thể thay đổi, trừ khi thực hiện lại hành động đó. Chuỗi dài nhất không chỉ đóng vai trò làm bằng chứng cho trình tự các sự kiện đã xảy ra, mà chỉ ra rằng nó đến từ bộ xử lý trung tâm (CPU) lớn nhất. Miễn là phần lớn sức mạnh tính toán được kiểm soát bởi các nút (nodes) không hợp tác tấn công mạng, chúng sẽ tạo ra chuỗi dài nhất và vượt qua kẻ tấn công. Bản thân mạng sẽ chỉ yêu cầu cấu trúc tối thiểu. Các thông điệp được phát sóng theo phương thức nỗ lực tối đa, và các nút có thể thoát và tham gia lại mạng bất kỳ lúc nào, chấp thuận chuỗi POW dài nhất như một bằng chứng cho những gì đã xảy ra khi các nút không có mặt.”

Nội dung trên đây là bản tóm lược cho Sách trắng của ông Satoshi Nakamoto.

Trong phần tóm tắt gốc, Bitcoin đã đặt ra mục tiêu xây dựng một hệ thống tiền điện tử không cần bên thứ ba đáng tin cậy, thông qua cơ chế POW.

Tính đến năm 2024, 15 năm sau khi Bitcoin được công bố lần đầu tiên, Bitcoin gốc (Bitcoin Original) đã phát sinh một số vấn đề vì nguồn thông tin xác thực rằng khả năng tương thích giữa chương trình Bitcoin bản cập nhật mới và chương trình gốc không hoạt động như mong đợi. Điều này đặt ra câu hỏi về tính bền vững của Bitcoin trong tương lai, và như một giải pháp thay thế để giải quyết vấn đề, một chương trình tiền điện tử mới được đề ra nhằm có thể vận hành liên tục mà không cần bất kỳ cập nhật nào trong tương lai và cũng không cần bên thứ ba đáng tin cậy, nhưng vẫn đáp ứng các mục tiêu của Bitcoin gốc. Chúng tôi xin phép được công bố chương trình này với tên gọi Bitcoin Krypton.

0. Sự Khác Biệt Giữa Đồng Bitcoin Của Satoshi Nakamoto So với Bitcoin Hiện Tại

Bitcoin là một chương trình bắt đầu với việc phát hành mã nguồn vào tháng 1 năm 2009 và hoạt động theo mô hình P2P. Mặc dù ban đầu xuất hiện những nghi ngại về tiềm năng thành công, Bitcoin đã phát triển thành một tài sản quan trọng trong tài chính toàn cầu, với số lượng người dùng và khối lượng giao dịch tăng đều đặn. Giới hạn cố hữu 1 megabyte cho mỗi khối cho phép khoảng 2100 giao dịch mỗi khối, và trong dung lượng sổ cái phân tán giới hạn này, một hệ thống cạnh tranh đã được giới thiệu để đảm bảo giao dịch nào trả phí cao nhất sẽ được ưu tiên xử lý trước, còn các giao dịch có phí thấp hơn sẽ được lưu trữ trong không gian bộ nhớ Mempool. Khi nhu cầu sử dụng mạng lưới tăng lên, phí giao dịch cũng được thiết kế để tăng theo.

Trong số những đề xuất có thể cải thiện đáng kể giới hạn truyền tải của Bitcoin, thì bản cập nhật SegWit sử dụng Lightning Network đã tách phần chữ ký và phần dữ liệu khi ghi lại một giao dịch trong khối, và chuyển phần chữ ký số sang Lightning Network. Đề xuất này áp dụng phương pháp kép: ghi dữ liệu giao dịch trên mạng lưới Bitcoin và chuyển phần chữ ký

sang Lightning Network. Mặc dù đề xuất SegWit đưa ra được phương pháp kép trong việc ghi nhận các khối dữ liệu và ghi chúng lên mạng Bitcoin, nhưng lúc ban đầu đã gặp phải sự phản đối từ mạng lưới các thợ đào Bitcoin cùng với các nhóm người dùng và người ủng hộ. Tuy nhiên theo thời gian, tính hiệu quả của phương pháp này đã được chứng minh, và các khối dữ liệu đã được ghi nhận thành công trên mạng Bitcoin. Đến năm 2017, khi góc nhìn về lợi nhuận trở nên rõ ràng hơn, có quan điểm cho rằng nâng cấp SegWit chỉ đơn giản là một soft fork (nhánh mềm) được chấp nhận. Điều này đồng nghĩa rằng mã nguồn gốc của Bitcoin và mã nguồn mới trong tương lai sẽ vẫn tương thích với nhau, và dữ liệu blockchain được đồng bộ hóa giữa các nút (node). Cuối cùng, bản SegWit nâng cấp đã được đưa vào mã nguồn gốc của Bitcoin, cải thiện tốc độ xử lý giao dịch của Bitcoin lên gấp đôi.

