InterValue

Kết nối, truyền tải và trao đổi tất cả các loại tài sản số trên khắp thế giới

DỰ ÁN BLOCKCHAIN 4.0 THỰC TIỄN ĐẦU TIÊN CỦA THẾ GIỚI

THẾ HỆ INTERNET GIÁ TRỊ TOÀN CẦU

CƠ SỞ HẠ TẦNG HỖ TRỢ XÂY DỰNG CÁC CHUỖI CÔNG NGHIỆP LỚN

NỀN TẢNG PHÁT TRIỂN DAPP VỚI KHẢ NĂNG MỞ RỘNG CAO

(Bản tiếng Việt được người hâm mộ cộng đồng dịch và không chính thức.)

TÀI LIỆU KỸ THUẬT

Team InterValue

Tháng 3, năm 2018

Đặc điểm kỹ thuật

Tài liệu này là Báo cáo bạch về kỹ thuật của InterValue phiên bản V4.5. Bản này sẽ chủ yếu giới thiệu tổng quan, vị trí, đặc thù kỹ thuật và các trường hợp ứng dụng InterValue. Trong tương lai, chúng tôi sẽ liên tục nâng cấp tài liệu để phù hợp thống nhất với những tiến trình công nghệ mới. Để biết thêm các thông tin mới nhất của InterValue, chẳng hạn như báo cáo bạch kỹ thuật, các bản phát hành phần mềm, cộng đồng các nhà phát triển và hơn thế nữa, xin vui lòng truy cập trang web chính thức: http://www.inve.one.

Liên hệ chúng tôi:

Về Báo cáo bạch, tại: whitepaper@inve.one

Về Quản lý cộng đồng, tại: community@inve.one

Tổ chức sáng lập, tại: foundation@inve.one

Các vấn đề khác: support@inve.one

Tuyên bố bản quyền

Miễn trừ trách nhiệm

Cùng với sự phát triển của công nghệ blockchain, nhóm InterValue sẽ cải thiện và sàng lọc những vấn đề công nghệ còn tồn tại, và bản báo cáo bạch sẽ tiếp tục được nâng cấp sửa đổi.

Nội dung

Tóm lược

Công nghệ blockchain được mệnh danh là đợt sóng công nghệ thứ năm mang đến những cải cách vượt bậc về năng suất và quan hệ sản xuất, sau động cơ hơi nước, năng lượng điện năng, công nghệ thông tin và Internet. Từ khi có sự xuất hiện của công nghệ blockchain mà tiêu biểu là Bitcoin vào năm 2009, công nghệ này đã tạo nên bước tiến bộ to lớn và ngày càng nhận được nhiều sự quan tâm chú ý. Đặc biệt là các năm gần đây, công nghệ blockchain đã thực sự trở thành tâm điểm của cả thế giới.

Đến nay người ta đã tiến hành những khám phá toàn diện dành cho blockchain, từ những công nghệ cốt lõi đến các ứng dụng chuỗi. Tuy nhiên, như những gì được biết về công nghệ blockchain hiện tại, vẫn còn có một khoảng cách lớn giữa công nghệ chuỗi và rất nhiều các ứng dụng đa dạng. Đặc biệt là về mặt công nghệ cốt lõi cũng đã có không ít vấn đề xảy ra và chúng ta rất cần một bước chuyển đột phá. Ở thời điểm hiện tại, cấu trúc hạ tầng hỗ trợ phát triển các ứng dụng blockchain còn chưa đạt đến mức ổn định, khiến cho nhiều ứng dụng trở nên không hiệu quả. Do đó, chúng ta cần gấp rút nghiên cứu và phát triển cấu trúc hạ tầng blockchain, nhờ đó cung cấp cho các ứng dụng blockchain một nền tảng hỗ trợ ổn định, khuyến khích việc quảng bá rộng rãi ứng dụng thực tiễn của blockchain trong tất cả các ngành công nghiệp, khiến cho blockchain trở thành một công cụ phục vụ con người nhanh hơn và tốt hơn.

Chúng tôi đề xuất một cơ hở hạ tầng cho toàn bộ mạng Internet Giá trị trên khắp thế giới, đó là InterValue. Mục đích của nó là giải quyết các vấn đề như khả năng ứng dụng thấp, tắc nghẽn giao dịch, chi phí cao, thời gian chờ xác nhận dài, khả năng chống đỡ rất yếu đối với các tấn công của máy tính lượng tử, tính ẩn danh trong giao tiếp và giao dịch còn kém, thiếu khả năng trong giao dịch chéo cũng như hợp nhất các chuỗi khác nhau, tốn không gian lưu trữ, vv. InterValue sẽ tối ưu hóa và cải thiện công nghệ blockchain ở hầu hết tất cả các yếu tố từ giao thức đến cơ chế, và quyết trở thành một cơ sở hạ tầng thực tiễn thực sự, blockchain 4.0. Bên cạnh đó, InterValue cũng sẽ cung cấp một nền tảng phát triển Dapp (các ứng dụng phân tán) và các giải pháp thực tế dành cho việc kiến trúc nên mạng Internet giá trị toàn cầu.

InterValue tập trung vào công nghệ cốt lõi, cơ sở hạ tầng và nền tảng blockchain. Mục tiêu của chúng tôi là xây dựng một cơ sở hạ tầng khắc phục tất cả các vấn đề kỹ thuật lớn mà hầu hết chúng ta đang gặp phải, hỗ trợ tất cả các ứng dụng miền dưới quan điểm hợp tác sinh thái. Những cải tiến công nghệ chính của InterValue bao gồm: **(1) Mạng ngang hàng,** kết hợp những ưu thế của cơ sở mạng ẩn danh Tor (mạng củ hành) và VPN phân tán trên cơ sở blockchain, chúng tôi thiết kế một mạng bao phủ ngang hàng ẩn danh hoàn toàn mới, bao gồm phương pháp tiếp cận ẩn danh và giao thức giao tiếp mã hóa, phương pháp này sẽ tăng cường tính bảo mật của các node mạng và đảm bảo rằng sẽ rất khó có thể truy ra địa chỉ nút hay phá vỡ giao thức giao tiếp trong mạng này.

(2) Cấu trúc dữ liệu, cấu trúc dữ liệu mới, HashNet xuất phát từ cấu trúc dữ liệu DAG (cấu trúc đồ thị có hướng không tuần hoàn), cấu trúc này giảm thiểu tối đa không gian lưu trữ 1 node phải có và nó cũng cải thiện được hiệu quả cũng như tính bảo mật trong lưu trữ dữ liệu.

(3) Đồng thuận, chúng tôi thiết kế nên một cơ chế đồng thuận phân lớp kép an toàn và hiệu quả kết hợp giữa đồng thuận HashNet và đồng thuận BA-VRF (đồng thuận Byzantine dựa trên hàm xác nhận ngẫu nhiên), đồng thuận này giúp đạt được hiệu quả giao dịch đồng thời rất cao, xác nhận giao dịch nhanh chóng và xây dựng các hệ thống sinh thái cho nhiều viễn cảnh ứng dụng khác nhau. Trong phiên bản 1.0, do thực tế là đồng thuận HashNet rất khó thực thi, chúng tôi đã quyết định thực thi cơ chế đồng thuận kép kết hợp giữa đồng thuận BA-VRF với đồng thuận DAG chứ không phải HashNet. **(4) Chống tấn công lượng tử**, về khía cạnh này, chúng tôi đã tạo ra những thuật toán mới có khả năng chống lại tấn công lượng tử, thay thế seri các thuật toán SHA hiện tại bằng thuật toán băm Keccack-512, và thay thế thuật toán chữ ký ECDSA bằng một thuật toán dựa trên lattice số nguyên mang tên NTRUsign. Những thuật toán này sẽ giảm thiểu những mối nguy hại đến từ sự phát triển của năng lượng tính toán lượng tử cũng như sự gia tăng số lượng các máy tính lượng tử. **(5) Tính ẩn danh cho giao dịch**, dựa vào đặc tính ẩn danh của các loại tiền mã hóa như Monero và Zcash, chúng tôi áp dụng khóa 1 lần và chữ ký vòng trong giao dịch ẩn danh và bảo vệ quyền riêng tư với tỷ lệ tối ưu hóa hiệu suất chi phí cao và khả năng bảo mật xuất sắc. Và với vai trò hàm chọn lựa, bằng chứng không kiến thức được sử dụng để thỏa mãn các yêu cầu về bảo mật trong nhiều hoàn cảnh ứng dụng khác nhau. **(6) Các hợp đồng thông minh**, chúng tôi thiết kế máy ảo Moses (MVM) để hỗ trợ thực thi hợp đồng không Turing hoàn chỉnh dạng thức khẳng định cũng như là hợp đồng Turing hoàn chỉnh nâng cao lập trình bằng ngôn ngữ Moses. MVM có khả năng tiếp cận dữ liệu off-chain (dữ liệu bên ngoài) khiến việc tiếp cận trở nên thuận tiện và an toàn, hơn nữa MVM cũng hỗ trợ phát hành các tài sản bên thứ ba, sau này có thể được tích hợp vào các ứng dụng kể cả trên blockchain phức hợp, cấp quyền (blockchain cá nhân) hay blockchain công khai. **(7) Trao đổi chéo và hợp nhất chuỗi**, chúng tôi áp dụng công nghệ chuyển tiếp chuỗi để giải quyết các vấn đề trong giao dịch chéo chuỗi và đảm bảo các thao tác minh bạch giữa môi trường đa chuỗi, đặc biệt công nghệ này không những duy trì được tính chất độc lập của thao tác hay giao dịch chéo chuỗi mà còn có thể tái sử dụng lại nhiều hàm toán riêng biệt của InterValue. **(8) Động cơ phát triển hệ sinh thái**, chúng tôi áp dụng đa dạng các phương pháp phân bổ token, hỗ trợ hoạt động đào phân lớp kép về mặt cơ chế thưởng phạt. **(9) Ứng dụng công nghiệp**, chúng tôi thiết kế rất nhiều giao diện công nghiệp dưới dạng JSON-RPC, thỏa mãn được nhiều hoàn cảnh ứng dụng khác nhau như là thanh toán xoay vòng, truyền tải dữ liệu, nghiên cứu dữ liệu và thực thi hợp đồng.

InterValue hỗ trợ thực thi tổ hợp đa dạng các ứng dụng bao gồm các giao tiếp ẩn danh, chia sẻ điện năng, chia sẻ lưu trữ, chia sẻ băng thông, chia sẻ danh tiếng (bảo đảm độ tín nhiệm), và chúng tôi cũng cung cấp những giao diện mở dành cho việc phát triển DApp. Bằng việc liên kết những hoạt cảnh ứng dụng đa dạng, InterValue có thể hợp tác với các nhà cung cấp dịch vụ và các nhà cung cấp ứng dụng, hỗ trợ các tổ chức thương mại hay các cơ quan chính phủ xây dựng

các hệ thống ứng dụng chuỗi cấp quyền, phức hợp hoặc công khai dựa theo các đặc tính kinh doanh và yêu cầu của doanh nghiệp.

InterValue sẽ tái cấu trúc lại cách thức vận hành trên Internet hiện nay. Chúng tôi tạo ra hệ thống phân bổ token dùng cho cơ chế thưởng để khuyến khích cộng đồng duy trì chuỗi công khai InterValue và khuyến khích phát triển các DApp. InterValue sẽ thúc đẩy nhiều hơn nữa những hiệu ứng lan tỏa về mạng lưới cũng như về giá trị trên chuỗi công khai, và biến hệ thống khuyến khích theo mô hình kinh tế trở thành một hệ thống tự đối mới, tạo ra một hệ sinh thái hoàn toàn phân quyền dành cho Internet giá trị và chuyển giao giá trị.

1

Tổng quan

1.1 Tổng quan về sự phát triển của Blockchain

Blockchain có thể được sử dụng như một hệ thống phân quyền ngang hàng P2P dùng để lưu trữ các bản ghi chép giao dịch giả lập trong một môi trường không tin cậy. Blockchain chính là công nghệ cốt lõi tạo nên Bitcoin, lần đầu tiên được đề xuất vào năm 2008 và được tiến hành đi vào hoạt động từ năm 2009. Blockchain về cơ bản là một sổ cái phân tán, trong đó tất cả các giao dịch đã được thỏa thuận sẽ được lưu trữ thành một chuỗi. Chuỗi này liên tục lớn dần một khi các giao dịch mới được xác nhận.

Ngày nay, có lẽ chủ đề blockchain là một chủ đề phổ biến nhất. Trước tiên, đây được xem là một kiểu tư tưởng xã hội hướng đến kỷ nguyên mới về cải cách và thay đổi xã hội loài người. Tác giả Kelly trong cuốn sách "Out of Control" mô tả: sự tiến hóa về mặt tự nhiên, xã hội và công nghệ của logic sinh học đến từ bản lề đến trung tâm sau đó lại từ trung tâm đến bản lề, từ ngoài tầm kiểm soát cho đến có thể kiểm soát rồi lại vượt ra ngoài tầm kiểm soát một lần nữa, và cứ thế. Nền tảng công nghệ của Blockchain là kiến trúc mạng phân tán, nhờ có sự phát triển chính muồi của công nghệ mạng phân tán, chúng ta có thể thiết lập nên cấu trúc kinh doanh một cách hiệu quả nhờ đi đến trung tâm, trung tâm suy yếu (weak center), trung tâm phụ (sub center) và nhờ việc chia sẻ, đồng thuận và cấu trúc tổ chức được chia sẻ.

Công nghệ Blockchain ngày nay đã trải qua một vài tiến trình: **(1) Blockchain 1.0: Tiền mã hóa.** Vào đầu năm 2019, mạng Bitcoin đã chính thức được khởi động. Một hệ thống tiền tệ ảo, toàn bộ bitcoin được xác định bằng giao thức đồng thuận mạng. Không một cá nhân hay tổ chức nào có thể tự ý thay đổi lượng cung và các ghi chép giao dịch trên đó. Công nghệ đằng sau Bitcoin, công nghệ Blockchain thực chất là một sổ cái được chia sẻ phân tán cực kỳ khéo léo và là công nghệ chuyển giao giá trị ngang hàng, công nghệ này có tiềm năng ảnh hưởng giống như sự phát minh ra đời của sổ Kế toán kép. **(2) Blockchain 2.0: Hợp đồng thông minh.** Vào khoảng năm 2014, cộng đồng công nghiệp đã bắt đầu nhận biết được tầm quan trọng của công nghệ Blockchain, và tạo ra một nền tảng công nghệ chung cung cấp cho các nhà phát triển giải pháp BaaS (Blockchain dịch vụ), cải thiện đáng kể về tốc độ giao dịch, giảm thiểu mức tiêu thụ tài nguyên và hỗ trợ nhiều thuật toán đồng thuận như là PoW, PoS, DPoS, khiến cho việc lập trình phát triển DApp trở nên dễ dàng hơn. **(3) Blockchain 3.0: Ứng dụng công nghệ Blockchain.** Sau

năm 2015, với sự nổi lên của công nghệ Blockchain 3.0 dựa trên các cấu trúc dữ liệu DAG (các dự án như là Byteball và IOTA), các hệ thống Blockchain đã trở nên hiệu quả hơn, mở rộng hơn, tính tương hỗ cao và cung cấp cho người dung những trải nghiệm tốt hơn trước. Các ứng dúng của Blockchain dần dần được mở rộng ra các lĩnh vực như ý tế, bản quyền IP, giáo dục, và IOT (Internet vạn vật). Những ứng dụng rộng lớn hơn như nền kinh tế chia sẻ, truyền thông, quản lý xã hội, từ thiện, văn hóa và giải trí. **(4) Blockchain 4.0: Hệ sinh thái Blockchain.** Thời gian gần đây, công nghệ Blockchain 4.0 dựa trên cấu trúc dữ liệu Hashgraph ngày càng thu hút được nhiều sự chú ý từ cộng đồng công nghiệp. Thuật toán đồng thuận dựa trên Hashgraph có thể đạt được trình độ phát triển chất lượng về thông lượng giao dịch và khả năng mở rộng. Blockchain sẽ trở thành cơ sở hạ tầng của công nghiệp và định hình nên hệ sinh thái vững chắc, thay đổi cách sống của con người một cách sâu sắc và mạnh mẽ.

Trong hai năm gần đây, mặc dù một số quốc gia còn bảo thủ trong việc sử dụng và phát triển các loại tiền mã hóa, các công nghệ đằng sau cũng như những ứng dụng của Blockchain vẫn nhận được rất nhiều sự chú ý

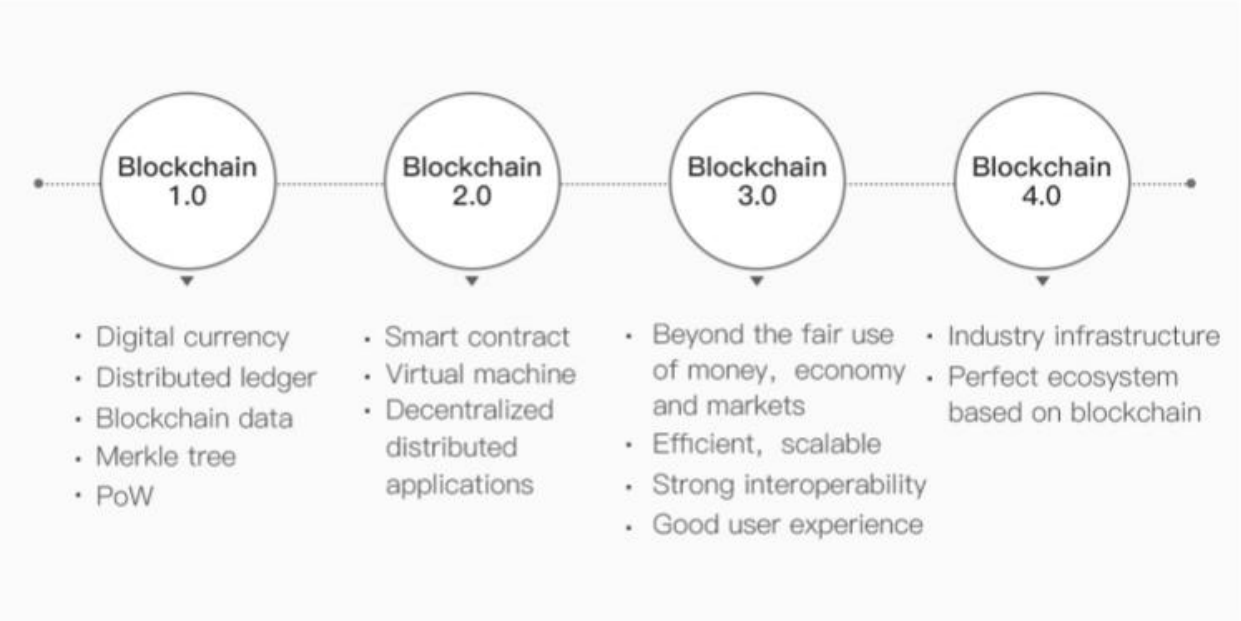


Figure 1–1: Blockchain Evolution Path

của cả thế giới. Càng tiến sâu vào nhận thức về công nghệ Blockchain và các miền ứng dụng, mọi người càng tỏ ra nhiệt huyết trong việc phát triển và triển khai các công nghệ Blockchain cốt lõi và các ứng dụng chuỗi.

Nghiên cứu và khám phá về công nghệ Blockchain chủ yếu tập trung vào 3 khía cạnh: (1) Công nghệ nền tảng và phân lớp cơ sở hạ tầng: chủ yếu bao gồm giao thức căn bản và phần cứng liên quan. (2) Ứng dụng chung và phân lớp mở rộng công nghệ: cung cấp các dịch vụ, giao diện và các exports kỹ thuật bao gồm hợp đồng thông minh, tính nhanh, dịch vụ đào, bảo mật thông tin,

dịch vụ dữ liệu, BaaS (blockchain dịch vụ), giải pháp, truy tìm chống làm giả, vv, đối với các ngành công nghiệp theo chiều dọc. (3) Lớp ứng dụng công nghiệp theo chiều dọc: Blockchain được thực thi trong các lĩnh vực theo chiều dọc như là tài chính, tiền điện tử, giải trí, chuỗi cung ứng, y tế, luật, năng lượng, phúc lợi công cộng, xã hội, Internet vạn vật và nông nghiệp. Hiện tại, người ta đầu tư rất nhiều tâm huyết vào phát triển và ứng dụng công nghệ Blockchain. Trong số những nhóm tham gia vào nghiên cứu và phát triển, thì tỷ lệ tham gia vào nghiên cứu và phát triển công nghệ ngầm định chiếm khoảng 20%, và tỷ lệ các nhóm sử dụng các chuỗi kịch bản ứng dụng và các ngành công nghiệp theo chiều dọc là 80%. So sánh với phân lớp ứng dụng thì các công nghệ ngầm định có thế tạo ra giá trị thị trường token. Thêm vào đó, nó có thể thay đổi phương thức Internet tập trung truyền thống, ví dụ như dữ liệu thường bị tập trung ở phân lớp ứng dụng. Với hệ thống Blockchain, lớp ứng dụng trở thành một nhà cung cấp dịch vụ hoàn chỉnh, không còn 1 trung khu duy nhất sở hữu lượt traffic và giá trị dữ liệu nữa. Những dữ liệu cá nhân này được phân tán tới toàn bộ người dùng, và các công nghệ ngầm định trở nên có giá trị hơn so với phân lớp ứng dụng.

1.2. Những công nghệ chủ chốt của Blockchain

Cấu trúc dữ liệu ngầm định. Blockchain lúc đầu là một phương thức lưu trữ dữ liệu trong các tiền mã hóa như là Bitcoin. Đây là một cấu trúc dữ liệu tự truy vấn dùng khi lưu trữ lượng lớn giao dịch. Các khối được liên kết theo trình tự, và sau cùng là thông tin không thể bị làm giả hay bị xáo trộn. Rất dễ dàng truy vấn các giao dịch. Cấu trúc dữ liệu blockchain truyền thống là một cấu trúc cổ chai ngăn cản quá trình tăng cường giao dịch đồng thời của blockchain. Những chuyên gia kỹ thuật liên tục tìm kiếm một dạng thức liên kết khối hiệu quả hơn. Cấu trúc sơ đồ có hướng không tuần hoàn (DAG) là một giải pháp tuyệt vời, và chúng tôi dùng "chuỗi DAG" trong suốt phần còn lại của báo cáo bạch. Trong DAG, không có quá trình gom khối, mà người dùng xác nhận giao dịch cho nhau, như vậy giảm thiểu thời gian xác nhận giao dịch đáng kể.

Thuật toán băm. Thuật toán băm thường được dùng để xử lý dữ liệu và khả năng trùng lặp rất thấp. Thuật toán này có thể giấu đi thông tin ban đầu. Những đối số hàm thể hiện dưới dạng chuỗi, kích thước output lúc nào cũng cố định, và hàm băm mang lại hiệu quả tính toán. Những thuật toán băm phổ biến gồm có chuỗi thuật toán MD5 và SHA. Tuy nhiên, thuật toán GROVER trong máy tính lượng tử có thể giảm độ phức tạp của thuật toán băm tấn công từ 0 (2^n) đến 0 (($2^{n/2}$). Do vậy thuật toán băm truyền thống bị đe dọa bởi các tấn công lượng tử.

Thuật toán chữ ký mã hóa. Thuật toán chữ ký mã hóa thông tin bằng cách sử dụng khóa riêng để đảm bảo không loại bỏ thông tin. Blockchains hiện tại chủ yếu sử dụng thuật toán chữ ký số ECDSA dựa trên các đường cong elliptic. Nó tạo ra cặp khoá công khai riêng: (sk, pk): = generateKeys (keyize). Người dùng giữ sk và pk có thể được chia sẻ với người khác. Thứ hai, người dùng có thể ký một thông điệp cụ thể với sk: Sig: = sign (sk, message). Điều này mang lại chữ ký sig. Cuối cùng, bên sở hữu pk có thể xác minh chữ ký: isValid: = verify (pk, message, sig). Tuy nhiên, thuật toán SHOR dưới máy tính lượng tử có thể làm giảm độ phức tạp của thuật toán ECDSA từ O ($2n$) đến O ($n2$ (log$n$) (loglog$n$)), do đó ECDSA không thể chống lại tấn công lượng tử.

Bảo vệ ẩn danh. Trong các chuỗi công khai, mỗi người tham gia có thể nhận được bản sao lưu dữ liệu hoàn chỉnh và tất cả dữ liệu giao dịch đều mở và minh bạch. Tuy nhiên, đây là một aw gây tử vong cho nhiều ứng dụng Blockchain. Không chỉ một số người dùng thông thường muốn bảo vệ thông tin về quyền riêng tư và giao dịch của tài khoản, mà hầu hết các tổ chức đều muốn bảo vệ thông tin tài khoản và bí mật thương mại. Bitcoin đạt được ẩn danh bằng cách chặn liên kết giữa địa chỉ giao dịch và danh tính thực sự của chủ sở hữu. Tuy nhiên, sự bảo vệ như vậy là yếu và sự tương quan giữa tài khoản và giao dịch vẫn có thể được theo dõi bằng cách quan sát và theo dõi thông tin của Blockchain thông qua địa chỉ và thông tin IP. Để đáp ứng yêu cầu bảo vệ quyền riêng tư trong Blockchain, có một số giải pháp, chẳng hạn như chữ ký vòng, mã hóa đồng cấu và bằng chứng không kiến thức.

Giao tiếp P2P. Hệ thống Blockchain sử dụng công nghệ mạng P2P để kết nối các đối tượng. Khác với chế độ mạng tập trung, mỗi nút trong mạng P2P có địa vị ngang hàng, mỗi nút có cùng quyền mạng và không có máy chủ tập trung. Tuy nhiên, do không có máy chủ tập trung, thông tin của nút có thể dễ dàng bị rò rỉ.