Dù có sự không tương thích giữa chương trình gốc ban đầu và phiên bản hiện tại, không ai chú ý đến vấn đề này.

Hiện tại, Bitcoin đang đối mặt với khủng hoảng. Satoshi Nakamoto đã biến mất, và chương trình gốc của Bitcoin mà ông tạo ra không còn hoạt động như ban đầu nữa.

Nếu suy xét kỹ, đây sẽ là mâu thuẫn và là mối đe dọa nghiêm trọng nhất đối với blockchain của Bitcoin – chính sự không tương thích này đã tạo nên mối nguy cho sự tồn tại của Bitcoin.

Nhóm phát triển Bitcoin đã đề xuất hai phương pháp là SegWit và SegWit2X nhằm cải thiện tốc độ truyền tải của Bitcoin và giải quyết tình trạng tồn đọng giao dịch trong Mempool. Tất nhiên, dù đã hoàn tất áp dụng SegWit vào năm 2017, các giao dịch chờ tích tụ trong vùng nhớ (memory pool) vẫn chưa được giải quyết triệt để.

Phương pháp đầu tiên, SegWit, không tăng trực tiếp dung lượng khối 1MB qua soft fork (nhánh mềm) mà tách riêng phần chữ ký và phần dữ liệu. Trong thực tế, phương pháp này có thể giúp khối chứa dữ liệu nhiều hơn, ước tính đạt 4MB. Đây là một đề xuất hoàn toàn tương thích với chương trình Bitcoin nguyên bản của Satoshi Nakamoto. Trong khi đó, SegWit2X lại nâng dung lượng khối lên 2MB, cải tiến nhiều phần và tạo ra một blockchain

hoàn toàn mới, không tương thích với chuỗi gốc - được gọi là hard fork (nhánh cứng). Hiển nhiên, hầu hết người dùng thích soft fork vì phương pháp này vẫn giữ nguyên bản sắc của blockchain do Satoshi Nakamoto tạo ra, đồng thời cải thiện tốc độ và bảo mật, sửa lỗi và đặc biệt là tăng gấp bốn lần số giao dịch mỗi giây (TPS) và giảm chi phí giao dịch. Người dùng mong đợi một bản nâng cấp hoàn hảo, hoàn toàn tương thích với chuỗi gốc. Thực tế rằng, không nhiều người biết rằng soft fork đã thất bại. (Bằng chứng cho luận điểm này được bổ sung ở Mục 5 cuối tài liệu).

Con số 21 là một 'Easter Egg' được Satoshi Nakamoto cài cắm. Tổng lượng phát hành là 21 triệu đồng Bitcoin, và sự kiện halving sẽ diễn ra sau mỗi 210.000 khối được đào. Một khối chứa được khoảng 2.100 giao dịch. Sau năm 2021, khi xảy ra thêm 21 đợt halving nữa, phần thưởng trên blockchain sẽ tiến dần về 0. Khi phần thưởng halving đạt đến phần thưởng ở đơn vị Satoshi, Bitcoin sẽ không còn bị chia nhỏ hơn nữa do quá trình halving.

Sau 80 năm nữa, Bitcoin sẽ không còn phần thưởng từ halving. Tuy nhiên, vì Bitcoin được thiết kế để có thể bù đắp cho các thợ đào thông qua tổng phí giao dịch trên mỗi khối, một phiên bản ban đầu của chương trình Bitcoin đã được xây dựng để đảm bảo mạng lưới có thể duy trì ngay cả khi không còn halving.

Vì vậy, việc thiết lập một cấu trúc phí phù hợp với nhu cầu hiện tại là điều rất quan trọng để duy trì mạng lưới Bitcoin. Nhưng cần nhớ rằng, nếu phí giao dịch bị giảm do việc áp dụng SegWit, điều này có thể khiến việc vận hành mạng lưới Bitcoin gốc không còn khả thi.

Dữ liệu từ Mempool.space cho thấy phần thưởng từ phí giao dịch khá biến động, trong đó, dao động từ 0 đến 0,3 BTC. Thậm chí có những trường hợp không thu được phần thưởng nào từ việc khai thác.

Giá trị và uy tín của Bitcoin được xây dựng dựa trên niềm tin vào tính bất biến của nó. Niềm tin này bao gồm việc chắc chắn rằng tổng cung tối đa của Bitcoin là 21 triệu BTC sẽ không bao giờ thay đổi, sự tin tưởng vào công nghệ blockchain với khả năng tạo ra một sổ cái "phi

tập trung” không thể bị giả mạo, và sự đảm bảo rằng tính phi tập trung của Bitcoin giúp mạng lưới này không thể bị kiểm soát hay loại bỏ bởi bất kỳ tác động bên ngoài nào. Chính những yếu tố này đã làm Bitcoin trở thành một trong những tài sản được đánh giá cao nhất thế giới.

Tuy nhiên, nếu trong tương lai có bất kỳ nhà phát triển nào phản bội những nguyên tắc cốt lõi này - như phát hành thêm nguồn cung vượt quá 21 triệu BTC, hoặc thay đổi các quy tắc hiện tại với lý do “cải tiến” hay “đổi mới” - giá trị của Bitcoin có thể sụp đổ theo những cách không thể đoán trước.

Hiện tại, với bản cập nhật SegWit, Bitcoin đã áp dụng một hệ thống sổ cái hai lớp, tách biệt dữ liệu và chữ ký. Và chính điều này đã làm lệch khỏi thiết kế sổ cái phi tập trung ban đầu.

Phải thừa nhận rằng đây là một dữ kiện quan trọng, làm giảm niềm tin của cộng đồng vào việc Bitcoin có thể tái hiện các đặc tính “vĩnh cửu” của vàng hay kim cương dưới dạng tài sản kỹ thuật số.

1. Giá Trị Bền Vững Của Phiên Bản Không Cập Nhật

Bitcoin Krypton là một dự án được phát triển với mục tiêu kế thừa hoàn toàn hệ thống tiền điện tử giữa các cá nhân mà không cần sự can thiệp của bên thứ ba đáng tin cậy, theo như thiết kế ban đầu của Bitcoin từ Satoshi Nakamoto.

Bitcoin Krypton được xây dựng dưới dạng chương trình tiền điện tử ngang hàng (P2P), có khả năng tiếp tục hoạt động trong tương lai mà không cần các bản cập nhật. Tuy nhiên, phiên bản gốc của Bitcoin Krypton được tạo ra bằng cách tham khảo, mô phỏng hoặc chỉnh sửa các chương trình mã nguồn mở nên không thể hoàn toàn tin cậy, mặc dù đã được kiểm tra gắt gao sau khi hoàn tất. Điều này đồng nghĩa với khả năng có thể xảy ra các lỗi hoặc vấn đề không xác định. Dù hiệu suất có thể được cải thiện, lỗi được sửa chữa và nâng cấp thông qua các quy trình tăng cường từ các nhà phát triển, nhưng phiên bản gốc của Bitcoin Krypton và các phiên bản nâng cao cần phải tương thích với nhau.

2. Sự Kiện Halving Và Chu Kỳ Của Các Khối

Tổng cung của Bitcoin là 21 triệu BTC và được thiết kế để đào một khối mỗi 10 phút. Cứ mỗi 210,000 khối được khai thác (khoảng 4 năm), phần thưởng khối Bitcoin sẽ bị giảm đi một nửa. Khi mỗi khối (block) Bitcoin được khai thác, thợ đào (miner) sẽ nhận phần thưởng là một lượng BTC nhất định, đây được gọi là phần thưởng khối. Ban đầu, phần thưởng này là 50 BTC cho mỗi khối, nhưng sau khi đạt 840.000 khối qua 4 đợt halving, chỉ còn khoảng 3.125 đồng BTC cho mỗi phần thưởng khối.