Cơ chế đồng thuận. Có một số loại cơ chế đồng thuận chính như: PoW, PoS, DPoS, PBFT. PoW (Proof of work) là một chiến lược đồng thuận được sử dụng trong mạng Bitcoin. Nó đòi hỏi một quá trình tính toán phức tạp trong xác thực. Trong PoW, mỗi nút trong mạng tính toán giá trị băm của phần header khối thay đổi liên tục. POW hoàn toàn phi tập trung, truy cập tự do, nhưng đào coin gây lãng phí rất nhiều tài nguyên, vì vậy đồng thuận tốn một lượng thời gian dài, không thích hợp cho các ứng dụng thương mại. PoS (Proof of stake) là một giải pháp tiết kiệm năng lượng cho PoW. Thay vì yêu cầu người dùng tìm kiếm mã nonce không giới hạn về không gian, PoS yêu cầu người dùng chứng minh quyền sở hữu số lượng tiền tệ vì người dùng có nhiều tiền hơn sẽ ít khả năng tấn công mạng và PoS vẫn phải đào. DPoS (Bằng chứng cổ phần ủy quyền). Tương tự như PoS, thợ đào được ưu tiên tạo ra các khối theo cổ phần tương ứng. Sự khác biệt lớn giữa PoS và DPoS là PoS mang tính dân chủ trực tiếp trong khi DPoS mang tính đại diện dân chủ. Và toàn bộ cơ chế đồng thuận vẫn phụ thuộc vào token, trong khi nhiều ứng dụng thương mại không cần đến token. PBFT (Dung sai lỗi Byzantine thực tế) là một thuật toán nhân bản để chịu đựng các lỗi Byzantine. Hyperledger sử dụng PBFT như là thuật toán đồng thuận của nó vì PBFT có thể xử lý tới 1/3 bản sao / nút độc hại byzantine. PBFT cần phải biết danh tính của mỗi nút để chọn ra một kế toán cho mỗi khối và các nút không thể tham gia hoặc thoát tùy ý, vì vậy PBFT luôn được sử dụng trong Blockchain tư nhân hoặc cấp quyền. Nó mang lại hiệu quả cao, nhưng yêu cầu các nút phải hoàn toàn tin tưởng lẫn nhau.

Cơ chế khuyến khích. Để đảm bảo hoạt động bình thường của hệ thống Blockchain, một số lượng lớn các nút trung thực cần phải duy trì tình trạng online. Cơ chế khuyến khích được sử dụng để thưởng cho những người dùng có đóng góp nhiều hơn cho hệ thống. Và nó sẽ có lợi cho người dùng trung thực hơn là người dùng độc hại.

Hợp đồng thông minh. Các hợp đồng thông minh được đề xuất vào năm 1994 bởi nhà khoa học mật mã Nick Szabo. Khi một điều kiện được đặt trước được thỏa mãn, các hợp đồng thông minh thực hiện các điều khoản hợp đồng tương ứng. Ethereum cung cấp một ngôn ngữ lập

trình hợp đồng hoàn chỉnh Turing, nhưng việc phát triển và triển khai các hợp đồng thông minh rất đơn điệu và dễ bị tấn công. Hợp đồng thông minh của Byteball dễ triển khai, nhưng không hoàn toàn Turing, và không thể mở rộng cho các ứng dụng hợp đồng.

1.3. Các vấn đề hiện tại của Blockchain

Hiện nay, các Blockchain khác nhau như EOS, NEO, ArcBlock và các dự án khác xuất hiện liên tục, nhưng hầu hết chúng đều dựa trên Ethereum. Họ chưa thể nào đáp ứng được các tiêu chí của Blockchain 4.0. Hầu hết các nhóm dự án thực hiện Blockchain với kịch bản ứng dụng bị giới hạn bởi hiệu suất, khả năng ứng dụng và tính ổn định của chuỗi cơ bản. Và họ hiện đang ở giai đoạn ban sơ. Mặc dù người ta ước tính rằng nhiều ứng dụng trong ngành có thể tăng lên vào năm 2018, với các khế ước liên tục thay đổi, thì hơn 98% dự án sẽ bị lịch sử cho vào dĩ vãng. Công nghệ Blockchain hiện tại chủ yếu gặp phải các vấn đề sau.

Vấn đề hiệu suất kém. Hiệu suất là một trong những thách thức chính dành cho công nghệ Blockchain hiện tại. Bitcoin được thiết kế để xử lý chỉ bảy giao dịch mỗi giây và Ethereum chỉ có thể xử lý thêm một vài giao dịch nữa. Tính đến tháng 12 năm 2017, một ứng dụng CryptoKitties đơn giản có thể làm đình trệ Ethereum và tăng phí giao dịch lên một cách đáng kể. Các ứng dụng tiêu dùng của ngày nay phải có khả năng xử lý hàng chục triệu người dùng hoạt động hàng ngày. Ngoài ra, một số ứng dụng sẽ chỉ trở nên có giá trị khi đạt được thông lượng nhất định. Bản thân nền tảng phải có khả năng xử lý một số lượng lớn người dùng đồng thời. Trải nghiệm tốt yêu cầu phản hồi đáng tin cậy chỉ trong vòng trễ thứ hai. Độ trễ dài làm người dùng thất vọng và làm cho các ứng dụng được xây dựng trên Blockchains kém cạnh tranh hơn với các lựa chọn thay thế không cần Blockchain hiện có.

Blockchain khó sử dụng. Các ứng dụng Blockchain của ngày nay được xây dựng cho một vài chuyên gia công nghệ cao cấp, chỉ những người này mới biết cách sử dụng chúng, thay vì những người dùng thông thường. Gần như tất cả các ứng dụng Blockchain yêu cầu người dùng hoặc chạy một nút Blockchain hoặc cài đặt một "nút nhẹ". Phải mất một thời gian dài để người dùng thích ứng với ứng dụng. Ví dụ, trong khi CryptoKitties trò chơi dựa trên Ethereum có lẽ là ứng dụng phân cấp thân thiện với người dùng nhất từng được xây dựng, nó vẫn yêu cầu người dùng cài đặt tiện ích mở rộng trình duyệt ví light Metamask. Người dùng cũng cần phải biết cách mua Ethers một cách an toàn và sử dụng Metamask. Để thu hút nhiều người, các ứng dụng Blockchain cần phải đơn giản như các ứng dụng Internet và di động ngày nay. Công nghệ Blockchain phải hoàn toàn minh bạch cho người tiêu dùng.

Giá thành cao. Chi phí cực kỳ cao khi sử dụng công nghệ Blockchain là rào cản lớn đối với việc áp dụng đại trà. Nó cũng hạn chế các nhà phát triển khi họ cần linh hoạt xây dựng các dịch vụ miễn phí. Cũng giống như Internet và ứng dụng dành cho thiết bị di động ngày nay, không cần phải chi trả cho mọi hoạt động trong giao dịch Blockchain. Tương tự như Internet, công nghệ Blockchain có thể hỗ trợ các ứng dụng miễn phí. Làm cho Blockchain miễn phí sử dụng là chìa khóa để áp dụng rộng rãi. Một nền tảng miễn phí cũng sẽ trao quyền cho các nhà phát triển và

doanh nghiệp tạo ra các dịch vụ mới có giá trị mà họ có thể kiếm tiền, thay vì yêu cầu người dùng trả phí sử dụng mạng Blockchain.

Bị khóa chặt trong một nền tảng. Giống như những ngày đầu của bất kỳ công nghệ máy tính nào, Blockchains có các vấn đề quan trọng "khóa chặt trong một nền tảng". Các nhà phát triển phải quyết định họ cần Blockchain nào để lập trình, sau đó triển khai code đặc trưng trong nền tảng đó, điều này khiến cho việc chuyển một ứng dụng sang một Blockchain khác trở nên rất khó khăn. Các nhà phát triển không muốn bị khóa chặt khi làm việc với một công nghệ Blockchain nhất định. Họ cần tự do đánh giá, sử dụng và chuyển đổi giữa nhiều lựa chọn. Một số ứng dụng thậm chí có thể cần chạy trên nhiều nền tảng để cung cấp trải nghiệm người dùng tốt nhất.

Khả năng ứng dụng thấp. Mọi người kỳ vọng cao vào Blockchain, các loại phương tiện truyền thông vẽ một tương lai tươi sáng hoặc các ứng dụng phi tập trung cho công chúng, đặc biệt là với mức giá ngày càng cao của tiền điện tử. Tuy nhiên, trên thực tế, công nghệ Blockchain vẫn còn trong giai đoạn sơ khai. Hầu hết các dịch vụ Blockchain đều thiếu các tính năng phong phú và không có cơ chế để khuyến khích cộng đồng cùng đóng góp.

Do đó, có một nhu cầu cấp thiết trong việc nghiên cứu cơ chế Blockchain, và thiết kế lại hoặc cải tiến các công nghệ chính của Blockchain để giải quyết các vấn đề như tắc nghẽn giao dịch, phí giao dịch cao, độ trễ hội tụ dài, khả năng chống tấn công lượng tử yếu, tính ẩn danh của giao tiếp và giao dịch còn thấp, khả năng giao dịch chéo và khả năng kết hợp chuỗi kém, cần lượng lưu trữ lớn. Chúng tôi hướng tới tiến hành một cơ chế hỗ trợ thực tiễn cho tất cả các cấp mạng chuyển giao giá trị, cung cấp cơ sở hạ tầng cho tất cả các loại ứng dụng chuyển giá trị và nền tảng phát triển cơ bản cho tất cả các loại DApps và các giải pháp thiết thực, khả thi để xây dựng hệ thống chuyển giao giá trị toàn cầu và internet giá trị.

2

Động cơ phát triển

2.1. Tên dự án
InterValue.

INVE: InterValue Token

2.2. Tầm nhìn
Chúng ta đều biết rằng Internet cho phép phổ biến và chia sẻ miễn phí một số thông tin, trong khi Blockchain giúp chuyển giao và trao đổi toàn bộ thông tin, dữ liệu thậm chí là tài sản thực một cách tự do, tạo nên mạng Internet giá trị. Tầm quan trọng của Internet và Blockchain là thiết lập và kết nối xã hội thực với xã hội ảo, ánh xạ thông tin được thực hiện trên Internet còn ánh xạ giá trị được thực hiện trên Blockchain. InterValue tập hợp các tính năng kỹ thuật và chức năng thiết lập kết nối về giá trị, trở thành cơ sở hạ tầng thực tiễn của Internet giá trị.

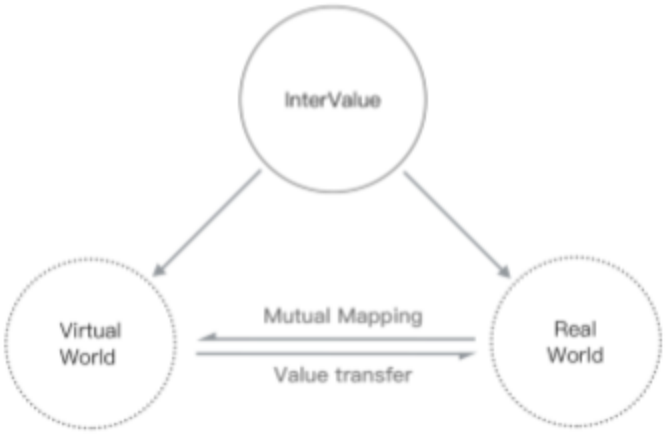


Figure 2–1: Mapping of Real World and Virtual World

Hãy tưởng tượng đến cả một thế giới bên trong InterValue, tất cả các hành vi và hoạt động của những người liên quan đến việc chi trả, định giá, thuê mướn, và chứng minh hợp pháp sẽ được vận hành hoàn toàn tự động. Mọi người có thể lưu trữ các hoạt động của cả đời mình trên các phương tiện truyền thông. Trong thế giới kỹ thuật số, một người ảo có thể được tạo ra, có ý thức hoàn toàn và hoàn toàn tự chủ, một khi trí thông minh nhân tạo phát triển. Sau khi giá trị của tất cả các loại tài sản được ánh xạ tới chuỗi, người ảo sẽ sống trong xã hội loài người độc lập. Vậy là một thế giới mới được sinh ra.

2.3. Mục tiêu

Mục tiêu của chúng tôi là xây dựng InterValue thành một cơ sở hạ tầng Blockchain 4.0 với các tính năng như là hệ thống DAG tăng cường, hỗ trợ đầy đủ chức năng, hiệu suất cao, dễ sử dụng, trải nghiệm người dùng thân thiện, khả năng mở rộng. Và sau đó chúng tôi sẽ tạo ra hệ sinh thái các ứng dụng Blockchain 4.0 trên InterValue. Các công nghệ chủ chốt trong nền tảng và các tính năng nằm trong cơ sở hạ tầng Blockchain chính là trọng tâm hàng đầu của InterValue. Các tính năng bao gồm giao thức P2P ẩn danh, thuật toán băm chống lượng tử mới, thuật toán chữ ký mới, cơ chế đồng thuận và hệ thống đào hai lớp duy nhất, phân lớp giao dịch ẩn danh, hợp đồng thông minh hoàn chỉnh Turing, vv. phân phối tài sản bên thứ ba, dữ liệu truyền thông xuyên chuỗi, chức năng hợp nhất nhiều chuỗi như chuỗi công cộng, chuỗi cấp quyền, chuỗi liên kết và các dạng khác thuộc vào hàng ứng dụng thực tế của cơ sở hạ tầng Blockchain 4.0.

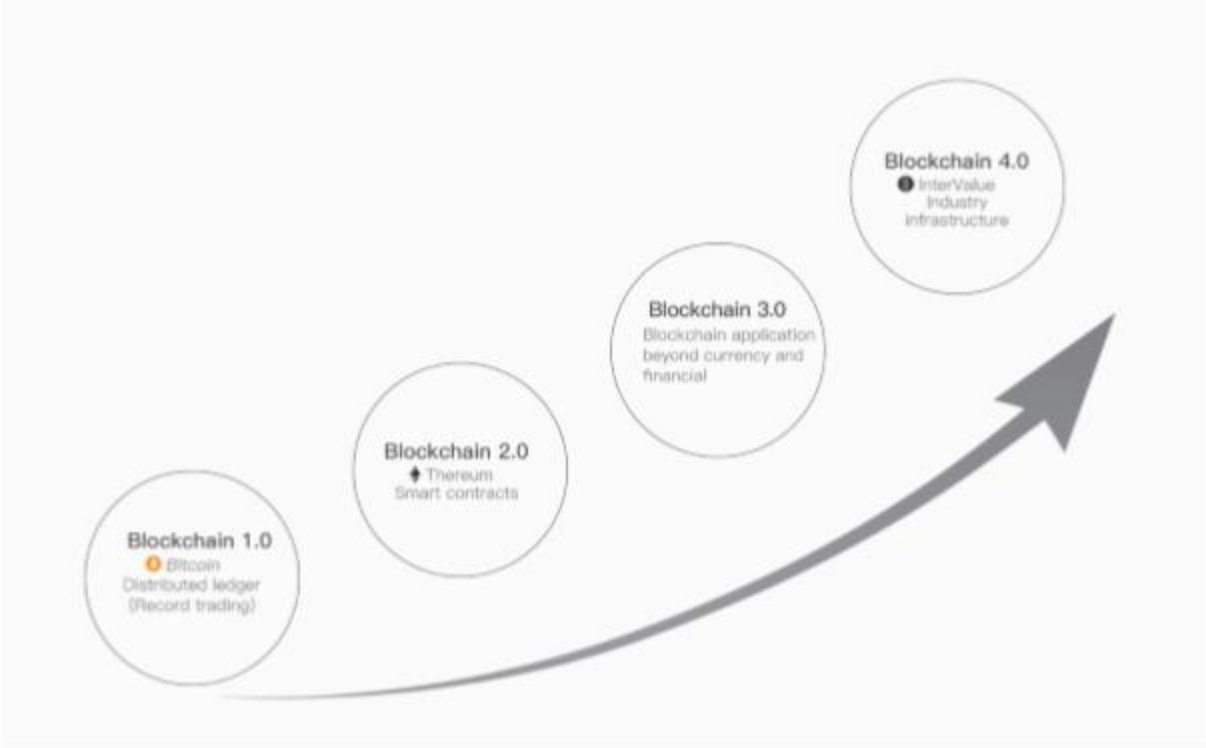


Figure 2–2: The Roadmap of Blockchain 4.0

Blockchain 1.0: Bitcoin – Sổ cái phân tán (ghi chép giao dịch)

Blockchain 2.0: Ethereum – Hợp đồng thông minh

Blockchain 3.0: Ứng dụng blockchain ngoài lĩnh vực tiền tệ và tài chính

Blockchain 4.0: InterValue – Cấu trúc hạ tầng công nghiệp

2.4. Hệ thống sinh thái

InterValue tận dụng lợi thế của Blockchain 1.0, 2.0 và 3.0, giải quyết các vấn đề nổi trội, đào sâu một số công nghệ then chốt, hỗ trợ hệ sinh thái ứng dụng thịnh vượng hơn. Như trong hình 2-3, InterValue thiết kế sáng tạo cơ chế ánh xạ dữ liệu chain-down và cấu trúc dữ liệu nâng cao mới dựa trên đồ thị tuần hoàn (DAG) và biểu đồ băm (HashNet), sự đồng thuận dựa trên HashNet và cơ chế đồng thuận Byzantine BA-VRF, một hợp đồng thông minh hoàn chỉnh Turing tiên tiến với các bộ kích hoạt bên ngoài , Keccack512 và NTRDSign Dựa trên thuật toán mã hóa chống lượng tử, chữ ký vòng và cơ chế bảo vệ ẩn danh bằng chứng không kiến thức zero-knowledge. Nó có các đặc tính chức năng của Blockchain 4.0 như giao dịch nhanh, chống lượng tử, chống tấn công lượng tử, giao tiếp ẩn danh giữa các nút, bảo vệ ẩn danh giao dịch, hợp đồng thông minh tiên tiến, liên kết dữ liệu và vân vân. Nó cũng hỗ trợ cơ chế phân phối công bằng để hỗ trợ phân phối tài sản của bên thứ ba và truyền thông liên kết chéo, đa chuỗi Fusion và các chức năng khác.

Tầm nhìn của chúng tôi đối với InterValue là xây dựng hệ thống Internet giá trị trên toàn cầu, cung cấp mạng nền tảng cho Blockchain hỗ trợ một loạt các ứng dụng dưới dạng Blockchain công cộng, Blockchain cấp quyền và Blockchains tư nhân. Đối với một ứng dụng cụ thể, dữ liệu vận hành bằng mã băm và giá trị được lưu trữ trực tiếp trên chuỗi InterValue. Tất cả các ứng dụng, như tiền tệ kỹ thuật số đại diện bởi Bitcoin trong bối cảnh Blockchain 1.0, các dịch vụ tài chính kết hợp của tiền kỹ thuật số và hợp đồng thông minh dưới nền tảng của Blockchain 2.0 và 3.0, đều có thể được xây dựng trên InterValue. Là một chuỗi công cộng, Blockchain 4.0, InterValue cũng hỗ trợ các ứng dụng rộng rãi hơn, chẳng hạn như chăm sóc sức khỏe, bản quyền IP, giáo dục, Internet of Things, kinh tế chia sẻ, truyền thông, quản lý xã hội, từ thiện, giải trí văn hóa vv.

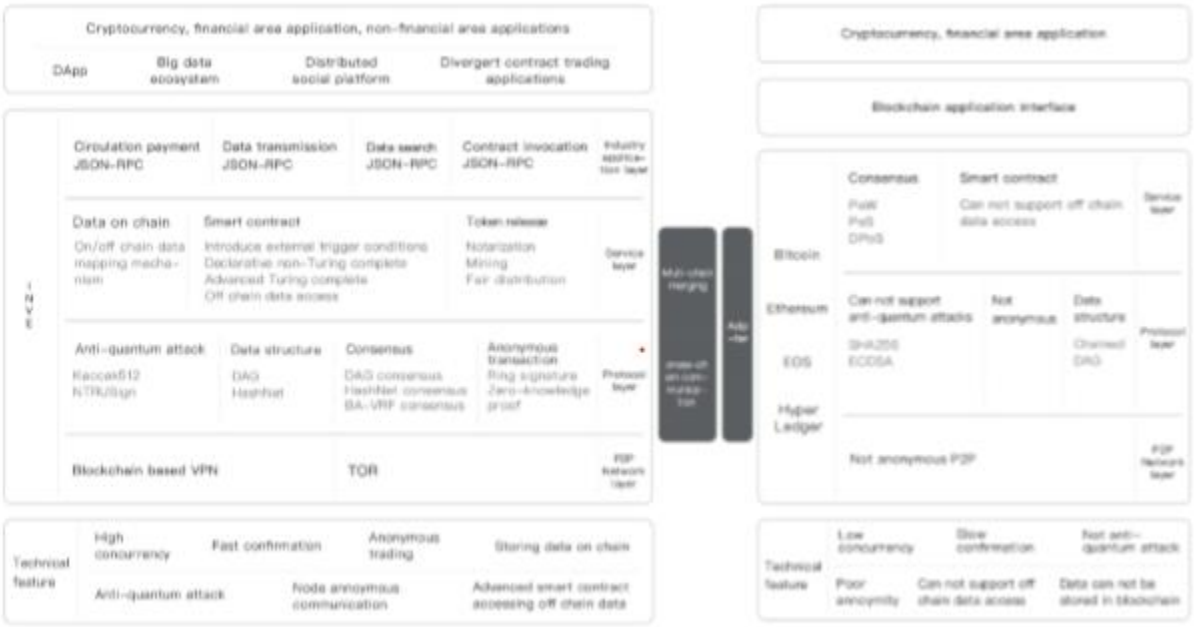


Figure 2-3: The Ecosystem Diagram of InterValue

Hình 2-3: Sơ đồ hệ sinh thái của InterValue

Giải thích:

Phía bên trái trên cùng là các lĩnh vực ứng dụng: Tiền tệ mã hóa, ứng dụng trong lĩnh vực tài chính và phi tài chính.

Tiếp theo là các phân lớp cụ thể. Lớp ứng dụng công nghiệp bao gồm: thanh toán xoay vòng ứng dụng lập trình JSON-RPC, truyền dữ liệu ứng dụng lập trình JSON-RPC, tìm kiếm dữ liệu, thiết lập hợp đồng ứng dụng lập trình JSON-RPC. Phân lớp bên dưới là phân lớp dịch vụ bao gồm: dữ liệu on-chain cơ chế tham chiếu dữ liệu on/off chain, hợp đồng thông minh: giới thiệu bộ kích ngoại biên, hợp đồng turing không hoàn chỉnh dạng thức khẳng định; phát hành token: công chứng, đào, phân bổ hợp lý. Phân lớp tiếp theo là lớp giao thức với các nhánh tính năng chống tấn công lượng tử nhờ Keccak512, NTRUSign, cấu trúc dữ liệu DAG, HashNet, đồng thuận

DAG, HashNet, BA-VRF, giao dịch ẩn danh nhờ chữ ký vòng, bằng chứng không kiến thức. Phân lớp cuối là phân lớp mạng P2P gồm blockchain dựa trên VPN, mạng củ hành TOR.

Phía dưới cùng là các đặc trưng kỹ thuật: nhiều giao dịch đồng thời, xác minh nhanh chóng, giao dịch ẩn danh, lưu trữ on chain, chống tấn công lượng tử, giao tiếp nút mạng ẩn danh, hợp đồng thông minh nâng cao tiếp cận dữ liệu off chain.

Kết nối với phía bên phải (các blockchain khác) là bộ phận hợp nhất đa chuỗi, giao tiếp chéo chuỗi, bộ điều biến khiến cho InterValue có thể đáp ứng tất cả các chức năng, ứng dụng thuộc về các blockchain thế hệ trước.

InterValue sẽ biến đổi hoàn toàn mô hình hoạt động trên Internet hiện tại và cải cách hệ thống khuyến khích kinh tế thành một hệ thống có thể lưu thông nội bộ, tạo ra một hệ sinh thái truyền dẫn giá trị phân tán hoàn toàn và hệ sinh thái cộng đồng hoàn toàn mở rộng ra ngoài ranh giới quốc gia, mỗi người tham gia đều có thể nhận được những giá trị tương ứng.

2.5. Các tính năng chính

InterValue đã có những cải tiến đáng kể trong tất cả các khía cạnh của cơ sở hạ tầng Blockchain, với những đổi mới đột phá ở một số cấp độ. Đổi mới công nghệ chính của InterValue bao gồm: **(1) Mạng P2P ngầm đinh**, kết hợp các ưu điểm ẩn danh dựa trên mạng củ hành Tor và VPN phân tán trên Blockchain, chúng tôi thiết kế lớp mạng phủ P2P ẩn danh mới, bao gồm phương thức truy cập ẩn danh và giao thức truyền thông được mã hóa, giúp tăng cường tính ẩn danh của các nút trong mạng và đảm bảo rằng rất khó để theo dõi địa chỉ nút và để crack giao thức truyền thông. **(2) Cấu trúc dữ liệu**, một cấu trúc dữ liệu mới dưới dạng HashNet có nguồn gốc từ DAG (đồ thị tuần hoàn hướng) được đề xuất, làm giảm đáng kể dung lượng lưu trữ yêu cầu cho các nút và cải thiện hiệu quả và bảo mật lưu trữ dữ liệu. **(3) Đồng thuận**, chúng tôi thiết kế một cơ chế đồng thuận hai lớp an toàn và môi trường bao gồm đồng thuận HashNet và BA-VRF (Hiệp định Byzantine dựa trên hàm ngẫu nhiên có thể xác minh), hỗ trợ tính đồng thời giao dịch cao, hội tụ nhanh và xây dựng hệ sinh thái cho nhiều môi trường kịch bản ứng dụng. Trong phiên bản 1.0, do thực tế là sự đồng thuận của HashNet khó thực hiện, chúng tôi thực hiện một cơ chế đồng thuận hai lớp kết hợp sự đồng thuận của DAG với BA-VRF. (4) Tấn công chống lượng tử, thuật toán chống lượng tử mới được tạo ra, thay thế thuật toán chuỗi SHA hiện có bằng thuật toán băm Keccak-512, và thay thế thuật toán chữ ký ECDSA bằng thuật toán chữ ký NTRUsign dựa trên số nguyên. Những thuật toán này làm giảm mối đe dọa đến từ sự phát triển của điện toán lượng tử và sự dần phổ biến của máy tính lượng tử. **(5) Ẩn danh giao dịch**, dựa trên các đặc điểm ẩn danh của tiền điện tử như Monero và ZCash, bằng chứng không kiến thức và chữ ký vòng được áp dụng cho tính ẩn danh giao dịch và bảo mật, thực hiện với hiệu quả chi phí cao và bảo mật tuyệt vời để đáp ứng các yêu cầu về quyền riêng tư trong các kịch bản ứng dụng khác nhau. **(6) Hợp đồng thông minh**, chúng tôi thiết kế máy ảo Moses (MVM) hỗ trợ hợp đồng khai báo không hoàn chỉnh cũng như hợp đồng hoàn chỉnh Turing tiên tiến được lập trình bằng ngôn ngữ Moses. MVM có thể truy cập dữ liệu on-Blockchain một cách thuận tiện và an toàn, đồng thời hỗ trợ phát hành các tài sản của bên thứ ba, có thể được tích hợp vào các ứng

dụng về công cộng, cấp quyền (tư nhân) hoặc Blockchain kết hợp. **(7) Liên kết và sáp nhập chuỗi**, chúng tôi áp dụng công nghệ chuyển tiếp chuỗi để giải quyết các vấn đề trong giao dịch chuỗi xuyên suốt và hoạt động minh bạch giữa nhiều chuỗi, không chỉ có thể duy trì hoạt động độc lập của chuỗi liên kết mà còn có thể tái sử dụng các chức năng khác nhau của InterValue. **(8) Động cơ sinh thái**, các phương thức phân bổ token khác nhau được vận dụng, hỗ trợ đào coin hai lớp phục vụ mục đích khuyến khích. **(9) Ứng dụng công nghiệp**, chúng tôi thiết kế rất nhiều giao diện phổ biến công nghiệp dưới dạng JSON-RPC, đáp ứng các kịch bản khác nhau như thanh toán lưu thông, truyền dữ liệu, tìm kiếm dữ liệu và yêu cầu hợp đồng.

Các tính năng chính của InterValue được thể hiện trong hình 2-4.

Figure 2–4: The Key Features of InterValue

Tóm lược các tính năng chính của InterValue:

• Cấu trúc dữ liệu DAG mới dựa trên HashNet với yêu cầu không gian lưu trữ nhỏ

• Nhiều cơ chế đồng thuận: Đồng thuận HashNet, BA-VRF và DAG

• Giao tiếp mạng P2P ẩn danh phân tán hoàn toàn

• Thuật toán băm và thuật toán chữ ký chống lại các cuộc tấn công lượng tử

• Ẩn danh giao dịch và bảo vệ quyền riêng tư dựa trên bằng chứng không kiến thức và chữ ký vòng

• Hỗ trợ hợp đồng thông minh khai báo Turing hoàn chỉnh nâng cao

• Hỗ trợ tính năng giao dịch đồng thời cao, thời gian giao dịch ngắn

2.6. Ưu điểm

Dự án InterValue sát nhập các lợi ích của Blockchain 3.0 hiện có bằng cách làm nổi bật những lợi ích của IOTA và Byteball. Dự án thiết kế và thực hiện một cơ chế đồng thuận mới cải thiện HashNet bằng cách giải quyết vấn đề cơ sở hạ tầng Blockchain hiện tại, áp dụng cơ chế đồng thuận hai lớp sáng tạo, thiết kế và sử dụng thuật toán mã hóa với đặc điểm tấn công chống lượng tử và xây dựng hệ sinh thái ứng dụng thịnh vượng hơn . Bảng 2-1 so sánh InterValue với các blockchain DAG hiện tại dưới khía cạnh token, vốn hóa thị trường, cơ chế đồng thuận, hợp đồng thông minh, mạng P2P, bảo mật lượng tử, bảo vệ quyền riêng tư, cơ chế thưởng, tốc độ giao dịch, phân loại nút và vân vân.

Table 2–1: Comparison with other DAG–Based Blockchain

	IOTA	ByteBall	Hedera Hashgraph	InterValue
Token	IOTA	Byte	Hashgraph	INVE
Market capitalization	14 billion	0.4 billion	-	-
Consensus mechanism	MCMC	12 notaries	Hashgraph	Double consensus
Smart contract	Nonsupport	Declarative contract	Turing complete contract	Declarative contract and Turing complete contract
P2P network	No Anonymity	No Anonymity	No Anonymity	Anonymity
Quantum security	Partial resistance	No	No	Yes
Privacy protection	No	Yes	No	Zero Knowledge Proof of Privacy Protection
Incentive mechanism	No	Transaction citations and notarization	Transaction proxy service	Transaction reference, notary, mining
Transaction speed	1000 TPS	100 TPS	-	>100000 TPS
Node cassification	Full node and light node	Full node and light node	Full node and light node	Confirm node, Full node, Local full node, Light node, Micro node

Từ tiến độ hiện tại của InterValue và kế hoạch phát triển tiếp theo, InterValue chủ yếu có những ưu điểm sau.

• Định vị dưới dạng một cơ sở hạ tầng Blockchain 4.0 thực tiễn với các tính năng kỹ thuật tiên tiến được thực sự hỗ trợ bởi sự hưởng ứng đông đảo của công nghệ Blockchain cấu trúc hạ tầng Blockbuster 3.0.

• Nhóm InterValue có sự kết hợp và phân công lao động hợp lý, khả năng nghiên cứu và phát triển công nghệ mạnh mẽ, khả năng xúc tiến thị trường và đáp cánh mạnh mẽ. Đảm bảo rằng INVE có thể đạt được các đặc điểm thiết kế khác nhau một cách thành công.

• Ứng dụng chuỗi trên InterValue đang tiến triển nhanh chóng. Hiện nay, nền tảng xã hội phân tán dựa trên InterValue và lưới lưu trữ phân phối toàn cầu dựa trên InterValue hiện đang được lên kế hoạch và phát triển. Ngoài ra, nhóm nghiên cứu vẫn đang lên kế hoạch cho một ứng dụng chuỗi có tính quyết định với một cơ sở người dùng lớn.

• Là một nhà cung cấp công nghệ, nhóm InterValue đã làm việc với nhiều công ty sử dụng công nghệ blockchain để tối ưu hóa và nâng cao các quy trình kinh doanh hiện có. Cơ sở hạ tầng InterValue đã được áp dụng cho nhiều ứng dụng và kịch bản thực tế và đang được phát triển và triển khai.

• Nhóm InterValue đang tích cực xây dựng một liên minh các đối tác để cố gắng áp dụng InterValue cho nhiều kịch bản ngành và vật lý nhất có thể.

• Nhóm InterValue đang tích cực xây dựng cộng đồng các nhà phát triển để đảm bảo rằng ngày càng có nhiều lực kỹ thuật hơn tham gia vào việc tối ưu hóa cơ sở hạ tầng của InterValue và phát triển DApp dựa trên InterValue.

• Nhóm InterValue đang tích cực xây dựng các công nghệ Blockchain để nhân rộng các cộng đồng và thúc đẩy việc phổ biến công nghệ Blockchain.

3

Giao tiếp ẩn danh trên mạng P2P

Mạng cơ bản của InterValue sử dụng kiến trúc lớp phủ P2P, cơ chế ẩn danh được xây dựng để đảm bảo tính bảo mật.

P2P là viết tắt của Peer-to-Peer, và là một loại mạng che phủ. IBM đưa ra định nghĩa như sau: “Một hệ thống P2P bao gồm một số máy tính được kết nối với nhau và có ít nhất một trong các đặc điểm sau: Hệ thống dựa trên sự hợp tác tích cực của các thiết bị máy chủ không có trung tâm, và mỗi thành viên trực tiếp hưởng lợi từ sự tham gia của các thành viên khác thay vì từ máy chủ. Mỗi thành viên không chỉ là một khách hàng, mà còn là một máy chủ. Người dùng nhận thức được sự tồn tại của nhau tạo thành một nhóm ảo hoặc nhóm thực tế. ”

Trong hệ thống P2P, mỗi peer là một người tham gia bình đẳng và đóng vai trò vừa là người tiêu dùng vừa là nhà cung cấp. Quyền sở hữu và kiểm soát tài nguyên được lan truyền trên toàn mạng. P2P giúp giao tiếp dễ dàng, đơn giản và giảm sự phụ thuộc vào các máy chủ ở mức tối thiểu. Công nghệ P2P đã thay đổi vị trí "nội dung", làm cho nó chuyển từ dạng thức "trung tâm" tỏa ra "lề cạnh". Điều này có nghĩa là nó đã thay đổi trạng thái cố hữu của Internet hiện tại đang chỉ tập trung xung quanh một trang web tập trung. Tài nguyên không được lưu trữ trên máy chủ mà được lưu trữ trên tất cả các máy tính của người dùng. Công nghệ P2P làm cho máy tính của người dùng không còn là khách hàng bị động, mà chúng trở thành các thiết bị kết hợp vài trò máy chủ và máy khách. Do vậy, InterValue được đặc trưng bởi tính phân quyền.

Cơ chế ẩn danh InterValue gắn với mạng P2P được thực thi bởi những yếu tố sau đây:

(1) InterValue chạy một máy chủ proxy cục bộ, định kỳ liên lạc với những người khác để duy trì một liên kết TLS, tạo thành một liên kết ảo trong mạng. Cụ thể, mỗi người dùng chạy proxy riêng của mình: nhận thư mục, liên kết xây dựng và xử lý kết nối. Các proxy này chấp nhận luồng dữ liệu TCP và tái sử dụng chúng trên cùng một dòng.

(2) InterValue mã hóa dữ liệu trong lớp ứng dụng, giả dụ, giao tiếp giữa mỗi nút chuyển tiếp được mã hóa bằng khóa point to point từ điểm này sang điểm kia. Mã hóa bao quát tất cả các gói dữ liệu người dùng giữa mỗi cặp nút giao tiếp, đảm bảo an toàn trong giao tiếp giữa các nút chuyển tiếp. Cụ thể, mỗi nút chuyển tiếp InterValue duy trì một khóa dài hạn và một khóa ngắn hạn. Khóa dài hạn kiểm tra khóa để ký một chứng chỉ TLS, ký tên vào bộ mô tả nút chuyển tiếp

và ký tên vào thư mục được sử dụng bởi một máy chủ thư mục. Khóa ngắn hạn được sử dụng để giải mã yêu cầu được gửi bởi người dùng và sau đó thiết lập liên kết trong khi thương lượng một khóa tạm thời. Giao thức TLS cũng sử dụng các khóa ngắn hạn giữa các nút chuyển tiếp giao tiếp để thay đổi nhất thời và độc lập ảnh hưởng của việc rò rỉ khóa.

(3) Thay vì đi theo đường trực tiếp từ nguồn đến đích, gói dữ liệu trên mạng InterValue tạo một lối tắt ngẫu nhiên thông qua một số rơle bao phủ các hệ thống truy cứu của người dùng để không có người quan sát nào tại điểm bất kỳ có thể biết được dữ liệu đến từ đâu. Để tạo một lối tắt mạng riêng tư, máy khách của người dùng sẽ xây dựng một mạch kết nối được mã hóa thông qua các rơle trên mạng. Các mạch được mở rộng một hop một lần, và mỗi đơn vị chuyển tiếp rơle trên đường đi chỉ biết rơle đã cho nó dữ liệu và rơle nào cần nó chuyển dữ liệu tới. Không có rơle riêng lẻ nào biết được đường dẫn đầy đủ mà gói dữ liệu đã thực hiện. Máy khách sẽ tạo ra một bộ khóa mã hóa riêng biệt cho mỗi hop dọc theo mạch để đảm bảo rằng mỗi hop không thể theo dõi các kết nối này khi chúng đi qua.

Nguyên tắc giao tiếp ẩn danh dành cho InterValue được thể hiện trong hình 3-1. Máy chủ thư mục là trung tâm mạng, có trách nhiệm thu thập thông tin nút chuyển tiếp và phát tán nó tới proxy dưới dạng snapshot và mô tả. Các nút chuyển tiếp tạo thành cơ sở hạ tầng trong mạng InterValue, hợp tác chuyển tiếp các gói dữ liệu được mã hóa thông qua các liên kết ẩn danh giữa nhiều nút chuyển tiếp. Proxy chạy trên ứng dụng máy khách InterValue chịu trách nhiệm thiết lập các liên kết ẩn danh và traffic mạng chuyển tiếp giữa ứng dụng của người dùng và liên kết ẩn danh. Trong hình 3-1, một liên kết ẩn danh được tạo thành bởi ba nút chuyển tiếp, được gắn nhãn là entry, middle và exit.

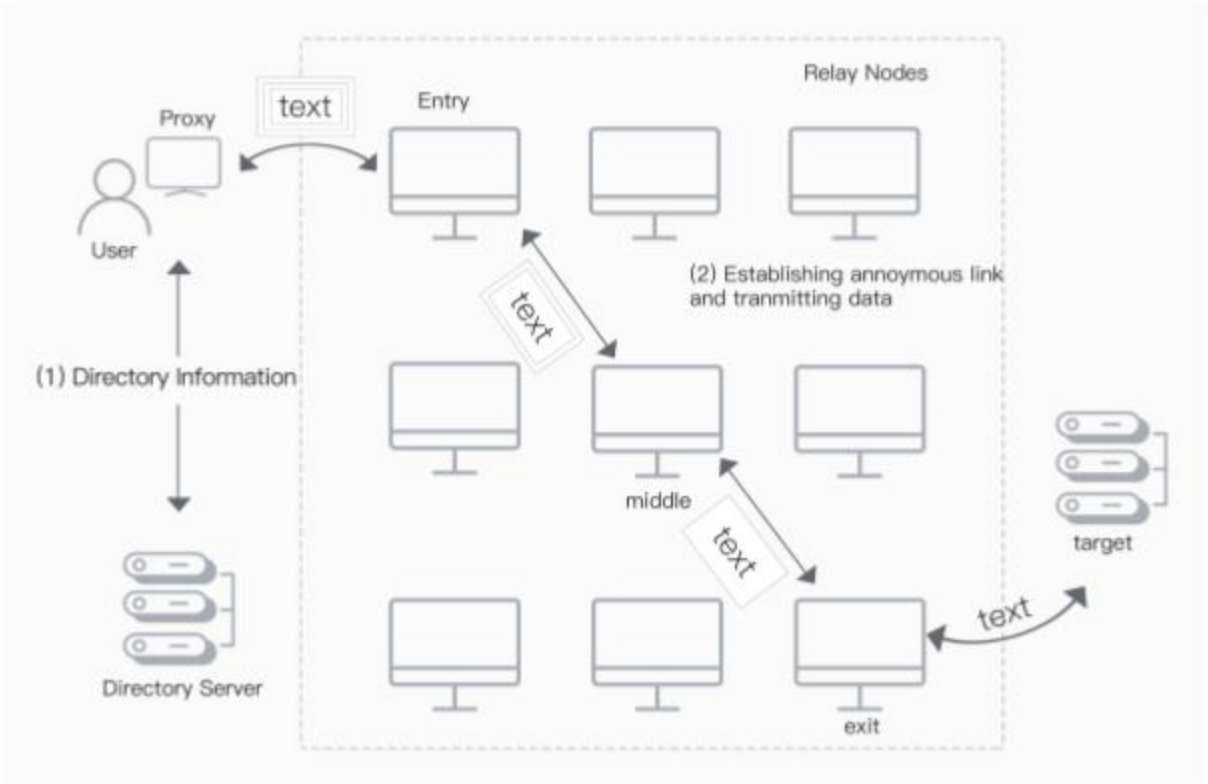


Figure 3–1: Principle of Anonymity Communication for InterValue

4

Cấu trúc dữ liệu

4.1. Cấu trúc dữ liệu của cơ bản DAG

InterValue sử dụng cấu trúc dữ liệu DAG cơ bản để lưu trữ dữ liệu giao dịch trong giai đoạn phát triển đầu tiên. Cấu trúc dữ liệu DAG cơ bản từng được áp dụng trong một số dự án (ví dụ IOTA và Byteball) để hỗ trợ hoạt động ổn định lâu dài của các blockchain công cộng, điều này chứng tỏ sự tiến bộ và hiệu suất của công nghệ chuỗi DAG. Trong InterValue, các tin nhắn giao dịch được nén thành các đơn vị (unit), và sơ đồ DAG được tạo nên bằng cách liên kết các đơn vị này. Một đơn vị phải xác nhận các đơn vị khác trước khi liên kết với các đơn vị đó. Do đó, chi phí tính toán và thời gian đồng thuận sẽ được giảm đi rất nhiều. Hệ thống này không còn các khối giao dịch nữa và cũng không có bước đồng bộ hóa dữ liệu. Kết quả là, chúng ta có thể tăng đáng kể thông lượng giao dịch và giảm thiểu thời gian xác nhận giao dịch.

Cấu trúc dữ liệu DAG của InterValue được thể hiện qua Hình 4-1. Các mũi tên ở giữa các đơn vị (A, B, C, D, vv) cho biết mối quan hệ tham chiếu của chúng. Có một mũi tên hướng từ đơn vị B đến A, thì có thể hiểu là đơn vị B đề cập đến đơn vị A (hoặc B đã xác nhận cho A), A là cha của B và B là con của A. Đồng thời, chúng ta có thể nói đơn vị C gián tiếp đề cập đến A, A là đơn vị tổ tiên của C. Đơn vị G không có bất kỳ đơn vị cha mẹ tổ tiên nào, thì được gọi là đơn vị Genesis và nó tồn tại duy nhất. Các đơn vị X và Y không có đơn vị con, các đơn vị như vậy được gọi là các đơn vị đứng top.

Mỗi đơn vị chia làm hai phần: phần tiêu đề và phần thông điệp. Tiêu đề chủ yếu chứa các trường sau:

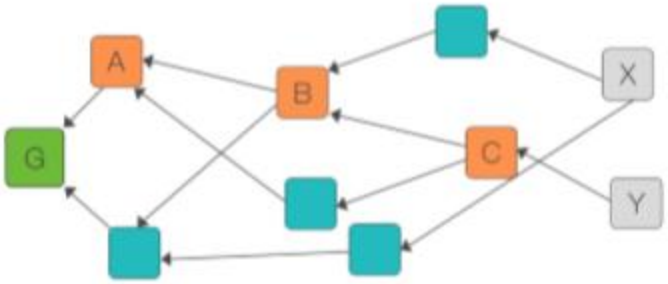


Figure 4–1: The DAG of InterValue

• Số hiệu phiên bản đơn vị;

• Tên phiên bản token;

• Chữ ký của người tạo ra đơn vị: có thể là chữ ký đơn hoặc đa chữ ký;

• Hàm băm của đơn vị gốc: giá trị băm của đơn vị được tham chiếu hoặc nhiều đơn vị gốc (như trong ví dụ giữa đơn vị A và B bên trên thì phần này là băm của đơn vị A);

• Danh sách nhân chứng

Tin nhắn đơn vị được dùng để lưu trữ thông tin giao dịch, InterValue có nhiều loại giao dịch, bao gồm thanh toán, lưu trữ dữ liệu, bỏ phiếu, vv. Mô tả chi tiết về cấu trúc dữ liệu được thể hiện trong Bảng 4-1.

Bảng 4-1: Mô tả chi tiết cấu trúc dữ liệu DAG

version	Phiên bản giao thức
alt	Kí hiệu cho biết đây là một loại tiền tệ thay thế.
message	Một mảng dữ liệu (array hay một biến đặc biệt) gồm một hoặc nhiều tin nhắn chứa dữ liệu thực tế. • app: loại tin nhắn, ví dụ: 'Thanh toán' cho các khoản thanh toán, 'văn bản' cho các tin nhắn văn bản tùy ý, v.v. • payload_location: vị trí đặt phần dữ liệu được vận chuyển của tin nhắn. Có thể là 'nội tuyến' nếu phần dữ liệu được vận chuyển được bao gồm luôn trong tin nhắn, ‘uri’ nếu phần dữ liệu được vận chuyển có sẵn tại địa chỉ Internet, ‘không’ nếu phần dữ liệu được vận chuyển chưa được xuất bản. • payload_hash: băm của phần dữ liệu được vận chuyển bằng mã hóa base64 • payload: phần dữ liệu được vận chuyển thực tế (vì nó là 'nội tuyến' trong ví dụ này). Cấu trúc phần dữ liệu được vận chuyển thì đặc trưng cho mỗi app. - input: một mảng - các coin input được tiêu thụ trong thanh toán. Tất cả

	các chủ sở hữu của token input phải nằm trong số những người ký tên (tác giả) của đơn vị. ◊unit: mã hash của đơn vị tạo ra đồng coin. Để đồng coin có thể chi tiêu được bình thường, thì last_ball_unit phải có chứa đơn vị được đề cập bên trên. ◊ message_index: một chỉ mục vào mảng tin nhắn của đơn vị input. Chỉ mục này đề cập đến phần tin nhắn nào tạo ra token. ◊ output_index: một chỉ mục cho mảng kết quả output của tin nhắn message_index của đơn vị input. Cho biết output nào tạo ra token. - output: một mảng output cho biết ai sẽ là người nhận token. ◊address: địa chỉ của người nhận. ◊amount: số tiền thẻ.
authors	Một loạt các tác giả đã tạo ra và ký vào đơn vị này.
parent_units	Một mảng băm các đơn vị cha mẹ
witness_list_unit	Mã băm của đơn vị chứa danh sách nhân chứng.

Tương tự như trong blockchain mỗi khối mới cần phải xác nhận tất cả những khối trước đó, thì mỗi đơn vị mới trong DAG cũng cần phải xác nhận đơn vị cha mẹ và tổ tiên của nó. Nếu ai đó cố tình muốn sửa đổi một đơn vị trong DAG, thì họ cần phối hợp với 1 lượng người dùng đủ lớn và càng lúc càng gia tăng, hầu hết trong số họ là những người lạ ẩn danh. Sự phức tạp trong việc phối hợp với một lượng lớn người lạ khiến cho dữ liệu trong DAG khó lòng có thể bị đảo ngược. Những người này gần như không thể đi đến một thỏa thuận, bất cứ ai trong số đó đều mang khả năng đơn phương phá bỏ hợp tác. Một khi một đơn vị được đưa ra, thì ngay lập tức quá trình xác nhận được khởi động. Và bất kì đơn vị mới nào khác cũng có thể xác nhận cho đơn vị đó. Những người dùng trong mạng sẽ giúp đỡ lẫn nhau bằng cách phát hành một đơn vị mới để nó liên kết đến các đơn vị khác.

4.2. HashNet- một cấu trúc dữ liệu DAG mới

Như trong hình 4-2, HashNet là một đồ thị tuần hoàn có hướng (DAG) bao gồm một số lượng vô hạn các đỉnh và các cạnh có hướng.

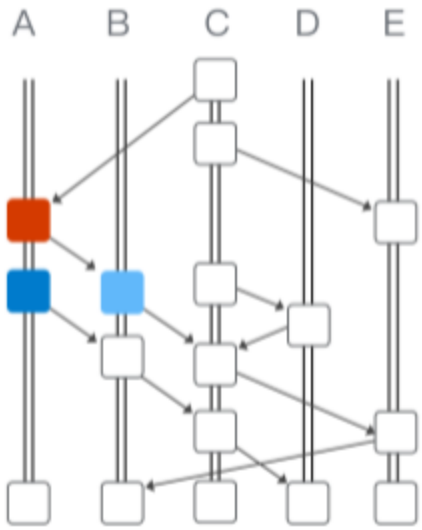


Figure 4–2: HashNet Data Structure

Hình minh họa này ghi lại lịch sử giao tiếp của các nút trong toàn bộ mạng, bao gồm cả người gửi thông tin cho ai theo thứ tự và thời gian nào. Mỗi nút có một bản sao HashNet trong bộ nhớ. Trong hình trên, có các nút A, B, C, D, và E. Mỗi nút có một cột thẳng chứa một số đỉnh (hay còn gọi là sự kiện). Đỉnh gần đây nhất được đặt ở đầu cột, vì vậy cấu trúc HashNet sẽ lớn dần cao dần lên theo thời gian.

• Các tính năng của HashNet

1. Đỉnh. Hay còn được gọi là sự kiện, bao gồm: xác nhận thời gian timestamp thiết lập, 0 hoặc nhiều hơn 0 giao dịch, chữ ký của người tạo ra và giá trị băm của đơn vị cha mẹ chính & các đơn vị cha mẹ khác.

2. Cạnh. HashNet có 2 loại cạnh, cạnh dọc và cạnh bevel.

Cạnh bevel kết nối 2 đỉnh, đỉnh nguồn và đỉnh đích, đại diện 1 quá trình đồng bộ, trong đó một nút A gửi tín hiệu đồng bộ sang B. Dữ liệu được gửi bởi A là 1 cái cây hoàn chỉnh, gốc của cây đó chính là đỉnh nguồn. • Cạnh thẳng đứng trông giống như một chuỗi, tại đó các sự kiện được đặt theo thứ tự mà chúng được tạo ra. Các sự kiện trên cùng một cạnh dọc được tạo bởi cùng một nút.

3. Mỗi nút chứa một cấu trúc HashNet trong bộ nhớ. Một đỉnh chỉ có 2 cạnh chỉ xuống dưới: một cạnh thì thẳng đứng, và một cạnh khác thì vát xuống.

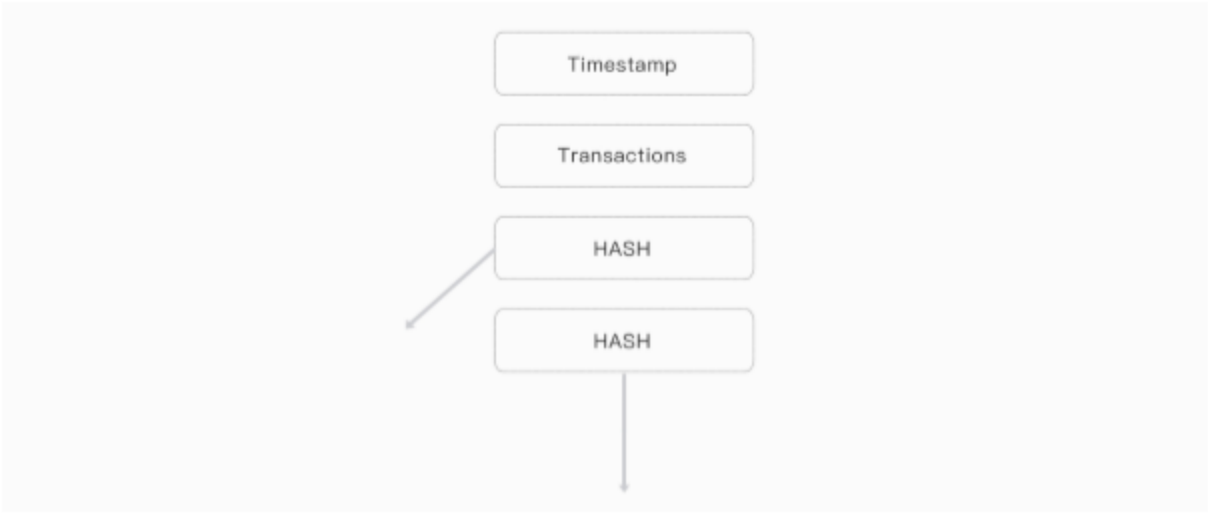


Figure 4–3: HashNet Vertex Inside

Sự kiện có màu đỏ cho biết thực tế B từng gửi một tín hiệu đồng bộ đến cho A (sự kiện xanh nhạt là đỉnh nguồn)

4. Mỗi đỉnh có một hoặc nhiều cạnh bevel hướng lên trên có nghĩa là tín hiệu đồng bộ được gửi từ chính nó đi các đỉnh khác. Ví dụ, có một cạnh bevel đi lên từ A (đỉnh nguồn là sự kiện màu đỏ) đến C. Nghĩa là dữ liệu mà A gửi tới cho C chính là tất cả các sự kiện trên 1 cây có gốc là sự kiện màu đỏ.