Nếu thời gian tạo khối được đặt ở mức tối thiểu để phát sóng giữa các mạng nhằm ngăn ngừa lỗi trong các bản ghi nút cho thuật toán chứng công việc, có nhiều biến số cần được xem xét. Cân nhắc thời gian chờ của Internet, v.v… vì thời gian càng dài thì càng ít lỗi xảy ra. Tuy nhiên, thời gian tối thiểu cho cho thuật toán POW không nên ngắn hơn 3 giây. Bitcoin đặt thời gian xác minh mỗi khối là 10 phút, điều này giảm khả năng xảy ra lỗi, nhưng thời gian khiến cho việc giao dịch trở nên không thuận tiện trong đời sống hàng ngày. Có nguồn ý kiến cho rằng thời gian tạo khối thoải mái nhất cho con người là dưới 1 phút cho mỗi khối, thay vì 10 phút cho mỗi khối. Dựa trên kinh nghiệm, việc gairm chu kỳ khối xuống 1 phút hoặc thậm chí 10 giây sẽ tạo ra trải nghiệm mượt mà và dễ chịu hơn cho người dùng.

Tuy nhiên, thời gian khối không cần thiết phải đặt dưới 1 giây. Một giây là đơn vị thời gian tối thiểu mà con người cảm nhận được. Blockchain với các đơn vị nhỏ hơn một giây không phải là một blockchain dành cho con người, cho dù được thực hiện, việc vận hành nó sẽ yêu cầu một chi phí khổng lồ. Nếu điều này xảy ra, việc đạt được tính ẩn danh và phân quyền của blockchain trở nên bất khả thi. Do đó, Bitcoin Krypton được thiết kế để duy trì các khối trong vòng 3 giây và cho phép bất kỳ ai sử dụng sổ cái phân tán trong một môi trường mà một nút haofn chỉnh vẫn có thể hoạt động trên một chiếc máy tính tại nhà. Nếu chu kỳ khối khoảng 3 giây, người dùng sẽ không cảm thấy chậm chạp hay không thoải mái.

Việc giảm một nửa phần thưởng khối sau mỗi bốn năm là một yếu tố quan trọng trong việc duy trì động lực cho blockchain của Bitcoin, nhưng nó cũng đồng nghĩa với những rủi ro đối với những người tham gia vào cơ chế POW. Để tham gia vào hoạt động này, người tham gia cần phải đánh giá khả năng sinh lời; nếu không có sự đảm bảo rằng việc tham gia sẽ mang lại lợi nhuận, họ sẽ không sẵn lòng tham gia. Điều này dấy lên những nghi ngại về khả năng bền vững trong tương lai của Bitcoin. Do đó, các khoản phí cao của Bitcoin đóng vai trò thiết yếu trong việc đảm bảo tính bền vững của nó. Đây là yếu tố cốt lõi trong hệ thống, khi mà nó bù đắp cho những người tham gia vào proof-of-work bằng cách đốt tổng số chi phí giao dịch Bitcoin trên mỗi khối, như đã được mô tả trong mã nguồn gốc của Bitcoin mà Satoshi Nakamoto phát triển, đồng thời thưởng cho những người tham gia dựa trên số lượng đã đốt.

Do đó, mục tiêu của SegWit là tăng cường số lượng giao dịch trên mỗi khối và giảm phí giao dịch. Tuy nhiên, việc này có thể làm lung lay độ tin cậy của Bitcoin blockchain, và những khoản phí thấp mà họ đề xuất có thể ảnh hưởng đến khả năng duy trì Bitcoin blockchain trong tương lai, dẫn đến những nghi ngại sau này.

Để giải quyết những nghi ngờ này, đảm bảo rằng Bitcoin Krypton sẽ bền vững trong tương lai và khuyến khích sự tham gia tiếp tục vào chứng minh công việc, nhiều yếu tố như chu kỳ khối, thời gian halving, và tổng phần thưởng đã được xem xét và áp dụng vào chương trình của Bitcoin Krypton.

Để thực hiện điều này, chương trình đã được thiết kế để có thể biểu diễn tới 11 chữ số thập phân (11 chữ số sau dấu phẩy), và phí chuyển nhượng đã được giảm so với phạm vi bồi thường, với mức phí được giảm xuống 1/10 sau mỗi ba lần halving. Điều này có thể được tính toán tới 1000 lần nhỏ hơn so với 8 chữ số thập phân của Bitcoin, nhưng hiệu suất dữ liệu trên mỗi khối đã được tăng cường bằng cách sử dụng kiểu dữ liệu unit64 của Bitcoin.

(Để tham khảo, 1 Satoshi tạo ra một đơn vị bổ sung là 1.000 Krypton.)