5. A và C sẽ thương lượng trước khi gửi đi toàn bộ cây. Trong thực tế, A chỉ gửi một phần cây mà C không có để giảm thiểu chi phí mạng.

6. Ngày càng nhiều nút gửi tín hiệu đồng bộ với nhau đến một lúc nào đó tất cả các sự kiện đã xảy ra sẽ chiếm hết cấu trúc HashNet trên mỗi nút. Đôi khi, đỉnh của HashNet trên mỗi nút có thể có sự khác biệt đi một chút, và đỉnh này sẽ sớm bị loại bỏ bởi những đồng bộ mới.

7. Nếu HashNets trên nút A và B cả hai đều chứa sự kiện x, thì đồng nghĩa là 2 HashNets phải chứa tất cả tổ tiên của x. A và B sẽ chạy thuật toán đồng thuận Byzantine cục bộ để đạt được sự đồng thuận về sự kiện x và tất cả tổ tiên của nó.

8. Mỗi nút gửi đi toàn bộ cây sự kiện mà anh ta có cho các nút khác (thực tế chỉ gửi phần cây mà người nhận không có để tối ưu hóa). Phần HashNet bị thiếu có sẽ sớm được nạp thông qua nhiều đồng bộ trên mạng.

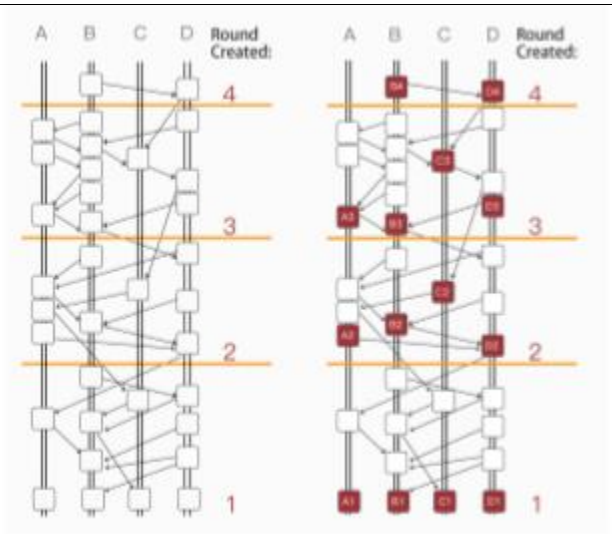
9. Vì # 6, # 7, # 8, chúng ta có thể giả định HashNets trên mỗi nút gần như giống nhau.

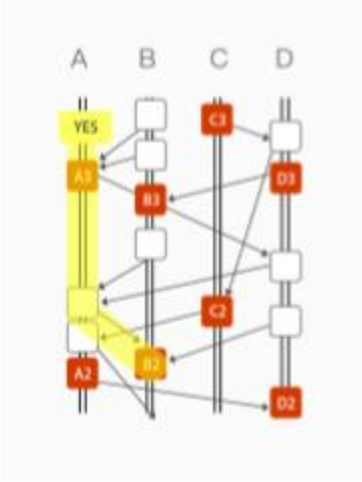
• Các thuật ngữ HashNet

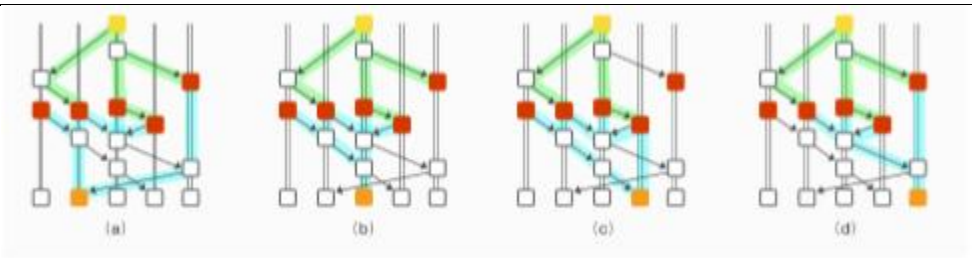
Bảng 4-2: Thuật ngữ HashNet

Thuật ngữ	Mô tả
Giao dịch	Bất kỳ nút nào cũng có thể tạo giao dịch có chữ ký tại thời điểm bất kỳ. Tất

	cả các nút đều nhận được một bản sao giao dịch và cộng đồng sẽ tạo ra thỏa thuận Byzantine về thứ tự của các giao dịch đó
Sự kiện (đỉnh HashNet)	HashNet chứa nhiều sự kiện, mỗi sự kiện chứa từ 0 giao dịch trở lên. Một sự kiện có thể được coi là một khối trong Bitcoin.
Đồng bộ (cạnh HashNet)	Cạnh vát hướng lên trên. Đại diện cho một giao tiếp mạng từ nút này sang nút khác.
HashNet	HashNet là một loại đồ thị có hướng không tuần hoàn (DAG), bao gồm nhiều đỉnh và cạnh. Biểu đồ bên dưới thể hiện lịch sử giao tiếp của nút. Trong DAG dưới đây, có 5 nút: A, B, C, D, E (Alice, Bob, Carol, Dave, Ed). Sự kiện xảy ra gần đây nhất được đặt ở trên cùng của biểu đồ, vì vậy biểu đồ HashNet sẽ gia tăng lên theo thời gian. 
World state (ws) Trạng thái toàn mạng	Trạng thái thế giới nghĩa là toàn bộ sổ cái. Trạng thái thế giới trong Bitcoin là một chuỗi, tuy nhiên trong InterValue thì trạng thái thế giới chính là một HashNet (một loại DAG)
Sự kiện self-parent (cha mẹ 1)	Sự kiện đầu tiên tạo bởi cạnh thẳng đứng hướng xuống gọi là sự kiện self-parent (sự kiện màu xanh đậm là self-parent của sự kiện màu đỏ).
Sự kiện self-ancestors (tổ tiên 1)	Sự kiện Self-parent và Self-parent của sự kiện màu xanh đậm là tất cả các sự kiện tổ tiên của sự kiện màu đỏ

Vòng khởi tạo & chỉ số vòng	 Trong HashNet, tất cả các sự kiện được sắp xếp vào từng vòng theo thời gian. Một đơn vị con không bao giờ có chỉ số vòng trước đơn vị cha mẹ của nó. Vì vậy, khi thời gian trôi qua, chỉ số vòng chỉ có thể giữ nguyên hoặc tăng lên. Mỗi vòng được quy thành một chỉ số bắt đầu từ 1. Trong vòng r, khi một sự kiện bắt đầu thấy rõ nhiều hơn số nhân chứng đa phần, thì chỉ số vòng của sự kiện sẽ tăng lên 1 vòng là r + 1
Nhân chứng	Sự kiện đầu tiên mà mỗi nút tạo ra trong mỗi vòng gọi là nhân chứng. Mỗi vòng có n nhân chứng (n số nút).
Nhân chứng nổi tiếng	Cộng đồng có thể sắp xếp một danh sách n giao dịch theo thứ tự bằng cách vận dụng các giao thức đồng thuận Byzantine riêng biệt trên $O(n\log n)$ câu hỏi dạng yes/no như là "sự kiện x đến trước sự kiện y phải không?" Một cách nhanh hơn đó là chỉ chọn một vài sự kiện (các đỉnh HashNet) làm nhân chứng, và một nhân chứng được định nghĩa là nổi tiếng nếu như cấu trúc HashNet cho thấy hầu hết các thành viên trong cộng đồng đều nhận được sự kiện đó khá sớm ngay sau khi nó được tạo ra. Sau khi thỏa thuận Byzantine chính xác đạt được trong tập hợp các nhân chứng nổi tiếng, việc sắp xếp tất cả các sự kiện trên HashNet sẽ trở nên dễ dàng
Bầu chọn	Quy trình để một nút quyết định một nhân chứng có được xem là nổi tiếng hay không
Vote	Trong quá trình bầu cử, nếu nhân chứng A trong vòng r + 1 có thể thấy nhân chứng B ở vòng r, A sẽ bầu cho B
Vòng nhận	Sự kiện x nhận được vòng r nếu đó là vòng đầu tiên và trong đó tất cả các nhân chứng nổi tiếng đều là hậu duệ của x, vòng r cũng quyết định danh tiếng của mỗi nhân chứng cho các vòng nhỏ hơn hoặc bằng r.
Thời gian nhận	Giả sử sự kiện x có một vòng nhận được là r. Alice tạo ra một nhân chứng nổi tiếng y trong vòng r. Thuật toán tìm ra z, self-ancestor (tổ tiên 1) đầu tiên của y đã từng biết về x trước đó. Để t là dấu thời gian mà Alice đặt bên trong z khi cô ta tạo ra z. Sau đó, ta coi t là thời gian mà Alice tuyên bố lần đầu tiên biết đến x. Thời gian nhận được dành cho x bằng trung bình cộng của các định mốc thời gian như trên, áp dụng đối với tất cả các bên tạo ra nhân

	chứng nổi tiếng trong vòng r.
Sự kiện other-parent (cha mẹ khác)	Sự kiện đầu tiên mà cạnh vát xuống chạm đến bắt đầu từ sự kiện màu đỏ được gọi là sự kiện other-parent của sự kiện màu đỏ
Gossip (đồn tin)	Mỗi nút gửi tất cả thông tin mà nó biết đến một nút ngẫu nhiên khác. Sau đó, nút nhận được tin nhắn tiếp tục làm điều tương tự tới các nút khác.
Gossip about gossip (đồn tin về tin đồn)	HashNet được lan truyền thông qua giao thức tin đồn. Thông tin bị đồn thổi là lịch sử của chính tin đồn đó, vì vậy ta gọi đó là "đồn tin về tin đồn).
Virtual voting (bỏ phiếu ảo)	Mỗi nút có một bản sao HashNet, do đó dựa vào các giao thức Byzantine truyền thống, Alice có thể tìm ra phiếu mà Bob sẽ gửi cho cô ta. Vì vậy, Bob không cần gửi phiếu bầu thực sự trên mạng. Mỗi nút đều có cùng một dữ liệu (HashNet), cùng kết quả được tính toán bằng cùng một thuật toán (BFT) mà không cần đến giao tiếp mạng. Do vậy, lượng tiêu thụ băng thông mạng cho thuật toán đồng thuận HashNet là rất thấp.
Supermajority (đại đa số)	Nếu m> 2n / 3 (n là số nút trong mạng), m được gọi là supermajority hay đại đa số
Nhìn thấy	Nếu sự kiện x có thể trực tiếp hoặc gián tiếp tiếp cận sự kiện y theo một đường dẫn xuống thì ta nói: • x có thể thấy y • y là tổ tiên khác other-ancestor của x • x là hậu duệ của y  A3 là x, B2 là y trong đồ thị trên
Nhìn thấy rất mạnh	Nếu x có thể nhìn thấy y bằng số đường nhiều hơn số đường hướng xuống xuất phát từ supermajority, chúng ta có thể nói x thấy y rất mạnh:

	 Trong đồ thị (d), sự kiện w màu vàng ở trên đầu có thể thấy được sự kiện x màu da cam, vì w có thể thấy x thông qua 4 đường đi xuống mỗi đường xuyên qua 1 sự kiện màu đỏ khác nhau.

5

Đồng thuận

Trong phiên bản v1.0, InterValue sử dụng cơ chế đồng thuận hai lớp kép kết hợp giữa đồng thuận DAG cơ bản với đồng thuận BA-VRF. Từ phiên bản v2.0 trở đi, đồng thuận DAG cơ bản của InterValue sẽ được thay thế bởi đồng thuận HashNet. Do đó, cơ chế đồng thuận của InterValue sẽ là sự kết hợp giữa HashNet và BA-VRF

5.1. Đồng thuận DAG

5.1.1. Chuỗi chính

Chuỗi chính là một chuỗi được xây dựng dựa theo liên kết giữa các đơn vị con-cha mẹ, và kết nối tất cả các đơn vị với nhau. Chuỗi chính có thể được tạo thành từ bất kỳ đơn vị nào. Nếu chúng ta chọn hai chuỗi chính từ hai đơn vị khác nhau với cùng một quy tắc, cả hai chuỗi chính sẽ hoàn toàn trùng khớp sau khi chúng giao nhau. Phần trùng khớp được gọi là chuỗi chính ổn định. Trường hợp xấu nhất, các chuỗi chỉ giao nhau tại đơn vị Genesis. Tất cả các đơn vị đều nằm trong chuỗi chính ổn định này hoặc có thể chạm tới được trong một vài bước tính từ một đơn vị nào đó trong chuỗi chính ổn định. Do đó, chuỗi chính ổn định có thể thiết lập một trật tự tổng hòa giữa hai đơn vị không có trật tự. Đầu tiên, hãy tạo chỉ số cho các đơn vị trực tiếp trên chuỗi chính ổn định. Chỉ số của đơn vị Genesis được đặt là 0, chỉ số của đơn vị con của đơn vị Genesis được đặt là 1, v.v. Thứ hai, nếu một đơn vị không nằm trong chuỗi chính ổn định, chúng ta sử dụng chỉ số của đơn vị đầu tiên nằm trong chuỗi chính ổn định và trực tiếp hoặc gián tiếp đề cập đến đơn vị này. Vì vậy, mỗi đơn vị được chỉ định một chỉ số chuỗi chính (MCI). Các đơn vị có MCIs nhỏ hơn có nghĩa là chúng được tạo trước. Nếu hai đơn vị có chính xác cùng một chỉ số MCI, đơn vị nào có giá trị băm nhỏ hơn là đơn vị hợp lệ.

Quá trình xây dựng chuỗi chính được gọi là quá trình đệ quy, thuật toán lựa chọn ra đơn vị cha mẹ tốt nhất. Chúng ta có thể tìm ra đơn vị cha mẹ tốt nhất của một đơn vị cụ thể bằng cách so sánh số lượng đơn vị chứng kiến trên đường thay thế. Nhân chứng có thể là những người không giấu mặt, tham gia cộng đồng lâu, hoặc có danh tiếng tốt, hoặc góp sức duy trì sự phát triển của mạng lưới. Do chúng ta mong đợi nhưng không hề tin tưởng vào việc tất cả các nhân chứng đều sẽ trung thực nên cùng lúc phải chọn ra nhiều nhân chứng.

5.1.2. Giao dịch lặp chi:
Giao dịch lặp chi: bất kỳ giao dịch hỏng/ hết hạn nào được phát hành dưới cùng 1 địa chỉ thì sẽ được coi là giao dịch lặp chi, ngay cả khi chúng không cùng output. Các giao dịch lặp chi cũng được gọi là giao dịch xung đột hoặc giao dịch mâu thuẫn.

Khi người dùng phát hành một đơn vị mới, đơn vị này phải trực tiếp hoặc gián tiếp xác nhận tất cả các đơn vị được phát hành trên cùng một địa chỉ. Do đó, tất cả các đơn vị có cùng địa chỉ thì đều phải được kết nối.

Khi tất cả các đơn vị có cùng một địa chỉ được kết nối, thì trong các giao dịch lặp chi, giao dịch nào xuất hiện trước trên đường dẫn thì giao dịch nó là giao dịch hợp lệ. Nếu 1 kẻ tấn công cố ý tạo ra một giao dịch lặp chi, chúng ta có thể giải quyết bằng chỉ số MCI: giao dịch với chỉ số MCI nhỏ hơn là giao dịch hợp lệ. Giả sử kẻ tấn công tạo ra một chuỗi giả và tạo ra một giao dịch lặp chi trên đó. Khi chuỗi giả liên kết với DAG thực, dựa trên chiến lược lựa chọn cha mẹ tốt nhất thì số lượng nhân chứng trong chuỗi giả đó sẽ là rất nhỏ. Do đó, chuỗi giả sẽ không phải là một phần của chuỗi chính, và vấn đề lặp chi trong trường hợp này đã được giải quyết. Lưu ý rằng, nếu hầu hết các nhân chứng đều cấu kết với kẻ tấn công và phát hành các đơn vị trên chuỗi giả kia thì kẻ tấn công đó đã tấn công thành công.

5.1.3. Tính dứt điểm giao dịch
Khi các đơn vị mới được thêm vào, mỗi người dùng theo dõi MC hiện tại của mình, MC này được xây dựng như thể anh ta sẽ phát hành một đơn vị mới dựa trên tất cả các đơn vị không có đơn vị con hiện tại. Các MC hiện tại có thể khác nhau tại các nút khác nhau bởi vì chúng có thể nhìn thấy những tập hợp các đơn vị không có con khác nhau. MC hiện tại sẽ liên tục thay đổi khi các đơn vị mới đến. Tuy nhiên, phần cũ của MC hiện tại sẽ không thay đổi.

Trong tương lai, tất cả MC sẽ va chạm với nhau tại một đơn vị ổn định. Đơn vị Genesis là một đơn vị ổn định tự nhiên. Giả sử rằng chúng ta đã xây dựng một MC hiện tại dựa trên các đơn vị không ổn định, và có một số đơn vị ổn định trên MC này. Nếu chúng ta có thể tìm một phương pháp để đẩy đơn vị ổn định cách xa đơn vị Genesis, sự tồn tại của đơn vị ổn định có thể được chứng minh bằng cảm ứng hoàn toàn. Các đơn vị do đơn vị ổn định giới thiệu được xác nhận MCI. Bên cạnh đó, các thông điệp trong các đơn vị này được xác nhận.

5.2. Đồng thuận của HashNet

5.2.1. Tổng quan về HashNet
Thuật toán đồng thuận HashGraph hiện có đạt được đồng thuận trong chuỗi giao dịch thông qua mạng tin đồn và chiến lược bỏ phiếu ảo. Điều kiện tiên quyết để đạt được đồng thuận này là khả năng bỏ phiếu của nút mạng, trên $2n$ / 3 kết quả phiếu bầu biểu quyết nhất trí cho ‘sự kiện nhân chứng nổi tiếng’, trong đó n là tổng số phiếu bầu, và thường được đại diện bởi số lượng token. Nhờ có các chiến lược bỏ phiếu địa phương, HashGraph đạt được tốc độ giao dịch nhanh chóng. Tuy nhiên, phương pháp này có các vấn đề sau:

(1) Trong môi trường mạng diện rộng, tính ổn định thấp và tính biến động trong khả năng biểu quyết n của toàn bộ mạng cũng tăng lên. Điều này có thể dẫn đến trong một thời gian dài hệ thống không thể tìm ra một sự kiện đáp ứng đồng thuận bỏ phiếu 2/3, và do đó không thể đạt được đồng thuận.

(2) Do các yếu tố như độ ổn định nút, công suất xử lý và băng thông, khả năng các nút khác nhau đáp ứng yêu cầu xử lý các sự kiện cũng theo đó mà biến động đáng kể. Nếu có một số lượng lớn các nút yếu như vậy tham gia bỏ phiếu trong hệ thống thì trong một thời gian dài đồng thuận có thể sẽ không đạt được.

(3) Trong môi trường mạng diện rộng, các biến động nút thường xuyên có thể làm cho mạng toàn cầu bị chia thành nhiều mạng con. Theo giao thức lan truyền tin đồn, một nút theo định kỳ sẽ loại bỏ những hàng xóm chưa được cập nhật trong một thời gian dài. Khi danh sách các nút xung quanh ổn định, nút đó đạt được đồng thuận trong mạng con. Nếu kích thước mạng con nhỏ, nút độc hại có thể dễ dàng tạo ra hai sự kiện nhân chứng nổi tiếng trong cùng một vòng, dẫn đến một giao dịch lặp chi.

(4) Khi quy mô hệ thống tăng lên, mỗi nút phải xử lý một số lượng lớn các gói tin đồn. Do đó, tốc độ truyền của hệ thống sẽ giảm khi số lượng nút tăng lên.

Để chấm dứt những tình trạng trên, chúng tôi đề xuất ra cơ chế đồng thuận HashNet. Như trong hình 5-1, HashNet sử dụng một cấu trúc liên kết hai tầng dựa trên sự đồng thuận của HashGraph. Ở tầng cao, mỗi nút được gọi là nút đầy đủ và các nút đầy đủ này chịu trách nhiệm về tính nhất quán của giao dịch. Để duy trì sự ổn định mạng, tất cả các nút đầy đủ được bầu chọn thông qua cơ chế DPOS. Mỗi nút đầy đủ nhận hai loại dữ liệu từ mạng cơ bản: dữ liệu giao dịch và dữ liệu giao dịch mạng con chéo. Ở tầng dưới, mỗi nút được gọi là các nút đầy đủ cục bộ và chịu trách nhiệm duy trì tính nhất quán của giao dịch intrasubnet. Khác với nút đầy đủ, quá trình bầu chọn nút đầy đủ cục bộ dựa trên các yếu tố như số lượng token, dung lượng xử lý, băng thông và thời lượng trực tuyến. Nút đầy đủ cục bộ đạt được đồng thuận của các giao dịch mạng con thông qua HashGraph.

Những lợi thế chính của HashNet nằm ở hai điểm sau:

(1) Nút đầy đủ và nút đầy đủ cục bộ có khả năng xử lý và ổn định mạnh, chúng có thể tránh được vấn đề mà HashGraph gặp phải đó là không thể đạt được đồng thuận trong thời gian dài. Trong khi đó, các nút đầy đủ này cũng có thể tránh được sự cố khiến toàn bộ mạng bị chia cắt thành nhiều mạng con.

(2) Vì chúng tôi sử dụng cấu trúc liên kết hai lớp để phân chia các loại nút, mỗi nút cục bộ chỉ cần đồng bộ hóa các giao dịch trong mạng con của riêng nó, đảm bảo hệ thống có thể mở rộng ở quy mô lớn.

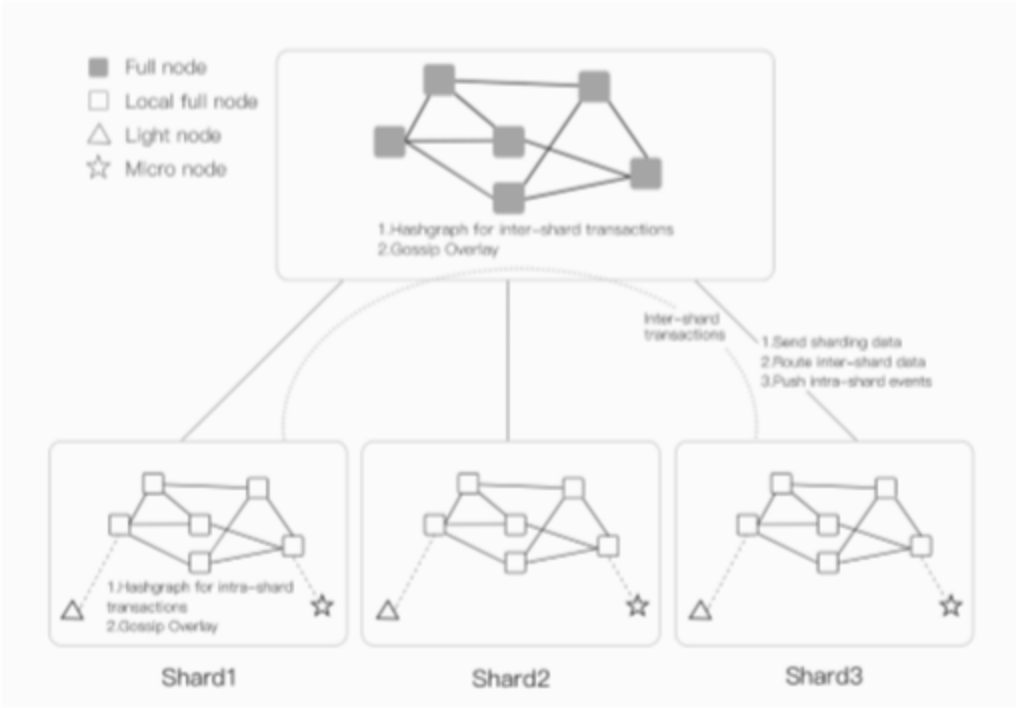


Figure 5-1: HashNet Overview Based on Two-layer Gossip Topology

5.2.2. Phân loại nút

Các nút HashNet được chia thành bốn loại: các nút đầy đủ, các nút đầy đủ cục bộ, các nút nhẹ và các nút vi mô.

• Các nút đầy đủ: chịu trách nhiệm duy trì toàn bộ dữ liệu giao dịch mạng và đảm bảo tính nhất quán của toàn bộ chuỗi giao dịch mạng.

• Nút cục bộ đầy đủ: chịu trách nhiệm duy trì dữ liệu giao dịch mạng con và đảm bảo tính nhất quán trong chuỗi giao dịch mạng con.

• Nút nhẹ: Thông thường, nó là một ví khách nhẹ. Nó đưa ra yêu cầu hoặc là gửi dữ liệu thông qua một nút cục bộ đầy đủ.

• Nút Micro: Nó thường là thiết bị Internet of Things (IoT) thông minh. Tương tự như nút ánh sáng, nó yêu cầu hoặc gửi dữ liệu thông qua một nút cục bộ đầy đủ.

5.2.3. Duy trì nút mạng

Trong HashNet, sự ổn định và sức mạnh xử lý của nút đầy đủ và nút đầy đủ cục bộ sẽ giúp cải thiện tốc độ truyền tải giao dịch. Để đạt được mục tiêu này, chúng tôi đã thiết kế một số cơ chế đáng tin cậy và có động lực để khiến cho các nút tự động tham gia và cập nhật.