Bitcoin Krypton sẽ được nhanh chóng thử nghiệm với chu kỳ khối là 3 giây từ khối số 1 đến khối thứ 1.100.000. Sau khối 1.100.001, mã nguồn và chương trình sẽ được công bố, và chu kỳ khối sẽ là 63 giây, kéo dài đến 2.1 triệu khối. Từ khối 1 đến khối 2.1 triệu, một phần thưởng 5 đồng sẽ được trao cho mỗi khối. Sau đó, chu kỳ khối sẽ giảm 3 giây cho mỗi 2.1 triệu khối, và trong lần halving thứ 21, chu kỳ khối sẽ giảm xuống còn 3 giây.

Tổng số tiền của Bitcoin Krypton giống như 21 triệu Bitcoin riêng lẻ, nhưng Ethereum vẫn là nguyên lý cơ bản. Do đó, nó vẫn được thiết kế để tương thích với các Dapp của Ethereum.

Bitcoin Krypton sử dụng phương pháp Bitcoin hiện có, Mempool, và không áp dụng phương pháp cạnh tranh với chi phí quá cao, và dự định sử dụng phí tương ứng với trọng lượng dữ liệu theo thực tế sử dụng của mỗi giao dịch. Ngoài ra, nó được thiết kế để giảm tỷ lệ phí xuống 1/10 cho mỗi 6.3 triệu khối, và giới hạn sử dụng là 3 lần, nhưng được thiết kế để tăng thêm 100kb cho mỗi khối mỗi 21 triệu khối.

3. Tốc Độ Tăng Trưởng Dữ Liệu Và Phân Cấp Của Các Nút Blockchain

Mỗi ba năm, các nút Bitcoin sử dụng khoảng 100GB không gian lưu trữ của nút đầy đủ (full node) và cần 577GB dung lượng lưu trữ nút tính đến ngày 5 tháng 6 năm 2024.

Mặt khác, mạng chính của Ethereum (Ethereum mainnet) có dung lượng lưu trữ của nút đầy đủ là 18.195TB tính đến ngày 5 tháng 6 năm 2024, và hơn 5TB phải được bổ sung vào nút hằng năm.

Và, phiên bản cập nhật của Ethereum 2 được gọi là bản cập nhật “The Merge” vào tháng 9 năm 2022, mang ý nghĩa chuyển đổi từ cơ chế proof-of-work (POW) hiện tại sang cơ chế proof-of-stake (POS), điều này sẽ dẫn đến sự thay đổi nhanh chóng trong mạng lưới Ethereum. Mức độ sử dụng đã gia tăng.

Với phương án áp dụng bản nâng cấp Dencun của Ethereum (EIP-4844, ngày 13 tháng 3 năm 2024), tỷ lệ phí Ethereum đã giảm xuống đến 1/60, và trung bình giảm hơn 75%. Điều này sẽ giảm bớt gánh nặng tài chính cho nhiều người dùng hơn nhờ vào sự phát triển và sử

dụng hợp đồng thông minh (smart contracts) và DAPPs qua mạng lưới Ethereum. Theo đó, vấn đề lớn nhất của Ethereum là sự gia tăng dung lượng ổ cứng vật lý của nút để sử dụng. Ngoài ra, bản nâng cấp Verkle Tree đã được ứng dụng nhằm giảm bớt vấn đề này ở một mức độ nào đó và quản lý hiệu quả không gian lưu trữ dữ liệu khóa thì dung lượng lưu trữ cho dữ liệu dự kiến vẫn sẽ tiếp tục tăng.

Theo dự kiến, các nhà phát triển liên quan đến Ethereum sẽ gặp khó khăn hơn trong việc trực tiếp vận hành các nút đầy đủ, và số lượng nút sẽ không thể tránh khỏi giảm so với hiện tại. Điều này chứng tỏ rằng theo thời gian, blockchain đang gặp phải vấn đề cấu trúc, dẫn đến việc chuyển đổi từ sổ cái phân tán sang sổ cái tập trung thay vì giữ nguyên hình thức phân tán.

Trong khi đó, kích thước của Bitcoin Krypton mỗi khối bắt đầu ở mức 100kb, và dung lượng lưu trữ được sử dụng bởi một nút đầy đủ sẽ tăng dần theo thời gian. Dung lượng đĩa dự kiến sẽ được sử dụng trong một năm ước tính khoảng từ 30GB đến 50GB, và nó được thiết kế để không gặp vấn đề gì ngay cả khi dữ liệu khối tăng khoảng 5%/năm. Khi so với giá của các thiết bị lưu trữ, nó đang giảm hơn 10% mỗi GB dựa trên công nghệ hiện tại, và chi phí bảo trì đã được tính toán để đảm bảo tính bền vững trong tương lai.