(1) Duy trì nút đầy đủ

1) Gia nhập hệ thống nút đầy đủ dựa vào cơ chế DPoS

Bởi vì toàn bộ nút cần duy trì dữ liệu của toàn bộ mạng, sự ổn định của chúng là vô cùng quan trọng. Với mục đích này, chúng tôi thiết lập tổng cộng 36 nút đầy đủ. Quá trình chọn các nút đầy đủ được thể hiện như sau: a) Nền tảng INVE đưa ra các yêu cầu tối thiểu để trở thành một nút đầy đủ. b) Người tham gia gửi thông tin cấu hình nút đến nền tảng INVE. c) Đối với nút được phê duyệt, tất cả những người nắm giữ token trên toàn mạng sẽ bỏ phiếu cho những người nộp đơn mà họ tin tưởng; d) Theo kết quả bình bầu DPOS, nền tảng INVE chọn ra 36 ứng viên hàng đầu trở thành các nút đầy đủ và xây dựng cấu trúc phân lớp cao cấp của HashNet.

2) Quá trình cập nhật nút đầy đủ dựa vào điểm danh tiếng

Thông thường, tất cả các nút đầy đủ đều ở trực tuyến 100%. Tuy nhiên, có hai rủi ro bảo mật tiềm ẩn khi lượng nút đầy đủ được cố định. Một là các nút đầy đủ có thể âm mưu cấu kết với nhau và tấn công đồng thuận HashNet. Hai là không thể tránh khỏi những hành vi bất thường của các nút đầy đủ, chẳng hạn như lỗi phần mềm, tắc nghẽn mạng hoặc các cuộc tấn công nguy hiểm.

Để chấm dứt tình trạng trên, mỗi nút đầy đủ có một thang đánh giá điểm danh tiếng năng động dựa trên sự ổn định và khả năng nguy hại của nó. Trong mỗi vòng, sáu nút có giá trị danh tiếng thấp nhất bị thay thế bằng lượt ứng viên DPOS hàng đầu mới.

(2) Duy trì nút đầy đủ cục bộ

1) Đánh giá nút đầy đủ cục bộ dựa trên điểm trọng lượng

So với nút đầy đủ thì số lượng nút đầy đủ cục bộ lớn hơn rất nhiều và các nút này sẽ được đánh giá định kỳ. Để tiến hành, chúng tôi sử dụng kết hợp các cơ chế PoS + PoW + PoB + PoO để tự động xác định danh tiếng, khả năng xử lý, khả năng băng thông và tính ổn định của ứng viên. Cụ thể, PoS là bằng chứng về cổ phần, tức là, ứng viên giao nộp bằng chứng về số lượng token cho một nút đầy đủ. PoW là bằng chứng của công việc, tức là, ứng viên ngẫu nhiên nhận được một bài toán băm với một mức khó khăn cụ thể từ 1 nút đầy đủ. Nút đầy đủ ghi lại thời gian tính toán của nó để đánh giá khả năng xử lý. PoB là bằng chứng về băng thông, trong đó nút đầy đủ gửi các gói dữ liệu back-to-back để đo băng thông của ứng viên. PoO là bằng chứng về thời lượng trực tuyến, nơi ứng viên gửi thời lượng trực tuyến dài nhất của mình đến nút đầy đủ. Cuối cùng, tổng hợp điểm của mỗi ứng viên là:

$$\text{Điểm số} = \alpha\text{PoS} + \alpha\text{PoW} + \alpha\text{PoB} + \alpha\text{PoO}\ldots$$

Trong đó α là tỷ trọng tương ứng. Theo xếp hạng điểm số, các ứng viên có điểm số top-N được chọn làm các nút đầy đủ cục bộ.

2) Cập nhật toàn bộ nút cục bộ dựa trên sharding

Nút đầy đủ cục bộ theo định kỳ sẽ cập nhật tổng điểm của nó cho nút đầy đủ. Khi một vòng ứng tuyển mới bắt đầu, nút đầy đủ cục bộ hiện tại và ứng viên mới sẽ cạnh tranh nhau vào vòng tiếp theo. Sau đó, nút đầy đủ có nhiệm vụ phân vùng các nút đầy đủ cục bộ thành nhiều mạng con thông qua quá trình sharding.

5.2.4. Sharding

Sau khi nút đầy đủ đã vượt qua tất cả các ứng viên cục bộ cho vòng tiếp theo, cần phải phân vùng các ứng viên này thành nhiều shard để đảm bảo khả năng mở rộng của hệ thống.

(1) Số lượng shard

Số lượng shard là một biến cần được tính toán cẩn thận. Nếu con số đó quá nhỏ, tỷ lệ thông lượng giao dịch của hệ thống không thể được cải thiện một cách trực tiếp. Nếu con số đó đủ lớn, khả năng mạng con bị tấn công bởi 1/3 nút độc hại tăng lên đáng kể và các nút đầy đủ phải xử lý một số lượng lớn các giao dịch qua mạng con. Để khắc phục vấn đề này, chúng tôi thiết lập số lượng tối thiểu của các nút trong mỗi subnet là 1000. Trong trường hợp cực đoan, số lượng shard là 1, nếu tổng số nút cục bộ nhỏ hơn 1000.

(2) Chi tiết về Sharding

Để phân vùng tất cả các nút đầy đủ cục bộ, lớp mạng trên cùng chọn ngẫu nhiên một nút đầy đủ bằng cách sử dụng giao thức tin đồn. Đặc biệt, lớp mạng trên cùng lưu trữ một token ảo. Nút đầy đủ giữ token ảo này được gọi là nút đầy đủ chịu trách nhiệm, chịu trách nhiệm về hoạt động sharding. Để chọn nút đầy đủ có trách nhiệm, mỗi nút đầy đủ sẽ tạo ra một số ngẫu nhiên. Thông qua giao thức trao đổi tin đồn, nút tạo ra số ngẫu nhiên trung bình được chọn là nút đầy đủ chịu trách nhiệm cho sharding trong vòng tiếp theo. Nút đầy đủ chịu trách nhiệm xác định số lượng shard dựa trên kích thước sharding tối thiểu và phân chia ngẫu nhiên tất cả các nút đầy đủ cục bộ vào mỗi mạng con. Mỗi mạng con có một id subnet_id nhận dạng duy nhất và ID nút tương ứng trong mạng con được bắt đầu bằng subnet_id mạng con của nó. Giả sử rằng có bốn mạng con trong mạng và các id mạng phụ của chúng tương ứng là 00, 01, 10 và 11. Nếu có bốn nút đầy đủ cục bộ trong mạng con 00, id nút tương ứng là 0000,0001,0010,0011. Thông qua định tuyến prefix, mỗi nút có thể lấy id mạng con của nút khác. Sau đó, nút đầy đủ chịu trách nhiệm phân bổ danh sách hàng xóm ban đầu cho mỗi nút đầy đủ cục bộ. Do đó, các nút đầy đủ cục bộ sẽ tự động xây dựng mạng con dựa trên danh sách lân cận của chúng.

(3) Xác nhận giao dịch

Các giao dịch được nhóm thành bốn trường hợp sau:

Trường hợp 1: input (1) → output (1), input và output đều thuộc về shard 1;

Trường hợp 2: input (1) → output (2) + output (3), input thuộc sharding 1, và hai output lại thuộc shard 2 và 3 tương ứng.

Trường hợp 3: input (1) + input (2) → output (3), hai input thuộc shard 1 và 2 tương ứng, và output thuộc shard 3.

Trường hợp 4: input (1) + input (2) → output (3) + output (4), hai input thuộc về shard 1 và 2 tương ứng, và hai output thuộc về shard 3 và 4 tương ứng.

Trong trường hợp 1, vì input và output đều thuộc cùng một shard, giao dịch chỉ cần đạt được đồng thuận HashGraph, và giao dịch đó sẽ được thực hiện ngay lập tức.

Trong trường hợp 2, vì input và output thuộc về các shard khác nhau, giao dịch cần đạt được đồng thuận HashGraph trong nhiều shard. Ví dụ, Alice trong shard 1 gửi 2 INVE và 3 INVE tới Bob trong shard 2 và Lily trong shard 3 tương ứng. Đầu tiên, một giao dịch được tạo ra trong shard 1, trừ đi 5 INVE từ tài khoản của Alice và tạo một biên nhận có chữ ký của Alice. Sử dụng HashGraph, shard 1 xác nhận biên lai và gửi biên lai đến nút đầy đủ. Sau đó, nút đầy đủ top level tạo ra hai giao dịch: một là thêm 2 INVE vào tài khoản của Bob và một là thêm 3 INVE vào tài khoản của Lily. Các giao dịch này được gửi đến shard 2 và 3 tương ứng, cùng với biên nhận trước đó có chữ ký của Alice. Tiếp theo, cả hai thông báo về giao dịch 2 và 3 mà giao dịch nhận được của họ là hợp pháp và biên lai không được sử dụng. Do đó, tài khoản của Bob và Lily tăng 2 INVE và 3 INVE tương ứng. Để đảm bảo tính nguyên tử của các giao dịch, shard 2 và 3 cần gửi toàn bộ một nút thông báo rằng biên lai đã được sử dụng. Sau đó, nút đầy đủ chuyển tiếp tin nhắn đến shard 1. Giả sử rằng đoạn 2 và 3 không thể hoàn tất giao dịch do tắc nghẽn mạng hoặc các lý do khác. Sau khi hết thời gian chờ, nó gửi đi thông báo giao dịch 1 rằng biên lai không được sử dụng và vui lòng thêm 5 INVE vào Alice. Do đó, giao dịch được thực hiện bởi slice 1.

Các input trong trường hợp 3 và 4 đến từ các shard khác nhau, vì vậy chúng ta cần phải có được xác nhận của nhiều shard để tiếp tục giao dịch. Chúng tôi giới thiệu các thao tác “khóa” và “mở” để đảm bảo tính hoán đổi nguyên tử của giao dịch. Ví dụ, Alice trong shard 1 và Bob trong shard 2 cùng trả 5 INVE cho Lily trong shard 3, trong đó Alice trả 2 INVE và Bob trả 3 INVE. Giả sử rằng thông tin giao dịch được tạo bởi shard 1. Bước 1, thông tin giao dịch đạt được đồng thuận trong shard 1 thông qua HashGraph và hai INVE trong tài khoản Alice bị khóa. một chứng nhận hợp lệ có chữ ký của Alice được tạo ra và được gửi đến nút đầy đủ toplevel. Bước 2, nút đầy đủ cấp cao nhất định tuyến thông tin giao dịch đến shard 2. Nếu có đủ số dư trong tài khoản của Bob, 3 INVE bị khóa. Tương tự như vậy, một chứng nhận hợp lệ được ký bởi Bob được tạo ra và được gửi đến nút đầy đủ cấp cao nhất. Bước 3, khi nút đầy đủ cấp cao nhất nhận được xác nhận hợp lệ của Alice và Bob, nó sẽ gửi hai giao dịch đến shard 1 và 2 tương ứng: một là trừ 2 INVE khỏi tài khoản của Alice, và cách khác là trừ 3 INVE khỏi Bob tài khoản. Bước 4, sau khi nút đầy đủ nhận được các biên nhận từ cả hai shard 1 và 3, nó sẽ gửi đến 3 giao dịch mới để thêm 5 INVE vào Lily. Bước 5, giao dịch mới được ghi lại và biên lai không được tiêu thụ. Do đó, 5 INVE được thêm vào tài khoản của Lily thành công. Có một số trường hợp bất thường. Ví dụ: Bob không có đủ số dư hoặc 5 INVE không thể được thêm vào tài khoản của Lily do lỗi mạng. Để đảm bảo tính nguyên tử của giao dịch, nút đầy đủ cấp cao nhất sẽ gửi thông báo rollback đến shard 1 và 2 nếu xảy ra trường hợp bất thường.

(4) Trật tự sự kiện tổng thể

Về lý thuyết, chiến lược sharding nói trên đã có thể đạt được đồng thuận của các giao dịch nội mạng con và giao dịch qua mạng con. Tuy nhiên, rất khó có thể sắp xếp tất cả các sự kiện theo thứ tự vì nút đầy đủ cục bộ cần chuyển đổi định kỳ. Để chấm dứt điều này, chúng tôi sử dụng nút đầy đủ cấp cao nhất để đạt được trật tự tổng thể của tất cả các sự kiện. Ý tưởng cơ bản là nút đầy đủ cục bộ định kỳ gửi các giao dịch đã xác nhận của nó đến cho các nút đầy đủ cấp cao nhất theo thứ tự. Vì vậy, các nút đầy đủ sử dụng các bản ghi giao dịch qua mạng con để đạt được sự đồng thuận của toàn bộ mạng. Cụ thể, mỗi shard phân loại thông tin giao dịch được xác nhận của nó theo thuật toán đồng thuận HashGraph. Mỗi shard chọn một nút đầy đủ ngẫu nhiên trên cùng một lớp định kỳ. Các giao dịch được xác nhận bởi các nút đầy đủ cục bộ nhưng không phải các nút đầy đủ được gửi đến nút đầy đủ đã chọn. Sau đó, nút đầy đủ sử dụng giao thức tin đồn để phân phối sự kiện trong cấu trúc liên kết lớp trên cùng. Vì nút đầy đủ ghi lại thứ tự các giao dịch mạng con chéo, chúng ta có thể nhận được tổng số lệnh giao dịch cho tất cả các shard. Giả sử rằng hệ thống chứa ba shard. các sự kiện đã xác nhận được sắp xếp theo từng shard. Như trong Hình 5-2, các nút trắng đại diện cho các giao dịch nội mạng con. Các nút màu xanh dương, đỏ và cam thể hiện giao dịch crosssubnet và các dòng cho biết thứ tự giao dịch qua mạng con. Tức là, b2 xảy ra trước e1, d1 xảy ra trước c2, và b3 xảy ra trước d2. Chúng tôi sử dụng phương pháp sắp xếp từ dưới lên. Ý tưởng cơ bản là đi qua các sự kiện của từng shard lần lượt, bỏ qua shard nơi sự kiện có sự kiện phụ thuộc và không được khắc phục. Trong Hình 5-2, chúng ta đi ngang qua đoạn 1, từ a1 đến e1. Vì e1 phụ thuộc vào b2 và b2 chưa được duyệt qua nên chúng tôi chuyển sang shard 2. Sự kiện a2 và b2 trong shard 2 không phụ thuộc vào các sự kiện khác. Sự kiện c2 phụ thuộc vào sự kiện d1 đã được duyệt qua. Sự kiện d2 phụ thuộc vào b3 chưa được duyệt qua. Do đó, nó chuyển sang shard 3. Tất cả các sự kiện trong shard 3 không có sự kiện phụ thuộc. Tiếp theo, nó chuyển sang shard 1 để thu được e1 và chuyển sang shard 2 để thu được d2 và e2. Cuối cùng, tổng số thứ tự của tất cả các sự kiện là: a1, b1, c1, d1, a2, b2, c2, a3, b3, c3, d3, e3, e1, d2, e2.

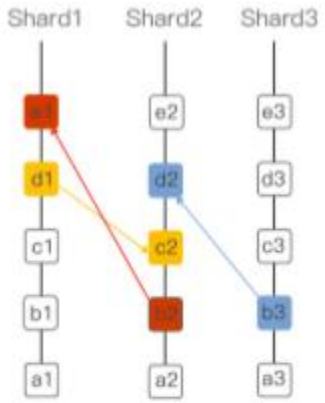


Figure 5–2: Event Total Order in the Full Nodes

Giả sử rằng tổng số nút đầy đủ cục bộ là N và tổng số trong mỗi shard là N_0. Vì vậy, số lượng phân đoạn là $C = \frac{N}{\mathbb{N}_0}$. Giả sử rằng các giao dịch trên mỗi giây (TPS) của mỗi mạng con là α, và TPS giữa hai mạng con là β. Do đó, tổng TPS của HashNet là:

$$f(C) = \frac{2\alpha + \beta}{2C} + \frac{\beta(C^2 - C - 1)}{2}$$

Chứng minh: Tỷ lệ giao dịch xảy ra trong mạng con bên trong là $p = \frac{N_0(N_0-1)}{N(N-1)} \approx \frac{1}{c^2}$. Tương ứng, tỷ lệ giao dịch xảy ra trong các mạng con phụ là 1 − p. Do đó, tổng TPS của mạng con bên trong là:

$$f^1(C) = C * p * \alpha = \frac{\alpha}{C}$$

Tổng TPS của các mạng con phụ là:

$$f^2(C) = \frac{C(C-1)}{2} * (1-p) * \beta$$

Chúng ta có tổng TPS của HashNet:

$$f\,(C) = \; f^1(C) + f^2(C) = \frac{2\alpha+\beta}{2C} + \frac{\beta(C^2-C-1)}{2}$$

Từ công thức trên, đạo hàm bậc hai của $f\,(C)$ lớn hơn 0. Cho biết $f\,(C)$ có giá trị nhỏ nhất. Với sự tăng trưởng của C, $f^1(C)$ giảm và $f^2(C)$ tăng dần. Do đó, lượng TPS của HashNet tăng theo tăng trưởng của C.

5.3. Hiệp định Byzantine dựa trên hàm ngẫu nhiên có thể kiểm chứng

BA-VRF là một cơ chế đồng thuận dựa trên thuật toán ngẫu nhiên có thể xác minh (VRF) và thuật toán Byzantine (BA), nó chọn ngẫu nhiên một số lượng nhỏ các nút đầy đủ. của các nút chứng nhận. BA-VRF được thực thi mỗi một phút. Mỗi khi đạt được sự đồng thuận, một số nút đầy đủ sẽ được chọn làm nút chứng nhận ngẫu nhiên. các nút chứng nhận có thẩm quyền gửi các đơn vị tham dự phải tuân theo quy tắc tham chiếu lẫn nhau giữa đơn vị cha mẹ và con của DAG. Một khi đơn vị chứng nhận được gửi bởi nút chứng nhận ổn định trên MC, nút chứng nhận sẽ nhận được phần thưởng xác nhận. Khi giao dịch được kích hoạt và các đơn vị mới được tạo liên tục, các nút chứng nhận sẽ nhận được phần thưởng xác nhận của họ kịp thời. Giả sử rằng các giao dịch ít hoạt động hơn hoặc không có đơn vị mới nào được tạo trong cửa sổ thời gian một phút cuối cùng. Trong những trường hợp này, nút chứng nhận sẽ nhận được phần thưởng của nó sau khi đơn vị chứng nhận trở thành đơn vị MC ổn định. Trong khi đó, những nút không gửi đơn vị chứng nhận sẽ không nhận được phần thưởng xác nhận.

5.3.1. Trạng thái đồng thuận

BA-VRF có hai loại trạng thái đồng thuận: thỏa thuận đồng thuận và dự kiến. Khi một nút đầy đủ đạt được đồng thuận cuối cùng, điều đó có nghĩa là các nút đầy đủ khác cũng đạt được đồng thuận cuối cùng, hoặc các nút đầy đủ trong cùng một vòng phải tán thành trên cùng một kết quả đồng thuận (đồng thuận dự kiến), bất kể giả thiết đồng bộ hóa mạnh. Đồng thuận dự kiến có nghĩa là một số nút đầy đủ có thể đã đạt được đồng thuận dự kiến trên các đơn vị chứng nhận khác, và không có nút đầy đủ nào được đồng thuận cuối cùng. Tất cả các đơn vị tham dự phải trực tiếp hoặc gián tiếp hướng đến các đơn vị chứng nhận đã được tạo ra trước đó, đảm bảo trạng thái an ninh của BA-VRF. Có 2 trường hợp BA-VRF cuối cùng sẽ đạt được đồng thuận dự kiến. Trường hợp 1, giả sử mạng được đồng bộ mạnh mẽ. Với một xác suất nhỏ, kẻ tấn công có thể khiến BA-VRF đạt được đồng thuận dự kiến. Do đó, BA-VRF sẽ không đạt được đồng thuận cuối cùng và sẽ không xác nhận rằng mạng có đồng bộ hóa mạnh mẽ. Nhưng sau một vài vòng, có khả năng là đồng thuận cuối cùng sẽ được xác lập.

Trường hợp 2, giả sử rằng mạng được đồng bộ yếu. Kẻ tấn công thâu tóm được toàn bộ mạng lưới, BA-VRF có thể đạt được đồng thuận dự kiến và chọn các bộ nút chứng nhận khác nhau, nhiều nhánh đồng thuận được hình thành. Điều này sẽ ngăn BA-VRF đạt được đồng thuận cuối cùng, bởi vì các nút đầy đủ được chia thành các nhóm khác nhau và các nhóm này không thỏa hiệp với nhau. Để trở lại trạng thái hoạt động bình thường, BA-VRF sẽ được tiến hành định kỳ cho đến khi bất đồng được giải quyết. Khi mạng trở về trạng thái đồng bộ hóa mạnh, đồng thuận cuối cùng sẽ được xác lập trong một thời gian ngắn.

5.3.2. Chọn nút đầy đủ

Thuật toán xổ số được xây dựng trên cơ sở một hàm ngẫu nhiên có thể xác minh (VRF) chọn một tập con ngẫu nhiên của các nút này dựa trên trọng số của mỗi nút đầy đủ tham gia vào đồng thuận BA-VRF. Xác suất của một nút đầy đủ được chọn tương đương với tỷ lệ của trọng số riêng của nó đối với tổng trọng số. Sự ngẫu nhiên của xổ số đến từ VRF và một lần gieo ngẫu nhiên có thể kiểm chứng công khai. Mỗi nút đầy đủ có thể xác minh cho dù nó được chọn bằng cách sử dụng biện pháp gieo (seed) ngẫu nhiên.

Định nghĩa VRF: Cho một chuỗi tùy ý, VRF đưa ra giá trị băm và kết quả của bằng chứng.

$$(hash, \pi) \leftarrow VRF_{s_k}(seed \| role)$$

Giá trị băm $hash$ được xác định duy nhất bằng khóa riêng tư sk và chuỗi đã cho ($seed\ role$), $hash$ không thể phân biệt được với số ngẫu nhiên nếu không biết được khóa sk. Kết quả của bằng chứng π cho phép các nút này biết khóa công khai tương ứng với khóa sk có thể xác minh xem giá trị băm có được liên kết với $seed$ hay không .$seed$ được chọn ngẫu nhiên và công khai, $seed$ của mỗi vòng được tạo từ $seed$ của vòng trước đó. Thuật toán xổ số hỗ trợ phân công vai trò, chẳng hạn như chọn người tham gia tại một thời điểm nhất định trong quá trình đồng thuận. Tất cả các nút đầy đủ đều thực hiện thuật toán xổ số để xác định xem chúng có phải là người chứng thực được ủy quyền hay không. Các nút đầy đủ đã chọn sẽ phát kết quả xổ số của họ tới các nút đầy đủ khác thông qua mạng P2P. Lưu ý để bảo vệ chống lại một cuộc tấn công

Sybil, xác suất chọn một nút đầy đủ bằng xổ số là tỷ lệ thuận với trọng số của toàn bộ nút. Một nút đầy đủ với trọng số cao có thể được chọn nhiều lần, trong đó thuật toán xổ số sẽ báo cáo số lượng nút đầy đủ đã được chọn. Nếu một nút đầy đủ được chọn nhiều lần, nó sẽ được coi như nhiều nút đầy đủ khác nhau.

5.3.3. Hiệp định Byzantine

Đàm phán Byzantine (BA) xác định quá trình ưu tiên công chứng cho bộ nút đầy đủ được chọn và cung cấp bằng chứng ưu tiên công chứng. Thuật toán BA được lặp đi lặp lại cho đến khi đạt được đồng thuận Byzantine. Trong thuật toán BA, mỗi lượt đàm phán được bắt đầu bằng hình thức quay xổ số. Các nút đầy đủ sẽ phải kiểm tra xem mình có được chọn tham gia vào quá trình BA hiện tại hay không. Một thành viên nào đó phát đi một tin nhắn chứa quyền ưu tiên chọn công chứng viên và sau khi nhận được thông báo này, các nút đầy đủ sẽ lập tức khởi tạo thuật toán BA. Quá trình trên lặp đi lặp lại cho đến khi đạt đủ số lượng nút đầy đủ cho sự nhất trí tại một vòng đàm phán. Lưu ý rằng thuật toán BA không đồng bộ giữa các nút đầy đủ. Khi một nút đầy đủ thấy các bước trước đó đã hoàn tất rồi, nó sẽ ngay lập tức kiểm tra kết quả bầu cử mới. Một nút đầy đủ được phép tham gia lần đàm phán tiếp theo cho đến khi tất cả các nút đều vote và đạt được sự đồng thuận.

Một tính năng quan trọng của thuật toán BA là người tham gia chỉ cần lưu trữ khóa riêng, thay vì duy trì các trạng thái riêng tư. Vì vậy, sau mỗi bước thì chúng ta có thể thay đổi người tham gia để giảm thiểu các tấn công vào họ. Khi mạng được đồng bộ mạnh, thuật toán BA đảm bảo rằng đồng thuận cuối cùng có thể đạt được trong vài bước tương tác nếu tất cả các nút đầy đủ trung thực được khởi tạo với cùng một nội dung. Trong trường hợp này, tất cả các nút đầy đủ trung thực sẽ đạt được đồng thuận cuối cùng trong giới hạn tương tác ngay cả khi có một lượng nhỏ nút tấn công.

6

Thuật toán băm và thuật toán chữ ký chống lại các cuộc tấn công lượng tử

6.1. Thuật toán băm chống tấn công lượng tử

Thuật toán băm trong mã hóa, còn được gọi là hàm băm, đóng vai trò quan trọng trong mã hóa hiện đại. Thuật toán băm là một hàm mã hóa công khai H ánh xạ thông điệp M có độ dài bất kỳ thành một giá trị có độ dài cố định và ngắn hơn thông điệp ban đầu $h. h$ được gọi là thông điệp biến tấu , hay còn được gọi là giá trị băm, hoặc băm. Cấu trúc của thuật toán băm được hiển thị trong Hình 6-1

Figure 6-1: Hash Algorithm Schematic

Để đảm bảo cho dữ liệu không bị thay đổi, Blockchain sẽ lưu cả các giá trị hàm băm cộng với dữ liệu gốc hoặc bản ghi giao dịch. Dữ liệu giao dịch trên Blockchain thường giữ giá trị băm Merkle bản cuối sau khi trải qua nhiều lần băm. Thường thì thông tin địa chỉ trên blockchain sẽ có được bằng cách tính toán ra giá trị băm rồi sau đó chuyển đổi giá trị băm này thành một chuỗi gồm các số và chữ cái thông qua một dạng mã hóa riêng biệt (chẳng hạn như trong bitcoin là sử dụng dạng mã Base58).