4. Mục Tiêu Của Bitcoin Krypton

Mục tiêu của Bitcoin Krypton là duy trì một hệ thống bù đắp hiệu quả cho những người tham gia bằng cơ chế POW trong tương lai, hoạt động như một chương trình tài chính ngang hàng (peer-to-peer) theo đuổi tính ẩn danh hoàn toàn, không có sự can thiệp từ bên thứ ba và đảm bảo rằng các phiên bản cải tiến trong tương lai sẽ tương thích với chương trình gốc đã phát hành. Mặc dù Bitcoin Krypton 2024 được phát triển bởi một nhóm và nhà phát triển cụ thể, sau một khoảng thời gian từ khi công bố, nhiệm vụ của nhóm phát triển ban đầu và Satoshikei được chỉ định ban đầu sẽ được chấm dứt, và tất cả các quyền sẽ được chuyển giao cho một Satoshikei mới, là người thay thế ẩn danh. Việc quản lý tên miền, mã nguồn

mở, email và tài sản khai thác ban đầu đều được ủy thác, và nhóm phát triển ban đầu sẽ giải tán trước ngày 31 tháng 12 năm 2024.

Bitcoin Krypton không được bảo chứng bởi bất kỳ tài sản nào, và cũng không có kế hoạch về chiến lược phát triển, niêm yết, tầm nhìn, hoặc vận hành cộng đồng trong tương lai.

Mạng lưới Bitcoin Krypton không tồn tại chính thức hoặc thuộc về bất kỳ cá nhân hay tổ chức nào. Nếu ai đó muốn, việc niêm yết Bitcoin Krypton là hoàn toàn có thể, và bất kỳ ai cũng có thể sử dụng tên gọi này theo ý muốn. Tuy nhiên, không được tuyên bố quyền lợi nào khi sử dụng tên, cũng như không được sử dụng bất kỳ danh xưng hoặc tên gọi chính thức nào. Để đáp ứng điều kiện niêm yết, các nội dung về các chủ đề chính thức, thành viên, tổ chức và cộng đồng không nên được viết tùy ý mà không tuân thủ các tài liệu cơ bản mà các sàn giao dịch thông thường yêu cầu.

Nhà phát triển gốc của Bitcoin Krypton và những người đã tham gia vào quá trình phát triển sẽ không chịu trách nhiệm pháp lý hay kinh tế đối với bất kỳ hậu quả nào phát sinh từ Bitcoin Krypton trong tương lai.

Tuy nhiên, mọi ý tưởng, đề xuất, thảo luận về phát triển mới, xác minh và chứng nhận mã nguồn mới có thể được gửi qua email đến địa chỉ satoshi.k@bitcoinkrypton.org. Không thể đảm bảo sẽ nhận được hồi đáp, nhưng bất kỳ đề xuất nào với thái độ thân thiện và lịch sự, và không lạm dụng, hoặc gian lận sẽ được lắng nghe và xem xét. Trong một số trường hợp, việc Bitcoin Krypton bồi thường cho việc tự nguyện niêm yết trên các sàn giao dịch v.v… có thể được cân nhắc thảo luận.

5. Thử Nghiệm Của Satoshi Nakamoto Trên Mã Nguồn Bitcoin

Mã nguồn gốc Bitcoin, phiên bản Bitcoin-V0.1, dựa trên tài liệu “white paper” (bitcoin.pdf) do ông Satoshi Nakamoto viết vào ngày 1 tháng 11 năm 2008 và được công bố chính thức vào lúc 14:27 ngày 8 tháng 1 năm 2009. Phiên bản công khai chính thức được phát hành lúc 18:40 (EST), trong khi phiên bản riêng tư đã ra mắt trước đó vào ngày 16 tháng 11 năm 2008. Phiên bản mã nguồn này không được lưu trữ tại địa chỉ mã nguồn công khai hiện tại

của Bitcoin (https://github.com/bitcoin/bitcoin), mà ở một địa chỉ công khai khác (https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html).

Về SegWit, chúng tôi đã tiến hành một thí nghiệm thực tế để bác bỏ những tuyên bố sai lệch về "soft forking" được đưa ra bởi các nhóm phát triển hiện tại.

Trước tiên, khi biên dịch và chạy mã nguồn từ metzdowd.com, chúng tôi không thể tìm thấy các node mới nhất để phát tín hiệu. Điều này dẫn đến việc không thể đồng bộ hóa với các node, khiến thí nghiệm mất đi ý nghĩa. Sau khi thực thi, chỉ có thông báo lỗi "Not Connected" xuất hiện. Qua nhiều lần thử nghiệm, chúng tôi phát hiện rằng các địa chỉ phát tín hiệu để kết nối với nhiều node hiện đã ngừng hoạt động, và địa chỉ IRC dùng cho mục đích này cũng không còn tồn tại.

Kỳ lạ là tài khoản GitHub chính thức của Bitcoin chỉ lưu trữ các phiên bản 24.x là phiên bản cũ nhất và phiên bản mới nhất hiện là 27.x.

Tiếp theo đó, chúng tôi đã thử nghiệm với mã nguồn phiên bản bitcoinv0.3.

Tuy nhiên, tại khối 124,276, quá trình đồng bộ hóa các nút không thể tiếp tục và thông báo xuất ra như sau: [hiển thị thông báo lỗi]:

```
ERROR: ConnectInputs() : fb0a1d8d34 VerifySignature failed
InvalidChainFound: invalid block=000000000004939267f
height=124276  work=6613870563198902508
```

Trong phiên bản V0.4 và V0.5, việc đồng bộ hóa không thể tiếp tục tại khối 258,354 và thông báo sau được hiển thị:

```
EXCEPTION: 11DbException
Db::put: Cannot allocate memory
bitcoin in ProcessMessage()

ProcessMessage(block, 901212 bytes) FAILED
received block 0000000000000023e872
REORGANIZE
```

Phiên bản V0.6 không thể tiếp tục đồng bộ tại khối 364,670, và thông báo bên dưới xuất ra như sau:

```
EXCEPTION: 11DbException
Db::put: Cannot allocate memory
bitcoin in ProcessMessages()

ProcessMessage(block, 999787 bytes) FAILED
received block 00000000000000001d3
```

Phiên bản V0.7 cũng gặp lỗi đồng bộ hóa từ khối 364,671, và thông báo lỗi xuất ra như sau:

```
received block 0000000000000000221
ERROR: ConnectBlock() : UpdateTxIndex failed
InvalidChainFound: invalid block=0000000000000000221  height=364671
ERROR: SetBestChain() : SetBestChainInner failed
ERROR: AcceptBlock() : AddToBlockIndex failed
ERROR: ProcessBlock() : AcceptBlock FAILED
```

Nguyên nhân của tất cả các lỗi này được kết luận là do cùng một vấn đề. Khi chia khối thành phần dữ liệu và phần chữ ký, có thể nhận định rằng các nút mới nhất áp dụng SegWit và các nút cũ hơn đang xảy ra xung đột do một số nguyên nhân chưa được xác định rõ. Nói cách khác, điều này chứng minh rằng việc thực hiện soft fork đã phá vỡ giả định rằng các chương trình trước đây và hiện tại có thể tương thích với nhau một cách hiệu quả.

6. Về Krypton

Krypton là một nguyên tố hóa học độc đáo, ký hiệu Kr và có số nguyên tử 36. Được biết đến như một loại khí trơ không màu, không mùi, không vị, Krypton chỉ tồn tại với hàm lượng rất nhỏ trong khí quyển và được chiết xuất thông qua quá trình chưng cất phân đoạn không khí lỏng. Năm 1898, sau khi ông đã thành công tìm ra Elium và Argon, William Ramsay đã phát hiện ra Krypton tại Anh.

Trong hành trình tìm kiếm các khí hiếm có trọng lượng nguyên tử từ 4 đến 40, Ramsay và đồng nghiệp đã chưng cất một lượng nhỏ không khí lỏng qua đồng và magie nung đỏ, và từ đó, khám phá ra nguyên tố màu xanh bí ẩn này. Chính vì sự khó phát hiện hơn hẳn so với các khí hiếm khác, họ đã đặt tên nó là 'Krypton', theo tiếng Hy Lạp có nghĩa là “vật ẩn giấu.”

Không chỉ đơn thuần là một khí trơ, Krypton có một đặc điểm rất thú vị: khi tiếp xúc với các phân tử có năng lượng cao, nó làm giảm tốc độ chuyển động của chúng. Điều này thể hiện rõ khi hít khí Krypton, giọng nói phát ra sẽ có tần số thấp hơn nhiều so với âm cao của helium. Đặc điểm kỳ lạ này đã truyền cảm hứng cho cái tên "Kryptonite" trong các tác phẩm giả tưởng, như là điểm yếu của Superman, lấy cảm hứng từ Krypton.