Hiện nay, thuật toán lượng tử mạnh nhất có thể tấn công thuật toán băm là thuật toán GROVER, thuật toán này làm giảm độ mức độ phức tạp của thuật toán băm từ (2n) xuống O (2√n) lần, hiện tại thì thuật toán băm PIREMD160 dùng trong hệ thống bitcoin không còn an toàn trước tấn công lượng tử nữa bởi vì độ dài của dữ liệu đầu ra sau khi dùng hàm này chỉ có 160 bit. 1 biện pháp khá hiệu quả để chống lại tấn công lượng tử là tăng độ dài dữ liệu đầu ra lên. Hiện nay, người ta thường nhìn nhận chung chung là các thuật toán băm hiệu quả có thể chống lại được các tấn công lượng tử miễn là chiều dài dữ liệu đầu

ra của thuật toán băm đó là nhỏ hơn 256 bit. Ngoài các mối đe dọa tấn công lượng tử, một loạt các hàm băm được sử dụng rộng rãi (như MD4, MD5, SHA-1 và HAVAL) thực tế đã bị tấn công bởi các phương pháp truyền thống như phân tích chéo, phân tích vi phân mô đun và phân tích sửa đổi thông điệp , do đó, thuật toán băm trong Blockchain cũng cần phải xem xét là khả năng đề kháng với các tấn công truyền thống.

Các dự án Blockchain trước đó như bitcoin, Litecoin và Ethereum sử dụng chuỗi thuật toán SHA với một vài lỗi thiết kế (tuy nhiên không đến mức nghiêm trọng) và các dự án Blockchain gần đây hầu hết đều sử dụng các thuật toán trong chuỗi thuật toán SHA-3 của Viện Tiêu chuẩn và Công nghệ Hoa Kỳ. InterValue sử dụng Keccak512 là thuật toán vượt trội hơn hẳn so với SHA-3. Keccak512 chứa nhiều concept và ý tưởng mới về hàm băm và thiết kế thuật toán mã hóa, với thiết kế đơn giản, rất dễ thực thi trên phần cứng. Thuật toán được đề xuất bởi Guido Bertoni, Joan Daemen, Michael Peters và Giles Van Assche vào tháng 10/2008. Keccak512 sử dụng cấu trúc bọt biển tiêu chuẩn để ánh xạ các bit đầu vào với độ dài bất kỳ thành các bit đầu ra có độ dài cố định. Thuật toán này xử lý rất nhanh, tốc độ trung bình là 12,5 chu kỳ mỗi byte trên bộ xử lý Intel Core 2 Duo.

Như trong Hình 6-2, trong giai đoạn hấp thu của cấu trúc bọt biển trong thuật toán, mỗi gói tin được XOR với *r* bit bên trong các trạng thái và sau đó được đóng gói thành gói dữ liệu 1600-bit cùng với *c* bit cố định sau khi hàm bánh xe f được thực thi và sau cùng là quá trình đẩy ra. Trong giai đoạn *vắt* dữ liệu, giá trị băm với độ dài dữ liệu đầu ra cố định n-bit có thể được tạo ra bằng cách lặp qua 24 lần lặp, chỉ có vòng cuối cùng trong hằng số vòng mới có sự khác biệt trong mỗi lần lặp, nhưng vòng hằng số này thường bị bỏ qua trong các cuộc tấn công va chạm . Thuật toán đã được chứng minh là có các tính chất vi phân rất tốt, cho đến nay phân tích mã hóa của bên thứ ba không cho thấy rằng Keccak512 có điểm yếu bảo mật nào. Loại mức độ phức tạp tấn công đầu tiên bằng Máy tính lượng tử đối với thuật toán Keccak512 là 2^{256}. Do đó, InterValue sử dụng thuật toán Keccak512 có thể chống lại tấn công lượng tử.

6.2. Thuật toán chữ ký chống lại các cuộc tấn công lượng tử

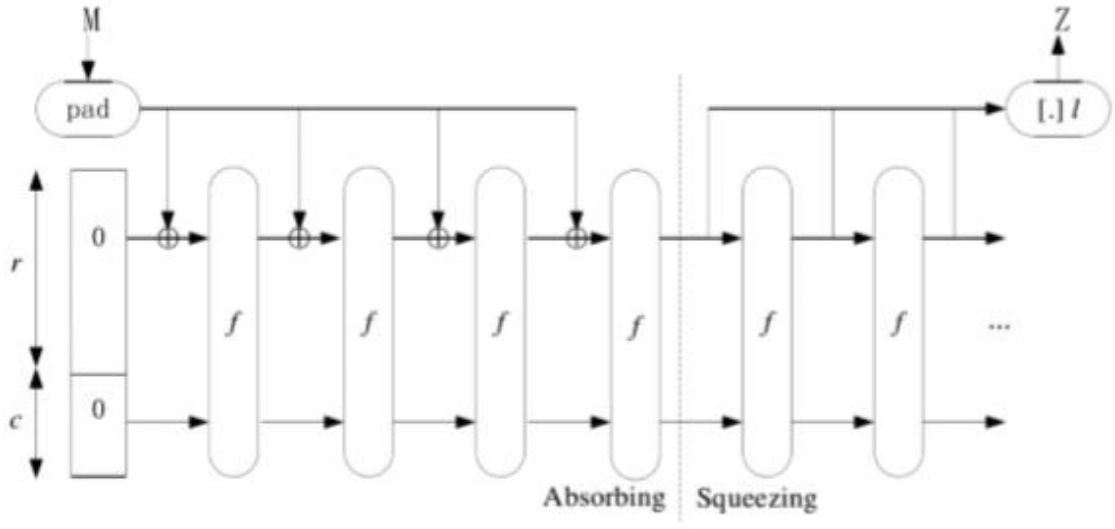


Figure 6-2: The Flowchart of Keccak512 Algorithm Implementation

Thuật toán băm có thể đảm bảo rằng dữ liệu giao dịch không bị điều chỉnh, nhưng nó không hề đảm bảo đối với các cuộc tấn công thay thế đồng thời trên dữ liệu và thông điệp mã hóa, hay không loại bỏ dữ liệu giao dịch. Thuật toán chữ ký số bao gồm khóa công khai, khóa riêng, ví và các công cụ khác. Nó có hai chức năng: một là xác nhận rằng thông điệp này được ký tên và gửi bởi người gửi, đảm bảo không loại bỏ, và hai là để hội tụ tính toàn vẹn của thông điệp. Công nghệ chữ ký số là mã hóa thông tin tóm tắt bằng khóa riêng của người gửi và truyền nó tới người nhận bằng tin nhắn gốc. Người nhận có thể giải mã thông tin thông tin được mã hóa chỉ với khóa công khai của người gửi và sau đó sử dụng thuật toán băm tạo ra thông báo nhận được và so sánh với thông báo đã giải mã. Nếu giống nhau nghĩa là tin nhắn nhận được là hoàn chỉnh và chưa bị sửa đổi trong quá trình truyền đi, nếu không thì có nghĩa là thông điệp đã bị thay đổi. Do đó, chữ ký số có thể xác minh tính toàn vẹn của thông điệp và đảm bảo không loại bỏ thông điệp.

Các hệ thống Blockchain hiện tại chủ yếu sử dụng ECDSA, một lược đồ chữ ký số đường cong elliptic dựa trên thuật toán chữ ký DSA. Theo tiêu chuẩn ANSI, IEEE, NIST và ISO thì ECDSA có những ưu điểm sau: tham số hệ thống nhỏ, xử lý nhanh, kích thước khóa nhỏ, chống tấn công mạnh và yêu cầu băng thông thấp. Ví dụ, ECC 160 bit có cùng độ bảo mật như 1024 bit RSA và DSA, trong khi đó ECC 224 bit có cùng độ bảo mật như 2048 bit RSA và DSS. Đối với máy tính lượng tử có thuật toán tấn công SHOR rất hiệu quả, thuật toán của SHOR phù hợp để giải quyết phân tách số nguyên lớn, đảo ngược logarit rời rạc và các vấn đề toán học khó khăn khác. Hiện nay, các hệ thống mã hóa khóa công khai chống lại tấn công lượng tử chủ yếu bao gồm các hệ thống mã hóa khóa công khai dựa trên lý thuyết mạng lattice, code lập trình sửa lỗi dựa trên mã khóa công khai tiêu biểu là McEliece và đa thức đa biến dựa trên hệ thống mã hóa khóa công khai tiêu biểu là MQ. Bảo mật McEliece dựa trên code lập trình sửa lỗi, an toàn nhưng hiệu quả tính toán thấp. Hệ thống mật mã MQ dựa trên hai phương trình đa thức biến thiên trong phạm vi hữu hạn. Tuy nhiên, thiếu sót bảo mật của nó là hiển nhiên. Ngược lại, hệ thống mã hóa khóa công khai dựa trên lý thuyết mạng lattice có những ưu điểm về tính đồng nhất, tốc độ tính toán nhanh và không gian lưu trữ nhỏ. InterValue sử dụng thuật toán chữ ký dựa trên lý thuyết mạng NTRUSign-251, thuật toán thực hiện quá trình cụ thể như sau:

1. Key Generation: Chọn hai đa thức f và g trên ring R sao cho số 1 trong các coefficients của f và g tương ứng là df và dg, tính toán khóa công khai h: $h = F\text{q} * g \pmod q$.

Giải phương trình đa thức (F, G) để nó thỏa mãn phương trình $f * G - F * g = q$.

Và $F \approx f \sqrt{N / 12}$, $G \approx g \sqrt{N / 12}$.

2. Qui trình chữ kí :

1) Chuyển đổi HASH của thông điệp M được chuyển thành đa thức $(m1, m2)$, trong đó các đa thức $m1$ và $m2$ là đa thức trên vòng Rq.

2) Các đa thức A, B, a, b trên vòng được tính toán để thỏa mãn:

$G * m1 - F * m2 = A + q * B$

$-g * m1 - f * m2 = a + q * b$

Và các hệ số của từng mục A và a được yêu cầu phải đáp ứng các điều kiện lớn hơn q / 2 và nhỏ hơn q / 2.

3) Đa thức s được tính như sau:

$s = f * B + F *$ (mod q)

là chữ ký được tính bằng chữ thô M bằng cách sử dụng khóa công khai h.

3. Quá trình xác minh:

Chuyển đổi băm thông báo M thành đa thức ($m1$, $m2$).

Được tính từ chữ ký xác minh s và đa thức khóa công khai H

$t = g * B + G *$ (mod q)

Tính khoảng cách giữa các đa thức (s, t) và ($m1$, $m2$): $m1 - s +$ $m2 - t$, Nếu khoảng cách lớn hơn NormBound thì xác minh không thành công, nếu không chữ ký được xác thực.

Chứng minh rằng sự an toàn của thuật toán chữ ký NTRUSign-251 cuối cùng tương đương với việc tìm ra lời giải cho bài toán vectơ ngắn nhất trong một mạng số nguyên 502 chiều. Vấn đề vector ngắn nhất trong mạng không hợp lệ theo thuật toán của SHOR, thuật toán heuristic tốt nhất tỷ lệ cấp số nhân tại thời điểm này, độ phức tạp thời gian của thuật toán NTRUSign-251 là khoảng vào 2^{168}, vì vậy InterValue sử dụng thuật toán NTRUSign-251 có thể chống lại thuật toán SHOR tấn công bằng tính toán lượng tử.

7

Giao dịch ẩn danh

Giao dịch ẩn danh và bảo vệ quyền riêng tư về bản chất là những thuộc tính của tiền tệ điện tử. Tuy nhiên, các loại tiền mã hóa kỹ thuật số hiện nay đang gặp phải 1 vấn đề, đó là tính thiếu hiệu quả trong các giao dịch ẩn danh và riêng tư. InterValue được thiết kế để trở thành một đồng tiền mã hóa với các giao dịch không liên kết và không thể truy tìm.

Blockchain 4.0 mang đến những khái niệm mới về khả năng phá bỏ các mối liên kết và ngăn cản việc truy tìm gốc tích. Phá bỏ các mối liên kết có nghĩa là đối với hai giao dịch, không thể chứng minh rằng chúng được gửi đến cho cùng một người. Ngăn cản việc truy tìm gốc tích có nghĩa là cho một dữ liệu đầu vào giao dịch, dữ liệu đầu ra của giao dịch thực sự sẽ được ẩn trong một tập hợp các giá trị khác. Để đảm bảo tính không liên kết và không thể truy cập, InterValue đưa ra giải pháp one - $timesecretkey$ và mật mã nguyên thủy gọi là $ringsignatures$. InterValue theo thiết kế sử dụng nghiêm ngặt $-knowledgeproof$ $-knowledgeproof$ để đảm bảo các giao dịch có tính chất.

7.1. Khóa bí mật sử dụng một lần

Khi sử dụng lược đồ khóa bí mật một lần, một cặp khóa duy nhất được sử dụng cho mọi giao dịch. Người gửi tạo khóa công khai một lần tạm thời dựa trên địa chỉ của người nhận và một số ngẫu nhiên. Với khóa công khai tạm thời, khóa giao dịch được tạo, là địa chỉ giao dịch. Vì vậy, các giao dịch được chuyển đến cùng một người nhận trên thực tế được gửi đến các khóa công khai một lần. Đồng thời, chỉ người nhận mới có thể khôi phục khóa cá nhân một lần để đổi tiền. Khả năng hủy liên kết có thể được duy trì vì tính ngẫu nhiên khác nhau trong mọi giao dịch.

7.2. Chữ ký vòng

Chữ ký Vòng là chữ ký kỹ thuật số ghi một nhóm người ký tên có thể sao cho người kiểm tra không thể biết thành viên nào đã thực sự tạo chữ ký. Nó có nguồn gốc từ chữ ký đa người dùng. Tuy nhiên, các vòng là các khu vực hình học với ngoại vi đồng nhất và không có trung tâm. Vì vậy, chữ ký vòng có một số ưu điểm như không có quản trị viên nhóm, với tính không thể truy cập mạnh, vv Nguyên tắc của lược đồ chữ ký vòng được hiển thị trong Hình 7-1.

Khi sử dụng chữ ký vòng, một tin nhắn được ký bởi một người dùng nhóm và người kiểm tra không thể biết ai là người dùng mục tiêu. Vì lý do này, các giao dịch với chữ ký vòng trong tiền điện tử là tự nhiên không thể truy cập và tính riêng tư. Mặt khác, các giao dịch có chữ ký vòng cũng bị kiện từ vấn đề chi tiêu gấp đôi khi người ký mục tiêu được ẩn từ một người dùng nhóm. Lược đồ chữ ký kết nối vòng có thể được sử dụng để tránh chi tiêu gấp đôi.

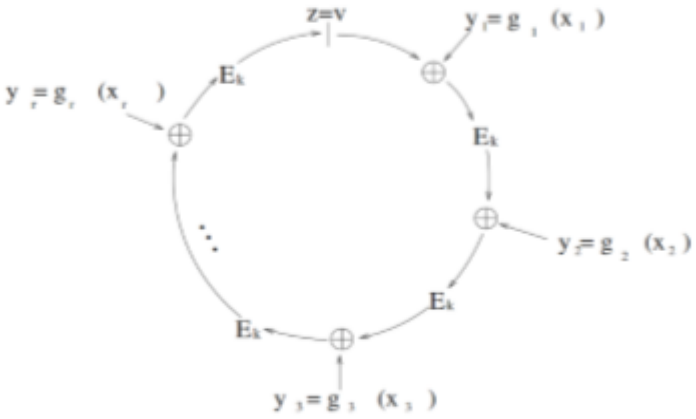


Figure 7–1: The Ring Signature

7.3. Bằng chứng không kiến thức (zezo knowlegede proof)

Đề án chứng minh kiến thức của Thezero ban đầu được đề xuất bởi Goldwasser, S.Micali và C.Rackoin1985 bằng cách yêu cầu cho mọi trình xác minh độc hại V, tồn tại một trình mô phỏng sinh thái có thể tái tạo lại quan điểm của một tương tác thực sự với prover, theo cách không thể phân biệt được cho mọi phân biệt thời gian đa thức.

Về cơ bản, bằng chứng tri thức không có nguồn gốc từ hệ thống chứng minh toán học truyền thống bằng cách giới thiệu tính ngẫu nhiên và biến tương tác. Đối với một ứng dụng có bằng chứng không có kiến thức, vấn đề về vấn đề độc hại, đòi hỏi người kiểm duyệt không thể đạt được kiến thức mới trong quá trình xác minh, là yếu tố chính cần tránh. ZCash là cryptocurrency đầu tiên sử dụng bằng chứng nhận biết để đảm bảo tính liên tục của các giao dịch.

7.4. Giao dịch bảo mật

InterValue được thiết kế để ẩn danh và riêng tư cho giao dịch có điều kiện. Lấy cảm hứng từ Monero, InterValue 1.0 đến 3.0 thực hiện khóa bí mật và chữ ký một lần để đáp ứng yêu cầu ẩn danh và riêng tư. Trong khi InterValueuse cải thiện RingCT 2.0 để giảm thiểu sự tấn công rò rỉ thông tin trong Monero. InterValue 4.0 sẽ thực hiện bằng chứng không có kiến thức mạnh mẽ kết hợp với RingCT để đạt được các giao dịch đầy đủ tiềm năng.

8

Hợp đồng thông minh

Công nghệ Blockchain mang đến cho chúng ta một hệ thống phân cấp, không tin tưởng, không làm sai lệch và độ tin cậy cao. Trong môi trường này, các hợp đồng thông minh mang 1 tiềm năng to lớn. Hợp đồng thông minh là các hợp đồng tự thực thi với các điều khoản của thỏa thuận giữa người mua và người bán được ghi trực tiếp vào các dòng mã. Mã và các thỏa thuận chứa trong đó tồn tại trên một mạng Blockchain phân tán, phân tán. Hợp đồng thông minh cho phép các giao dịch và thỏa thuận đáng tin cậy được thực hiện giữa các bên không xác định, ẩn danh mà không cần cơ quan trung ương, hệ thống pháp luật hoặc cơ chế thực thi bên ngoài. Họ làm cho các giao dịch theo dõi, minh bạch và không thể đảo ngược.

Hợp đồng thông minh cần phải có một sự cân bằng tinh tế giữa sự an toàn và tính năng sử dụng. Các blockchains hiện tại chủ yếu là được thiết kế đơn điệu, tìm kiếm sự cân bằng giữa tính an toàn và khả năng sử dụng dưới những hạn chế của một loại hợp đồng thông minh sẵn có và thường không thể đảm bảo trải nghiệm người dùng phong phú và đáp ứng các nhu cầu giao dịch khác nhau. Kịch bản giao dịch trong blockchain bitcoin là một nguyên mẫu ban đầu của hợp đồng thông minh. Đây là một dạng hợp đồng Turing-không hoàn chỉnh, với độ phức tạp thấp và trọng lượng nhẹ. Trong mười năm qua, trong Bitcoin, kịch bản giao dịch này chưa bao giờ gặp bất kỳ vấn đề nào về bảo mật. Tuy nhiên, tập lệnh giao dịch Bitcoin có chức năng rất hạn chế và chỉ có thể được sử dụng để xác minh thanh toán. Blockchain Ethereum hỗ trợ các hợp đồng thông minh hoàn chỉnh Turing được lập trình bằng ngôn ngữ Solidity. Nó làm phong phú thêm chức năng của hợp đồng thông minh và phần lớn mở rộng các kịch bản ứng dụng cho blockchain. Thật không may là hợp đồng thông minh Ethereum lại gặp phải các nguy cơ tiềm ẩn về an toàn. Sự cố the DAO là một ví dụ nổi tiếng, vấn đề an toàn trong hợp đồng thông minh Ethereum dẫn đến sự chia rẽ trong cộng đồng. Được xây dựng dựa trên hợp đồng thông minh và Máy ảo Moses (MVM), InterValue có ý tưởng tương tự như thiết kế phân cấp của hệ thống lưu trữ máy tính và hỗ trợ cả hợp đồng thông minh Turing không hoàn chỉnh và hợp đồng thông minh Turing hoàn chỉnh nâng cao. Người dùng lựa chọn giữa hai loại hợp đồng thông minh dựa trên kinh nghiệm và nhu cầu thương mại của họ, do đó đạt được sự cân bằng giữa an toàn, chức năng, phức tạp và chi phí. Hợp đồng khai báo dễ triển khai, có mức độ an toàn cao và gần với các báo cáo hợp đồng pháp lý. Hợp đồng tiên tiến này khó triển khai hơn và chủ yếu được sử dụng để phát triển DApp với logic phức tạp hơn. Hai hợp đồng thông minh có các sơ đồ tính phí di động. Hợp đồng khai báo tính theo số lượng byte được sử dụng, trong khi phí hợp đồng nâng cao theo số lượng mã INVE được sử dụng.

8.1. Hợp đồng thông minh khai báo Turing không hoàn chỉnh

Hợp đồng thông minh khai báo Turing không hoàn chỉnh có trọng lượng nhẹ, dễ lập trình và độ phức tạp thấp và mức độ an toàn cao. Nó bao gồm các câu lệnh và biểu thức boolean, do đó gần với ngôn ngữ

truyền thống của các hợp đồng pháp lý. Nó hỗ trợ các phép toán boolean và toán học, cũng như lưu trữ dữ liệu. InterValue cung cấp rất nhiều mẫu được tạo sẵn để người dùng sử dụng hoặc sửa đổi, do đó giảm độ khó triển khai và mức độ lỗi. Hơn nữa, trái ngược với hợp đồng thông minh hoàn thiện Turing, nó có mức độ an toàn cao hơn. Nó sử dụng cùng một lược đồ tính phí như các giao dịch thương mại thông thường, đó là nhờ các byte.

Nó thường đòi hỏi một mức độ kiến thức cụ thể về lập trình để thực hiện một hợp đồng thông minh. Để dễ dàng sử dụng người dùng thông thường, InterValue hỗ trợ nhiều loại mẫu hợp đồng thông minh khai báo Turing không hoàn chỉnh (Mẫu hợp đồng). Tất cả những gì người dùng cần làm là chọn một mẫu ưa thích và điền các tham số liên quan vào. Các mẫu có thể được sử dụng lại hoặc được trích dẫn trong các mẫu khác. Sau đây là một ví dụ về các hợp đồng thông minh như vậy.

[”contract template”, [

”hash of unit where the template was defined”,

{param1: ”value1”,param2: ”value2”}

]]

Mặc dù mức độ phức tạp thấp, nhưng Hợp đồng thông minh khai báo Turing không hoàn chỉnh vẫn có khả năng nâng cao các chức năng như lấy dữ liệu bên ngoài hoặc truyền thông blockchain liên thông.

Sau đây là ví dụ về lấy dữ liệu ngoài. Nếu dữ liệu được gửi bởi Alice, Bob hoặc Cara cao hơn giá trị dự kiến, điều kiện là đúng. Khác với "=", hợp đồng cũng hỗ trợ các hoạt động như "! =", ">", ">" = Và "<=". Kiểm soát điều kiện phức tạp có thể đạt được bằng cách xác định nguồn dữ liệu.

[” in data feed”, [[”Alice ”, ”Bob”, ”Cara” ...] , ”data feed name”, ”=”, ”expected value”]]

Sau đây cho thấy một ví dụ về giao tiếp interblockchain. Bob giao dịch cho BTC với Alice thông qua INVE và thời gian giao dịch được giao vào 2018-02-15. Trước thời điểm đó, nếu Alice chuyển 10 BTC cho Bob, thì oracle BTC sẽ có một hồ sơ tương ứng và hợp đồng sẽ kích hoạt. Sau đó, Alice sẽ nhận được INVE mà Bob đã ký gửi vào hợp đồng trước. Số lượng INVE chính xác dựa trên thương lượng về tỷ lệ chuyển tiền của Alice và Bob. Nếu Alice không chuyển 10 BTC trước thời điểm được thương lượng, Bob sẽ lấy lại khoản tiền gửi của anh ấy.

[”or”, [[

”and”, [[”address”, ”Alice ”] ,

[” in data feed”, [[”BTC oracle ”] , ”BTC from Alice to Bob”,

”=”,

”10”]]]] ,

[”and”, [[”address”, ”Bob”] ,

[” in data feed”, [[”TIMESTAMPER ADDRESS”] ,

”datetime”,

”<”,

”2018−02−15 00:00:00”]]

]]

]]

8.2. Hợp đồng thông minh Turing hoàn chỉnh nâng cao

Hợp đồng thông minh Turing hoàn chỉnh nâng cao hỗ trợ các logic goto và loop, do đó có thể cho phép nhiều chức năng phong phú hơn hợp đồng thông minh Turing không hoàn chỉnh. Tuy nhiên, nó cũng đòi hỏi nhiều kiến thức hơn để lên chương trình và dễ gặp vấn đề về an toàn hơn. Kết quả là, nó đòi hỏi phải có các chuyên gia đứng ra xây dựng và thử nghiệm trước. Để bảo vệ hiệu năng mạng khỏi bom logic và cung cấp cơ chế chống gian lận, các hợp đồng thông minh hoàn chỉnh Turing không còn tính phí theo các byte được sử dụng mà bắt đầu áp dụng một cơ chế tương tự như Gas được sử dụng trong hợp đồng thông minh Ethereum. Khi người dùng gọi một hợp đồng thông minh, họ phải gửi một lượng Gas nhất định trước. Khi hợp đồng thông minh được thực thi, Gas sẽ được tiêu thụ khi các hướng dẫn trong hợp đồng được kích hoạt. Sau khi hợp đồng thông minh được hoàn thành, Gas còn lại sẽ được trả lại cho nhà xuất bản. Nếu tất cả các khoản tiền gas được tiêu thụ trước khi hợp đồng được kết thúc, trạng thái của hợp đồng sẽ được chuyển về trạng thái ban đầu và gas tiêu thụ sẽ không được trả lại.

InterValue sử dụng một ngôn ngữ lập trình nâng cao mới được đề xuất, được gọi là Moses, để lập trình hợp đồng thông minh Turing hoàn chỉnh. Moses là ngôn ngữ object-oriented, có phong cách lập trình tương tự như JavaScript, do đó tạo điều kiện dễ dàng cho số lượng lớn các nhà phát triển Web di chuyển sang InterValue. Với Moses, các chức năng của hợp đồng thông minh chưa hoàn chỉnh Declarative Turing-cũng có thể được thực hiện. Tính năng độc đáo của InterValue Advanced Turing-hợp đồng thông minh hoàn chỉnh là hỗ trợ truy cập vào dữ liệu off chain. Khi các kịch bản ứng dụng của blockchain nhanh chóng mở rộng, nhu cầu truy cập dữ liệu off chain cũng tăng nhanh. Hợp đồng thông minh Ethereum chỉ hỗ trợ truy cập dữ liệu onchain đang trở nên hạn chế. Ở đây, dữ liệu off-chain thường không đề cập đến tất cả các dữ liệu không on-chain InterValue, nhưng về mặt dữ liệu trên các hệ thống lưu trữ phân tán dựa trên kỹ thuật blockchain. Loại dữ liệu này thường có chất lượng cao, nhưng liên quan đến vấn đề phân phối lợi nhuận, yêu cầu sử dụng hợp đồng thông minh để đạt được xác thực và cấp quyền truy cập dữ liệu.

• Truy cập dữ liệu off-chain an toàn: Moses có các giao thức dựng sẵn được thiết kế đặc biệt để truy cập dữ liệu off-chain. Ví dụ, giao thức IPFS tích hợp được thiết kế đặc biệt để truy cập dữ liệu trên hệ thống lưu trữ phân tán IPFS. Bằng cách có giao thức dựng sẵn, truy cập dữ liệu có thể bị hạn chế và nguy cơ truy cập dữ liệu / chương trình độc hại được giảm xuống. Vào thời điểm đó, InterValue cũng sẽ xây dựng hệ thống lưu trữ phân tán của riêng mình và xây dựng trong giao thức truy cập dữ liệu. Những người dùng lưu trữ dữ liệu trong hệ thống sẽ trả tiền cho mỗi mức kích thước, do đó đảm bảo chất lượng dữ liệu.

• Sử dụng dữ liệu off-chain an toàn: Moses cho phép đọc / ghi các hoạt động với dữ liệu off-chain, nhưng không cho phép thực hiện thao tác. Bằng cách đọc dữ liệu off-chain, Moses hỗ trợ logic kinh doanh hợp lý. Sự phức tạp của hợp đồng thông minh Turing hoàn chỉnh nâng cao không chỉ nằm trong logic chương trình của nó, mà còn là logic kinh doanh. Ví dụ, khi soạn một hợp đồng thông minh liên quan đến lập pháp, sự hỗ trợ từ các chuyên gia pháp lý là cần thiết, mà không thể được cung cấp bởi các

nhà phát triển chuyên nghiệp. InterValue cung cấp định dạng cấu hình dựa trên quy tắc có thể hỗ trợ để lưu trữ kiến thức trong một ngành nghề cụ thể dưới dạng các quy tắc ngoài blockchain. Bằng cách đọc các tài liệu này, hợp đồng thông minh nhận ra logic nghiệp vụ trong khu vực chuyên môn nhất định. Tài liệu tập trung trong một lĩnh vực chuyên môn cụ thể có thể tái sử dụng, do đó mở ra khả năng của một thị trường trao đổi dữ liệu. Nói chung, dữ liệu do người dùng cung cấp sẽ được xác nhận là an toàn từ trước

8.3. Máy ảo Moses (MVM)

Cả hợp đồng thông minh chưa hoàn chỉnh Declarative Turing và hợp đồng thông minh hoàn chỉnh Turing nâng cao đều được xác nhận và thực thi trong máy ảo Moses. Máy ảo Moses sử dụng cấu trúc dựa trên ngăn xếp. Nó không chỉ có thể đơn giản hóa việc thực thi các hướng dẫn và trình biên dịch, mà còn có thể cung cấp tính di động vượt trội. Cấu trúc dữ liệu của một MVM đang chạy được hiển thị bên dưới.

• Bộ đếm lệnh: Lưu địa chỉ bytecode của lệnh tiếp theo.

• Ngăn xếp máy ảo: Mỗi lần hợp đồng thông minh hoàn thiện Turing hoàn chỉnh được thực hiện, MVM sẽ tạo một ngăn xếp máy ảo trong khu vực điều phối lệnh. Ngăn xếp máy ảo bao gồm các khung ngăn xếp khác nhau, và mỗi lần thực hiện và hoàn thành một hợp đồng thông minh tương ứng lần lượt với quá trình ngăn xếp và pop.

• Ngăn xếp phương thức gốc: Thuộc sở hữu riêng của bộ phận điều phối hướng dẫn. Nó có chức năng tương tự như ngăn xếp máy ảo và được sử dụng để lưu trữ thông tin liên quan đến phương thức.

• Heap: Tất cả các đối tượng của hợp đồng thông minh được phân bổ một không gian lưu trữ ở đây.

• Vùng phương thức: Được sử dụng bởi MVM để tải class lớp, hằng số và các biến tĩnh.

Hợp đồng thông minh Turing hoàn chỉnh nâng cao đã được biên dịch thành bytecode trước khi được triển khai trên InterValue và MVM có thể tải và chạy trực tiếp nó. Ngược lại, hợp đồng thông minh không được khai báo Decuringative Turing-incomplete được nhúng vào dữ liệu giao dịch trong JSON, mà không thể được nạp và chạy trực tiếp bởi MVM. Trong máy khách InterValue, sẽ có một trình biên dịch cho hợp đồng thông minh khai báo Turing-không hoàn chỉnh, nó sẽ biên dịch hợp đồng thành một bytecode đối tượng hợp đồng mặc định. Bytecode sau đó được nạp vào MVM và chạy.

Hãy xem xét việc bảo vệ ở mức độ hệ thống của hợp đồng thông minh trước các cuộc tấn công nguy hiểm, MVM được thiết kế để trở thành một sandbox với các chính sách kiểm soát truy cập chặt chẽ. Dựa trên việc thực hiện môi trường thực hiện cách ly cấp tiến trình theo định hướng bytecode, một danh sách trắng được thực hiện theo nguyên tắc của các đặc quyền tối thiểu được sử dụng trong sandbox bảo mật của MVM. Mỗi phương thức được gọi bằng mã hợp đồng thông minh được kiểm tra nghiêm ngặt để hạn chế quyền truy cập để đáp ứng các chức năng hoạt động của nó được thiết kế. Và dữ liệu trong ngăn xếp và Heap được lưu trữ với các chính sách kiểm soát truy cập chặt chẽ cho mục đích sử dụng tin tưởng.

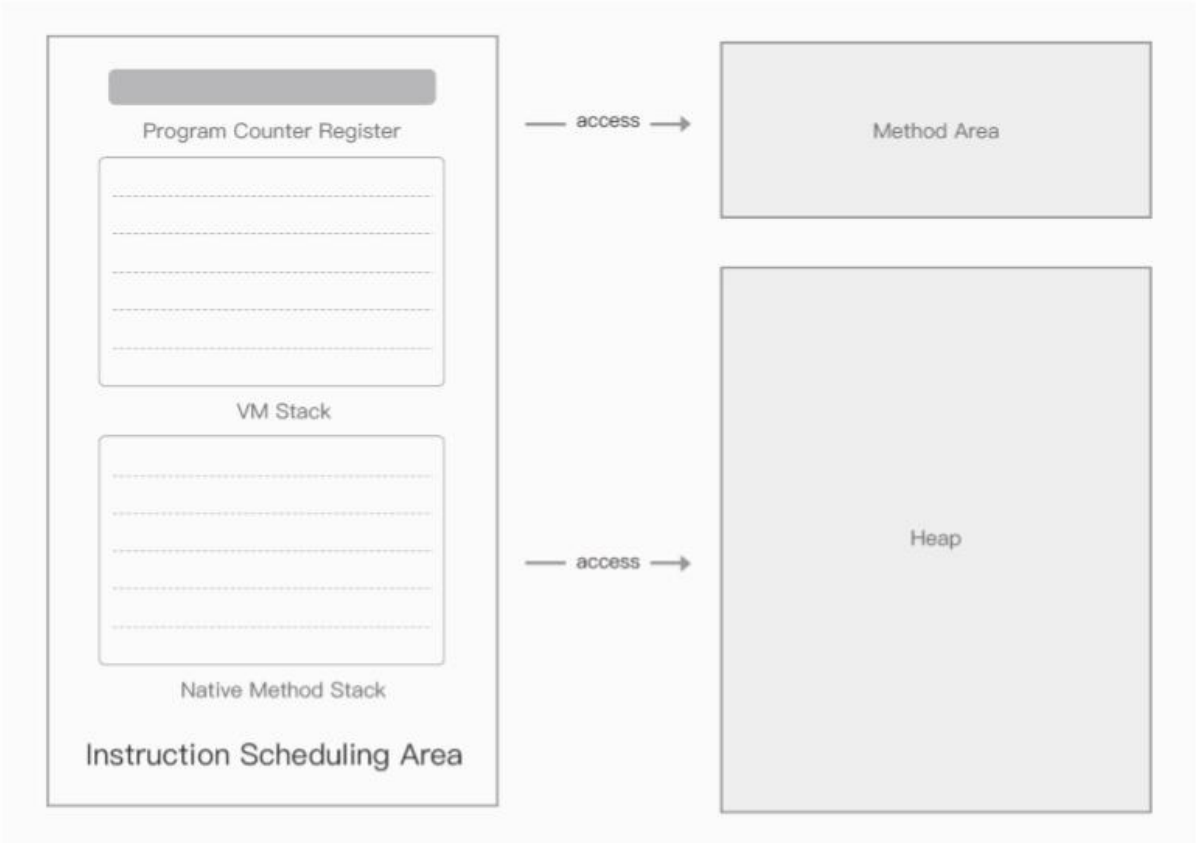


Figure 8–1: MVM Runtime Area

8.4. Tài khoản hợp đồng thông minh và giao dịch

Tương tự như tài khoản trong Ethereum, trong InterValue có những tài khoản ngoại biên và những tài khoản hợp đồng. Các hợp đồng bên ngoài được kiểm soát bởi người dùng, được sử dụng để triển khai giao dịch. Các tài khoản hợp đồng được kiểm soát bởi các tài khoản bên ngoài, bằng cách thực hiện các phép gọi từ các tài khoản bên ngoài và các tài khoản hợp đồng khác để bắt đầu thực hiện hợp đồng thông minh.

Hợp đồng thông minh khai báo Turing không hoàn chỉnh được nhúng vào dữ liệu của các giao dịch được khởi tạo bởi các tài khoản bên ngoài. Nó được sử dụng để cung cấp các điều kiện ràng buộc cho giao dịch và không có khái niệm về tài khoản. Tài khoản hợp đồng thông minh đặc biệt đề cập đến tài khoản được trả về sau khi hợp đồng thông minh hoàn chỉnh Advanced Turing được triển khai. Tài khoản bên ngoài và tài khoản hợp đồng có những trạng thái. Ví dụ: số dư tài khoản token INVE và số lượng giao dịch từng được thực hiện đều là các trạng thái của một tài khoản. Để loại bỏ sự tách biệt giữa tài khoản bên ngoài và tài khoản hợp đồng, số tài khoản bao gồm mã băm của mã MVM, không thể thay đổi được sau khi hợp đồng thông minh nâng cao hoàn thành được triển khai. Bên cạnh đó, để truy cập dữ liệu của người dùng được lưu trữ off-chain, các trạng thái tài khoản cũng bao gồm thông tin về ổ lưu trữ dữ liệu blockchain.

Trong InterValue, có hai loại phí giao dịch. Các giao dịch thông thường được khởi tạo bởi các tài khoản bên ngoài tính theo byte. Các giao dịch gọi một hợp đồng thông minh sẽ tính phí bằng số lượng chỉ dẫn được kích hoạt. Để loại bỏ sự tách biệt giữa hai loại phí, hai miền tương tự như giá Gas và giá Gas trong Ethereum được sử dụng trong cấu trúc dữ liệu giao dịch để thống nhất các lược đồ phí. Đối với các khoản phí theo mã byte, số byte của giao dịch được hiển thị (tức là, khoản phí được biết trước), sau đó chúng tôi có thể cố định giới hạn Gas và tự động tính giá Gas để tính phí tài khoản. Khi người dùng gửi một giao dịch của một hợp đồng thông minh hoàn thiện Turing nâng cao, trong cấu trúc dữ liệu giao dịch sẽ có một trường xác định mã MVM.

9

Ứng dụng và bối cảnh

9.1. Ứng dụng

9.1.1 Ứng dụng mạng xã hội phân tán

Ứng dụng mạng xã hội phân tán dựa trên công nghệ blockchain và công nghệ phân phối P2P, để đạt được tính phân cấp, truy cập miễn phí vào bất kỳ mạng xã hội nào, và cũng không bị ảnh hưởng bởi bất kỳ tổ chức nào. Khác với các mạng xã hội truyền thống, các mạng xã hội phân tán không có khái niệm về máy chủ. Tất cả các dữ liệu xã hội được ghi trong các máy tính phân tán. Bất kỳ ai cũng chỉ cần một cặp khóa không đối xứng để xuất bản các nội dung.

Mọi người có thể tìm ra máy tính của những người xuất bản trong mạng P2P thông qua khóa riêng của nhà xuất bản và tải xuống dữ liệu trang web. Sau ngày càng có nhiều người truy cập thì sẽ có một lượng máy tính chịu trách nhiệm lưu nội dung của các nhà xuất bản. Các máy tính đã truy cập vào trang chủ của bạn sẽ bắt đầu gieo rắc thông tin trang web mọi nơi. Giống như những hạt BT chúng ta đều biết, nội dung trang web của bạn sẽ sống trong vô số máy tính.

Miễn là có mạng kết nối với các 'hạt gieo' của trang web, nội dung của bạn sẽ không biến mất. Hơn nữa, khi mạng P2P đủ lớn, nội dung của bạn sẽ không bị xóa hoàn toàn, và chúng sẽ trở nên bất diệt với thế giới Internet.

Mạng xã hội phân tán đã trở nên rất bình thường vì các tính năng host không trung tâm của mạng P2P. Bạn không cần thuê máy chủ để đăng ký các URL. Tất cả những gì bạn cần là tạo một địa chỉ trang ngẫu nhiên theo mã HTML và xuất bản nó lên máy tính khác.

9.1.2. Ứng dụng giao dịch hợp đồng phân tán

Định nghĩa các ứng dụng giao dịch phân kỳ là một thị trường giao dịch bất đồng. Ví dụ: "Xổ số Bắc Kinh" là một thị trường giao dịch bất đồng, nơi người dùng không tán đồng về chiến thắng hoặc thất bại của nhóm.

Các ứng dụng giao dịch hợp đồng khác nhau dựa trên InterValue có thể đạt được một hệ sinh thái win-win từ 5 lĩnh vực :

• Các nhà cung cấp công nghệ: cung cấp tất cả các công nghệ nền tảng toàn phần

• Các nhà quá trình đào nền tảng: chuyển đổi giao diện mặt trước và cung cấp các hoạt động đa ngôn ngữ,

• Các nhà thiết kế phân kỳ : tìm sự bất đồng, thiết kế các hợp đồng khác nhau,

• Market maker hợp đồng: cung cấp thanh khoản,

• Các trader phân kỳ: mua và bán các hợp đồng khác nhau, cân bằng rủi ro và thu lợi nhuận.

9.1.3 Ứng dụng lưới lưu trữ tệp

Lưới lưu trữ tệp là nền tảng chuỗi thương mại công khai, cung cấp dịch vụ cơ bản để lưu trữ dữ liệu riêng lẻ. Cá nhân có thể xuất bản dữ liệu của họ trên chuỗi. Dựa trên dữ liệu cá nhân khổng lồ, nền tảng này thực hiện việc thu thập, chia sẻ và quản trị dữ liệu phi tập trung, bằng cách phát triển các loại DApp chuyên nghiệp. Nền tảng này tạo ra một hệ thống sinh thái cho việc lưu trữ dữ liệu phi tập trung, hội tụ, chia sẻ, quản trị vv.

• Nền tảng lưu trữ dữ liệu phân tán dựa trên lưới lưu trữ tệp,

• Cơ sở hạ tầng chuỗi thương mại công cộng an toàn, có thể mở rộng,

• Một hệ thống tín dụng.

Mục tiêu của chuỗi sinh thái dữ liệu lớn là hiện thực hóa lưu trữ phân tán và các ứng dụng phân cấp quy mô lớn. Hơn nữa, chuỗi sinh thái dữ liệu lớn có những đặc điểm sau đây trên chuỗi công cộng truyền thống.

• Khả năng lập trình,

• Khả năng mở rộng,

• Nâng cấp,

• Khả năng quản lý giao dịch,

• Khả năng hiển thị,

• Khả năng chi trả,

• An toàn,

• Tốc độ / hiệu suất,

• Độ tin cậy cao,

• Độ bền bỉ

9.2 Bối Cảnh

9.2.1. Phác thảo bối cảnh

Những bối cảnh chính của InterValue như sau: (1) Tiền kỹ thuật số; (2) Ứng dụng tài chính mở rộng; (3) Các ứng dụng phi tài chính. các ứng dụng.

• Tiền tệ kỹ thuật số

Các bối cảnh ứng dụng chính của tiền tệ kỹ thuật số như sau: 1 Phát hành tài sản của bên thứ ba; 2 Huy động vốn từ cộng đồng.

• Ứng dụng tài chính mở rộng

Các bối cảnh ứng dụng chính của các loại tiền tệ kỹ thuật số như sau: 1 Thanh toán chéo, Chuỗi cung ứng, Hóa đơn kỹ thuật số; 2 Đảm bảo tài sản, tham khảo ngân hàng, bảo hiểm.

• Các ứng dụng phi tài chính

Chăm sóc y tế: Sức khỏe điện tử (EHR), ví DNA, Thuốc giả mạo

Internet of things: Quản lý chuỗi cung ứng, Chia sẻ kinh tế, Quản lý năng lượng

Bản quyền IP & giải trí văn hóa: Bản quyền, Xác thực và truy tìm hình ảnh, Đăng ký sở hữu trí tuệ, Phân cấp quản lý quyền kỹ thuật số

Dịch vụ công cộng & Giáo dục: Kiểm toán công cộng, Quyền sử dụng đất, Dự án phúc lợi công cộng, Đăng ký thông tin giáo dục

Các ứng dụng cụ thể trên một chuỗi như sau:

Tài sản ảo: Thiết bị trò chơi, Phần thưởng phát sóng trực tiếp,

Thanh toán vô điều kiện: Thanh toán cho kiến thức, gọi API, Bảo hiểm tập trung, v.v.

Thỏa thuận giao dịch bảo mật: Đặt cược, Cờ bạc, v.v.

Giao dịch ngoại hối: Trao đổi tiền tệ,

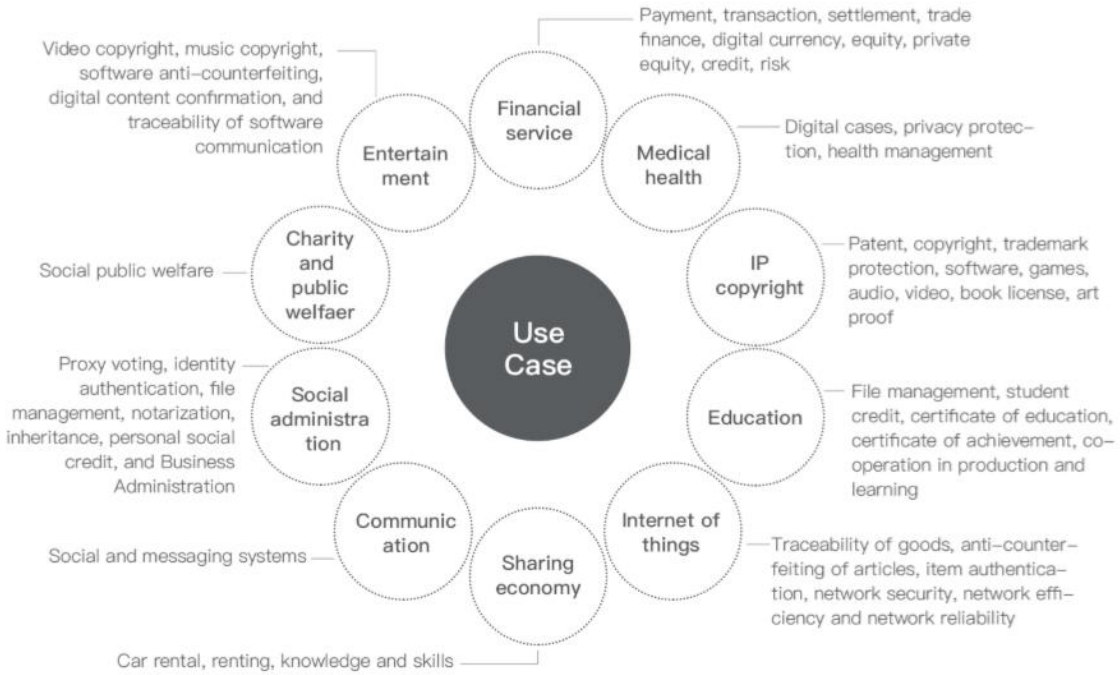
Giao dịch xã hội: Nhóm các gói màu đỏ, Biên nhận nhóm,

Chia sẻ kinh tế: Khuyến khích phân phối nội dung (CDN), Phân chia nợ quảng cáo.

9.2.2. Thực quyền giao dịch tài sản thực

• Chữ ký chung

Chủ sở hữu tài sản và tổ chức phù hợp ký thông tin tài sản để đảm bảo rằng cơ quan phê duyệt thông tin thực trên blockchain. Chủ sở hữu tài sản đăng ký các tài sản trên blockchain và cơ quan có thẩm quyền xác nhận tạo chữ ký chung trên thông tin phù hợp sau khi điều tra và xác định tài sản.



Hình 9-1 Bối cảnh của chuỗi

• Blockchain cộng với chứng chỉ số

Hiện tại, chứng nhận số được áp dụng chủ yếu cho các ngành liên quan đến trao đổi tài sản, chẳng hạn như thương mại điện tử, chứng khoán, bảo hiểm và thanh toán, v.v. Những ngành công nghiệp này cung cấp một bất động sản dựa trên xác thực danh tính mạnh mẽ, một hoạt động trực tuyến chống từ chối và chống hàng giả dựa trên chữ ký điện tử.

Trong quyền xác thực giao dịch tài sản thực, chúng tôi có thể đăng ký chứng nhận ECC tại cơ quan CA. Địa chỉ trên một blockchain tương ứng với khóa công khai. Khóa công khai này tương ứng với chứng nhận số tương ứng. Cơ quan phê duyệt chứng nhận kỹ thuật số này. Danh tính số có thể được xác thực miễn là chứng nhận kỹ thuật số được xuất bản trên blockchain. Sau đó, chúng tôi thực hiện đăng ký thông tin tài sản trên blockchain, bao gồm danh mục tài sản, tên, tổng số tiền, chủ sở hữu, quyền và thông tin khác và chuyển các nội dung thực thể được cơ quan có thẩm quyền phê duyệt.

9.2.3. Nền tảng dịch vụ du lịch phân cấp

Các nút thắt của nền tảng dịch vụ du lịch hiện tại là:

(1) Hệ thống niềm tin: Thị trường du lịch hiện tại là lưu trữ dữ liệu tập trung, ví dụ như các nền tảng như TripAdvisor, Dianping và Priceline. Tất cả họ đều kiểm soát dữ liệu tập trung cho mục đích kinh doanh và quảng cáo, và không thể đảm bảo trải nghiệm người dùng. Phản hồi đến từ những nơi khác nhau và chủ quan và trong nhiều trường hợp là giả mạo hoặc bị mua chuộc - đây là một vấn đề cụ thể khi các đánh giá tích cực có thể được mua gần như với giá bằng không. Để duy trì lợi ích lớn hơn, các nền tảng này tính một số lượng lớn chi phí trung gian thay vì tạo ra các dịch vụ du lịch tốt hơn cho các nhà cung cấp tài nguyên và người tiêu dùng.

(2) Du lịch thường lệ: Việc tìm kiếm các dịch vụ và trải nghiệm lối sống tin tưởng và phù hợp trong mỗi chuyến đi đòi hỏi bạn phải rà soát thông qua một loạt thông tin không liên quan, thường lạc hậu và đôi khi còn bị giả mạo bằng nhiều cách. Điều này rất tốn thời gian và nhức nhối. Làm cách nào để bạn tìm được thông tin phù hợp với những người như bạn và những người du lịch như bạn? Không chỉ là sự bất tiện - nghiên cứu cho thấy 56% khách du lịch muốn có thông tin cá nhân hóa hơn và liên quan hơn và 96% khách du lịch cảm thấy bức xúc với lượng thông tin áp đảo, trong khi 74% cảm thấy bị quấy rầy bởi những giờ trôi qua lãng phí cho việc nghiên cứu. Các phương pháp hiện có rất sai lệch , bắng nhắng & chủ quan- mô hình tìm kiếm và đánh giá rạn nứt.

(3) Hiệu suất blockchain: Công nghệ blockchain truyền thống hầu như là để giải quyết hệ thống tiền tệ; hiệu suất của nó thường không thể đáp ứng các kịch bản ứng dụng thực tế. Đại diện cho công nghệ là bitcoin thường chỉ hỗ trợ bảy giao dịch mỗi giây. ETH chỉ khoảng 25 giao dịch mỗi giây. Công nghệ blockchain truyền thống không thể hỗ trợ một thị trường du lịch toàn cầu lớn như vậy.