Trong lĩnh vực tiền mã hóa, Bitcoin Krypton ra đời với một mục tiêu độc đáo: mang đến cơ chế khai thác an toàn và công bằng hơn. Bitcoin Krypton không chỉ hỗ trợ khai thác dựa trên CPU mà còn tích cực chống lại các phương pháp khai thác bất hợp lý như sử dụng ASIC. Với tính năng khai thác chỉ cần một cú nhấp chuột trực tiếp trên nền tảng web, bất kỳ ai cũng có thể dễ dàng tham gia vào quá trình POW, mở ra cơ hội cho mọi người trở thành một phần của mạng lưới.

Bên cạnh đó, Bitcoin Krypton đã mở rộng đơn vị tối thiểu của nó từ Satoshi (8 chữ số thập phân) thành Krypton (11 chữ số thập phân), giúp tăng tính linh hoạt và khả năng sử dụng cho các giao dịch nhỏ. Cụ thể, 1 kr (Krypton) tương đương với 0.00000000001 BTCK, và 1000kr sẽ tương đương với 1 satoshi. Như vậy, 1BTCK có thể biểu diễn thành 100 triệu

satoshi hoặc 100 tỷ Krypton, cho phép tối ưu hóa trong giao dịch vi mô và đáp ứng các nhu cầu tài chính đa dạng.

Bitcoin Krypton cũng trải qua 21 lần giảm một nửa và 7 lần giảm phí, đưa ra các mức phí thấp hơn cả đơn vị Satoshi. Để duy trì tính ổn định, đơn vị Krypton đã được tích hợp vào hệ thống, với khả năng tính toán chính xác đến 11 chữ số thập phân nhờ vào cấu trúc dữ liệu unit64. Điều này giúp kích thước khối giảm hiệu quả hơn so với sử dụng unit128, tạo ra một môi trường giao dịch tối ưu cho tương lai.

7. Hành Trình Đến Mục Tiêu Phi Tập Trung Hoàn Toàn

Bitcoin Krypton hướng đến mục tiêu cuối cùng là sự phi tập trung hoàn toàn. Điều này có nghĩa là, để đạt được trạng thái này, bất kỳ tổ chức hay thực thể nào đang quản lý Bitcoin Krypton cũng cần phải dần biến mất, nhường chỗ cho một mạng lưới tự vận hành.

Đây không chỉ là sứ mệnh, mà còn là đặc điểm làm nên sự khác biệt của Bitcoin Krypton so với các dự án khác. Hệ thống các node trong Bitcoin Krypton bắt đầu bằng cách kết nối và khám phá các Seed Node được thiết lập sẵn trong mã nguồn.

Seed Node đóng vai trò nền tảng, liên kết mạng lưới Bitcoin Krypton như một mạng lưới chặt chẽ. Để hệ thống có thể tồn tại và phát triển, các Seed Node cần được liên tục bổ sung và cập nhật. Đây là yếu tố then chốt đảm bảo sức sống và sự bền vững của mạng lưới.

Nhằm thúc đẩy sự phát triển này, Bitcoin Krypton đã thiết kế một cơ chế đặc biệt, cho phép mạng lưới lan rộng như một “virus” thông qua sự tham gia của cộng đồng. Vì bất kỳ node nào cũng có thể trở thành Seed Node, dự án cung cấp phần thưởng để khuyến khích những người chia sẻ thông tin về các Seed Node này. Cách tiếp cận này được thiết kế để đảm bảo các Seed Node ban đầu được phổ biến một cách hiệu quả.

Và phần thưởng sẽ được tính dựa trên trạng thái của Seed Node—chẳng hạn như khả năng duy trì hoạt động của máy chủ. Mỗi Seed Node sẽ được đánh giá và cho điểm, từ đó phần thưởng sẽ được phân bổ hàng tháng theo mức độ điểm số.

Khi số lượng Seed Node trong hệ thống đạt đến mức đủ lớn, Bitcoin Krypton sẽ sở hữu một mạng lưới phi tập trung ổn định. Lúc này, mạng lưới có thể tự duy trì và vận hành thông qua sự phân bổ rộng rãi và đồng đều của các Seed Node.

BITCOIN KRYPTON

https://bitcoinkrypton.org