Theo quan điểm của các tính năng trên, sơ đồ đổi mới chính của nền tảng dịch vụ du lịch phân cấp dựa trên chuỗi công cộng InterValue như sau:

- **Hệ thống niềm tin** : Dựa trên công nghệ blockchain, chúng tôi bỏ qua sự khác biệt trung gian nền tảng để kết nối trực tiếp người tiêu dùng du lịch và nhà cung cấp tài nguyên du lịch. Từ các nhà hoạch định du lịch, hãng hàng không, chỗ ở khách sạn và đặt phòng, chúng tôi xây dựng một hệ sinh thái dịch vụ du lịch trong tương lai dựa trên ủy thác, ủy ban và số không. Dựa trên công nghệ hợp đồng thông minh, các nhà hoạch định du lịch, vé máy bay, chỗ ở khách sạn, vv được đặt với INVE. Các nhà cung cấp tài nguyên du lịch không phải trả bất kỳ khoản hoa hồng nào để giảm chi phí hoạt động của họ. Người dùng sẽ sử dụng giá thấp hơn để có được dịch vụ tốt hơn.
- **Thói quen du lịch**: InterValue kết hợp người dùng với những trải nghiệm và dịch vụ địa phương được cá nhân hóa tốt nhất được hỗ trợ bởi AI & Data Science độc quyền và được thúc đẩy bởi mật mã. Đó là không có ma trận - InterValue cắt giảm sự quấy rối, cho phép người dùng khám phá và đặt ngay các dịch vụ và trải nghiệm địa phương chất lượng cao phù hợp với sở thích của họ, người dùng có thể đặt hoặc đặt trước trực tiếp thông qua nền tảng. Ngoài ra, InterValue không dựa trên các đánh giá dài và chủ quan, thay vào đó tạo và quản lý việc ghi điểm và đại diện thực sự về trải nghiệm thông qua các giao dịch sử dụng công nghệ thông minh. InterValue tập trung rất nhiều vào việc cá nhân hóa và những người cùng lứa tuổi có sở thích và sở thích tương tự để làm cho thông tin và kết quả phù hợp nhất có thể. InterValue sử dụng nhiều lớp dữ liệu bao gồm bối cảnh, môi trường, hành vi và nhiều điểm dữ liệu khác để tạo ra một bức tranh hoàn chỉnh về "cuộc chiến". Khi hệ sinh thái phát triển InterValue sẽ mở ra nhiều hơn cho nhóm thuần tập người dùng được gọi là “Nhóm du lịch” để giới thiệu có chọn lọc và tận hưởng trải nghiệm cũng như tham gia và giúp xây dựng hệ sinh thái và cộng đồng InterValue.
- **Hiệu suất blockchain**: Du lịch chuỗi công cộng InterValue dựa trên công nghệ blockchain 3 và sử dụng thuật toán đồng thuận DAG để thực hiện giao dịch nhanh hơn và thích ứng với thị trường du lịch lớn trên thế giới. Du lịch chuỗi công cộng InterValue sử dụng hệ thống hợp đồng khai báo thông minh Turing không hoàn chỉnh. Các hợp đồng thông minh được tạo thành từ các câu lệnh

Boolean khai báo và đầy đủ, vì vậy nó gần gũi hơn với ngôn ngữ hợp pháp truyền thống, hỗ trợ các phép toán Boolean, các phép toán, lưu trữ dữ liệu và vân vân.

- InterValue đang tạo ra một mô hình kinh doanh mạnh mẽ, khuyến khích các nhà cung cấp và các nhà lãnh đạo ngành với các cơ sở khách hàng hiện có, tham gia vào mạng InterValue và thúc đẩy lưu lượng truy cập vào mạng. InterValue có thể xây dựng một mạng lưới gồm nhiều nhà cung cấp sẽ tham gia vào nền tảng này. Những nhà cung cấp này bao gồm tất cả mọi thứ mà khách du lịch sẽ muốn ở địa phương khi họ đang đi du lịch, ăn uống riêng, cuộc sống về đêm, trải nghiệm và hơn thế nữa. Các nhà cung cấp có thể cung cấp hàng hóa và dịch vụ của họ trên mạng lưới khách hàng trung thành của InterValue, lần lượt kiếm được INVE. InterValue tạo ra một giải pháp duy nhất cho thị trường du lịch dựa trên INVE - cách mạng hóa cách mọi người đặt trải nghiệm và sử dụng lòng tin. InterValue sẽ cho phép người dùng trao đổi lòng tin của họ trên nền tảng để giảm giá, hàng hóa và kinh nghiệm thực tế cũng như trao đổi lòng tin với những người dùng khác. Chúng tôi cho phép người dùng kiểm soát nhiều hơn sự tin tưởng của họ trong khi mang lại cho nhà cung cấp và thương hiệu cơ hội thu hút người dùng trên mọi bước hành trình của họ.

  InterValue sử dụng hệ thống "đánh giá độ thật", có nghĩa là chỉ những người đã giao dịch với nhà cung cấp hoặc tham gia vào hệ thống khách hàng trung thành với họ mới có thể cung cấp phản hồi. Điều này cho phép chúng tôi căn cứ đánh giá và phản hồi về các giao dịch thành công thực sự - không phải là các giả định, thông tin tiếp thị hoặc đánh giá được trả tiền. Phản hồi cũng được thực hiện theo cách thức theo ngữ cảnh xung quanh người dùng, nhà cung cấp và điều kiện. Phản hồi này xây dựng trên Blockchain không thay đổi, và sau đó được điều chỉnh bởi AI để hiểu được hình ảnh dữ liệu hoàn chỉnh. Điều này có nghĩa là các bài đánh giá ít có khả năng giả mạo hơn và nền tảng tăng độ tin cậy và duy trì dữ liệu được xác thực vững chắc, không giống như nhiều nền tảng hiện đang tồn tại. InterValue tạo ra một hệ thống danh tiếng định lượng để tổng hợp dữ liệu danh tiếng và báo cáo điểm tin cậy cho các nhà cung cấp. InterValue sẽ có thể sử dụng AI trên chuỗi để thu thập tình cảm và siêu dữ liệu để chỉ ra chính xác phản hồi có liên quan cho bên liên quan. Đối với các quỹ của các nhà cung cấp được phát hành cho mỗi một hợp đồng thông minh được viết bởi InterValue và các thông tin đăng nhập được gắn với một ID được lưu trữ trên Blockchain. Cả hai thực hiện một giao dịch và có khả năng trong các kết nối trong tương lai với hợp đồng thông minh sẽ phát hành các trình kích hoạt thanh toán. Điều này có nghĩa là phát hành các khoản thanh toán cho nhà cung cấp sẽ nhanh hơn và hiệu quả hơn nhiều, ngoài ra họ sẽ cung cấp mức độ hài lòng lớn hơn cho những người bán hàng và nhà cung cấp.

  Cuối cùng, InterValue đang trở thành một thị trường điểm đến "trọn gói" về du lịch vận hành bằng tiền điện tử. Chúng tôi có thể dễ dàng quản lý và tự động hóa một phần lớn tính khả dụng giữa tất cả các thị trường mà chúng tôi hoạt động với một cơ sở dữ liệu lớn được cập nhật trực tiếp với tất cả tính sẵn có của nó. Việc phân cấp niềm tin của chúng tôi cho phép quy mô và khả năng mang lại quyền sở hữu và khả năng kiếm điểm trung thành cho người dùng trong khi tạo các cách mới cho thương hiệu, nhà cung cấp và công ty có thể thu hút sự trung thành của khách hàng.

  Sức mạnh đằng sau InterValue là mã token INVE. Tất cả các hoạt động trong mạng xoay quanh INVE, từ hình thức khởi thủy là sử dụng làm phí và tài sản đảm bảo, là tiền tệ chính được sử dụng để mua những trải nghiệm, hàng hóa và dịch vụ, dự đoán và thưởng cho lòng trung thành.

INVE là người điều hướng của một nền kinh tế bền vững, khi mà nhu cầu tăng lên khi nhiều người dùng và nhà cung cấp tham gia vào hệ sinh thái.

9.2.4. Giao dịch cổ tức tài sản BlockChain

Dựa trên công nghệ blockchain, chúng tôi sẽ hiện thực hóa hệ sinh thái blockchain về giao dịch cổ tức tài sản. Chúng tôi cung cấp một nền tảng giao dịch an toàn và thuận tiện cho các tài sản, cho phép chủ sở hữu tài sản huy động vốn thông qua tài sản. Mua tài sản để đạt được hoặc tăng thêm giá trị cho các tài sản có tiền thưởng.

Các nhà quá trình đào hệ thống cung cấp sự thẩm định về giá trị tài sản, tính hợp pháp và tính sinh lợi của toàn bộ hệ thống, và hiện thực hóa giao dịch quyền lợi cổ tức thông qua việc tạo gói, niêm yết và tạo chuỗi các tài sản chất lượng cao. Chúng tôi sử dụng blockchain để phát hành tiền tệ kỹ thuật số cho giao dịch tài sản. Giao dịch có thể được thực hiện giữa chủ sở hữu tài sản và nhà đầu tư tài sản hoặc giữa các nhà đầu tư.

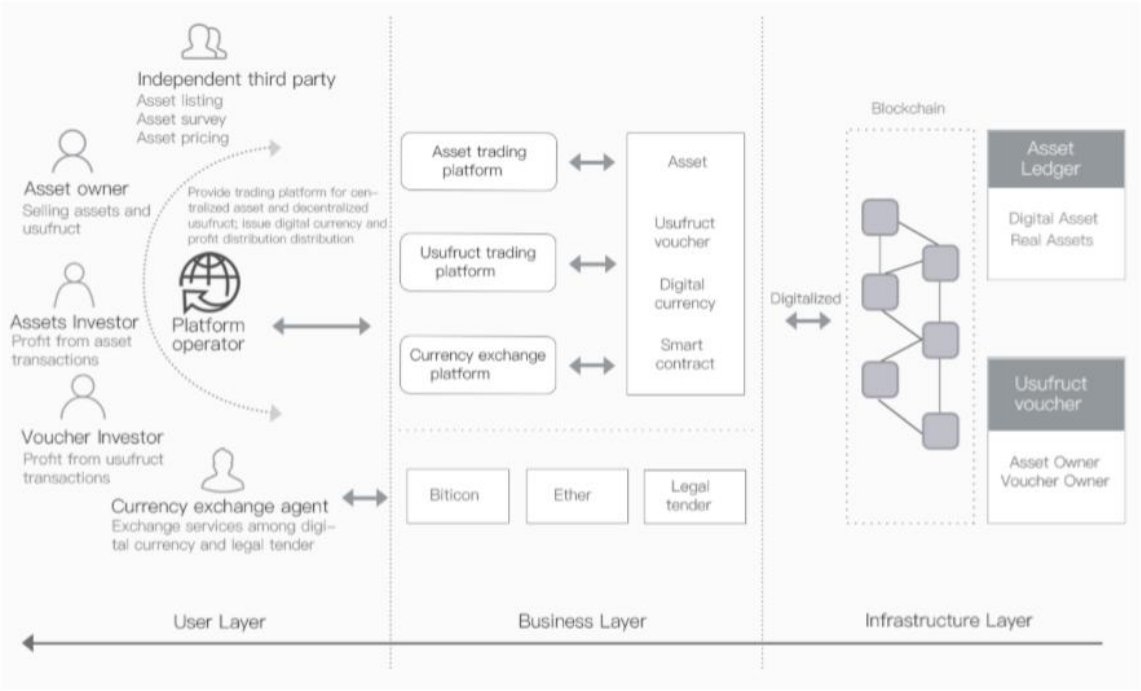


Figure 9–2: The Ecological of Asset Transactions

- **Phân chia vai trò** :
  - Chủ sở hữu tài sản: niêm yết tài sản và bán tài sản để gây quỹ. Sau khi tài sản được niêm yết, các quy tắc thưởng tương ứng sẽ được công bố. Sau khi tài sản được bán, nó tương đương với việc ký hợp đồng thông minh của hai bên theo các quy tắc, và thúc đẩy thực hiện tự động khi điều kiện được kích hoạt
  - Cơ quan niêm yết: tương đương với người làm thị trường, tài sản của chủ sở hữu phải được niêm yêt trên chuỗi tài sản để thực hiện thẩm định, để giải phóng lợi nhuận và giá trị tài sản. Họ có chiết khấu các giao dịch tài sản thấp hơn để hỗ trợ quá trình nghiên cứu.

- Blockchain tài sản: thông tin về blockchain không thể được thao tác. Các hợp đồng thông minh được thực hiện để chia cổ tức tài sản và giao dịch tài sản
- Nhà đầu tư tài sản: họ sử dụng vốn nhàn rỗi để đầu tư vào tài sản để thu được cổ tức hoặc lợi nhuận bằng cách tăng giá tài sản.
- Thợ mỏ: họ cung cấp tài nguyên máy tính và lưu trữ cho các ưu đãi tiền tệ kỹ thuật số
- Nhà đầu tư tiền tệ kỹ thuật số: họ kiếm tiền bằng cách tích trữ và giao dịch tiền tệ kỹ thuật số
- Nền tảng giao dịch tiền tệ kỹ thuật số: họ cung cấp trung gian cho các giao dịch tiền tệ kỹ thuật số để hiện thực hóa các loại tiền kỹ thuật số.

- Hợp đồng thông minh :

Chúng tôi sử dụng một ngôn ngữ cấp cao Turing hoàn chỉnh như một biện pháp thực thi hợp đồng thông minh, hỗ trợ việc thực thi và xác minh nội dung hợp đồng của cả hai bên. Chúng tôi nhanh chóng xác định và thử nghiệm các hợp đồng thông minh trong môi trường phát triển các ngôn ngữ nâng cao. Bytecode được biên dịch bởi một ngôn ngữ cấp cao cũng có thể được mã hóa ở một mức độ nhất định cho các hợp đồng thông minh. Việc thực thi hợp đồng đòi hỏi môi trường ngôn ngữ tiên tiến. Chỉ bằng cách sử dụng chuỗi lưu trữ khối và xác minh thông minh của hợp đồng, hợp đồng được thực thi bởi các hợp đồng blockchain trong máy chủ proxy đến máy chủ proxy, sau khi xác minh hợp đồng như một nút blockchain dành cho các đại lý thông minh và cung cấp môi trường thực thi hợp đồng. hợp đồng chỉ là mã đạt được. Máy chủ proxy nhận dữ liệu bên ngoài và truyền dữ liệu đến mã hợp đồng tải động hoặc chạy mã hợp đồng theo nút thời gian do chính hợp đồng cung cấp và hợp đồng có thể truy cập dữ liệu công khai bên ngoài trong quá trình hoạt động. Trong hệ thống giao dịch tài sản, hợp đồng thông minh cũng cung cấp cho các khoản đầu tư tài sản trước khi giao dịch và chủ sở hữu tài sản ký hợp đồng thông minh. Khoản đầu tư có quyền từ chối bán tài sản cho chủ tài sản.

Quy trình giao dịch tài sản :

Giải pháp giao dịch tài sản dựa trên blockchain có thể lưu trữ dữ liệu người dùng và dữ liệu giao dịch trong thị trường giao dịch tài sản, để giải quyết các vấn đề mà không cần có 1 trung tâm, giao dịch minh bạch và sự tin tưởng và vân vân.

Chia sẻ quy trình thưởng

Blockchain thông qua hợp đồng thông minh để giải quyết vấn đề cổ tức tự động. Khi các thông số tài sản phù hợp với điều kiện cổ tức, phần tài sản trong tài khoản của chủ sở hữu tài sản được phân bổ vào tài khoản của nhà đầu tư tài sản như cổ tức

10

Thông tin liên lạc chuỗi chéo và hợp nhất đa chuỗi

10.1. Giới thiệu về công nghệ chuỗi chéo

Các dự án Blockchain hiện tại không thể đáp ứng cho các ứng dụng thương mại một cách hiệu quả. Một lý do là khả năng của Blockchain bị giới hạn và tốc độ xác nhận giao dịch rất chậm, và 1 lý do quan trọng khác là thực tế mỗi dự án Blockchain đơn thuần chỉ là một mạng giá trị bị cô lập. Vấn đề mạng bị cô lập như thế sẽ cực kỳ hạn chế tiềm năng của công nghệ blockchain, vì tương tác giữa các dự án blockchain hiện có rất khó triển khai. Là một dự án Blockchain nhằm kết nối giá trị, InterValue muốn hiện thực hóa không chỉ kết nối giá trị giữa người dùng mà còn cả kết nối giá trị giữa các dự án blockchain hiện có. Mục tiêu của InterValue là thay đổi tình trạng độc lập ở các dự án Blockchain và cuối cùng là hiện thực hóa kết nối giá trị rộng khắp.

Giao tiếp chéo chuỗi đang trở thành một chủ đề nóng trong nghiên cứu Blockchain. Hiện đang có ba công nghệ xuyên chuỗi: các chương trình công chứng Notary scheme, sidechain / chuyển tiếp và hash-locking. Trong chương trình công chứng, một nhóm các nút đáng tin cậy đóng vai trò là công chứng viên để xác minh xem một sự kiện cụ thể đã xảy ra trên Blockchain Y và chứng minh nó với các nút của Blockchain X. Interledger được đề xuất bởi Ripple Lab là một đại diện của chương trình công chứng. Nếu Blockchain X cho phép xác minh dữ liệu đến từ Blockchain Y, Blockchain X được gọi là sidechain. Sidechains thường dựa vào các token được neo trên một blockchain nhất định, trong khi các Blockchains khác có thể tồn tại độc lập. Các dự án sidechain hiện tại không thể xây dựng hợp đồng thông minh xuyên suốt và hỗ trợ tất cả các loại chức năng tài chính, đó là lý do mà các dự án Blockchain không có được ưu thế trong các thị trường chứng khoán, trái phiếu và tài chính. Các bitcoin-sidechains nổi tiếng bao gồm BTC Relay (được đề xuất bởi ConsenSys), Rootstock và ElementChain (được đề xuất bởi BlockStream), và

các sidechains khác, không phải dành cho Bitcoin, gồm Lisk và Asch. Công nghệ chuỗi chuyển tiếp tạm thời khóa một lượng token của Blockchain gốc bằng cách chuyển chúng đến địa chỉ đa chữ ký của Blockchain gốc và những người ký này bỏ phiếu để xác định xem các giao dịch xảy ra trên chuỗi chuyển tiếp có hợp lệ hay không. Polkadot và COSMOS là các công nghệ chuỗi chuyển tiếp đại diện. Hash-locking là một cơ chế để thực hiện thanh toán bằng cách khóa một thời gian để đoán đoạn plaintext của giá trị băm, có nguồn gốc từ Lightening Networks. Tuy nhiên, khóa băm giới hạn hỗ trợ một số chức năng. Mặc dù nó hỗ trợ trao đổi tài sản chéo và chuỗi tài sản chéo trong hầu hết các kịch bản, nó không thể sử dụng cho di động tài sản chuỗi chéo và hợp đồng thông minh xuyên chuỗi. So sánh ba công nghệ xuyên chuỗi này được thể hiện trong Bảng 10-1.

Table 10–1: The comparison of cross–chain technologies

Cross-chain technique	Notary schemes	Sidechain/Relays	Hash-locking
Interoperability types	ALL	ALL (If relays exist on both chains; otherwise one-way causality only)	Cross-dependency only
Trust model	Majority of notaries honest	Chains do not fail or get "51% attacked"	Chains do not fail or get "51% attacked"
Usable for cross-chain exchange	YES	YES	YES
Usable for cross-chain asset portability	YES (but requires universal long-term notary trust)	YES	NO
Usable for cross-chain oracles	YES	YES	Not directly
Usable for cross-chain asset encumbrance	YES (but requires long-term notary trust)	YES	In many cases, but with difficulty

10.2. Bộ điều biến nút đầy đủ Hợp nhất đa chuỗi

Các dự án hiện tại tập trung vào việc làm thế nào để cải thiện giao dịch thông qua thông lượng và tốc độ, nhưng lại bỏ qua vấn đề bị khóa kín trong 1 nền tảng. Ví dụ, Alice và Bob đã cài đặt ứng dụng máy khách bitcoin, và họ chỉ có thể chuyển bitcoin bên trong Blockchain bitcoin. Nếu họ muốn chuyển giao eth, ứng dụng khách hàng eth cần phải được cài đặt cho cả Alice và Bob. Vấn đề khóa trong nền tảng này gây ra sự bất tiện trong chuyển đổi giữa các chuỗi khác nhau, tác động đến trải nghiệm người dùng. Bên cạnh đó, để sử dụng đồng thời nhiều chuỗi công cộng, người dùng cần trang bị cho các máy chủ có bộ nhớ và dung lượng cao, tốn nhiều tiền.

InterValue sử dụng kỹ thuật kết hợp đa chuỗi toàn bộ bộ điều hợp nút để kết nối các Blockchains khác nhau. Cụ thể, khi lối vào thống nhất, InterValue sử dụng nút kết hợp bộ điều hợp đầy đủ để kích hoạt

các giao dịch trên mạng con bên ngoài (BTC, ETH). Mạng nút đầy đủ cục bộ bao gồm một mạng con bên ngoài và một mạng con bên trong. Mạng con bên ngoài chủ yếu bao gồm các mạng chuỗi khác, chẳng hạn như BTC, ETH và vân vân. Mạng con nội bộ chủ yếu bao gồm mạng thành viên của InterValue. Mạng cấp cao chủ yếu bao gồm các nút cao hơn của tất cả các nút còn lại.

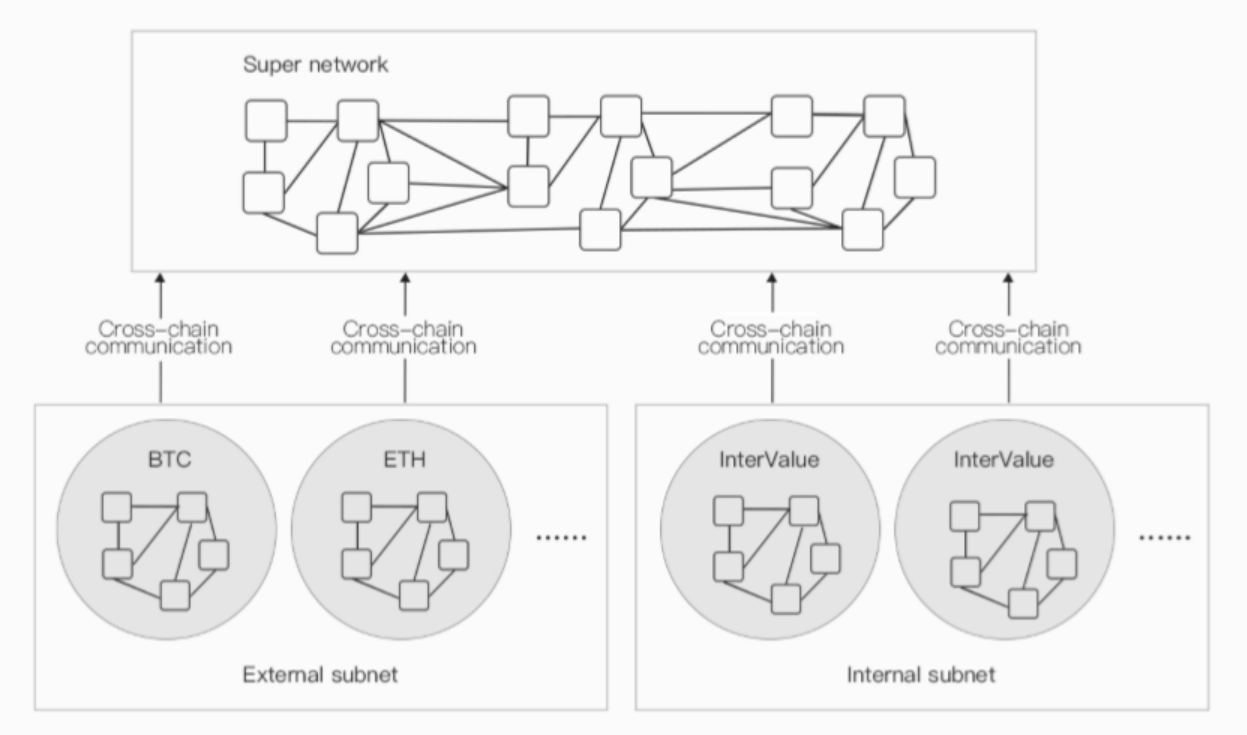


Figure 10-1: Full-node Adapter Multi-chain Merging

Chúng tôi triển khai mô-đun hợp nhất nhiều chuỗi vào trong nút đầy đủ, hoạt động như proxy giao dịch trên mạng con bên ngoài (BTC, ETH). Trong giai đoạn đầu, InterValue sẽ hỗ trợ giao dịch proxy giữa Bitcoin và Ethereum. Lấy giao dịch proxy Bitcion làm ví dụ, thông tin giao dịch được hiển thị như sau:

```
["cross chain transaction", [
   ["InterValue", ["Alice","Bob"]],
   "targetchain": "BITCOIN",
   "txproxy":{
   "txid":"TRANSACTION HASH IDNEX",
   "version":1,
   "locktime":0,
   "vin":[
      {"txid":"UTXO HSAH INDEX",
      "vout":0,
      "scriptSig":{"asm":"ASM STRING VALUE"
                   "hex":"HEX STRING VALUE":
                   },
      "sequece": SEQUENCE VALUE,
      }
   ],
   "vout":[
      {"value":0.5,
      "n":0,
      "scriptPubKey":{"asm":"SCRIPT CODE",
                      "hex":"HEX STRING VALUE",
                      "reqSigs":1,

                                  "type":"pubkeyhash",
                                  addresses:[  "Bob"]
                                  }
         },
      ....
      ]
]]
```

Nếu chúng ta muốn hỗ trợ giao dịch proxy của Ethereum, điều duy nhất cần làm là thay đổi miền txproxy. Lưu ý rằng, để thực hiện hợp nhất nhiều chuỗi, người dùng InterValue phải đăng ký tài khoản trên các chuỗi công cộng khác. Khi người dùng muốn giao dịch trong các chuỗi khác, họ chọn chuỗi mục tiêu, nhập giá trị giao dịch và khởi chạy giao dịch proxy. Sau khi giao dịch proxy được trao đổi trong InterValue, nút đầy đủ có được giao dịch này, trích xuất thông tin từ miền txproxy, phát tán giao dịch trong chuỗi mục tiêu. Do đó, InterValue hoàn tất giao dịch proxy và đạt được sự hợp nhất nhiều chuỗi.

10.3. Giao tiếp chéo

InterValue không chỉ là một mạng Blockchain khép kín mà còn là cầu nối để hỗ trợ các chức năng giao tiếp xuyên chuỗi, chẳng hạn như trao đổi tài sản qua chuỗi và chuyển đổi tài sản qua nhiều chuỗi. Bằng cách sử dụng nền tảng InterValue, bất kỳ ai cũng có thể phát triển các ứng dụng tài chính phù hợp với các yêu cầu kịch bản ứng dụng. Ý tưởng cơ bản của công nghệ xuyên chuỗi InterValue là áp dụng các ý tưởng chuỗi chuyển tiếp và thực hiện mô-đun truyền thông xuyên suốt như là một phân lớp các nút đầy đủ phủ bên trên chuỗi cơ bản của InterValue. Trong lộ trình công nghệ này, chúng tôi không chỉ duy trì sự độc lập về khả năng tương tác chéo chuỗi mà còn sử dụng lại tất cả các chức năng được cung cấp bởi chuỗi cơ bản InterValue.

Module truyền thông xuyên suốt của InterValue bao gồm ba loại nút: nút xác minh, nút nhận biết khối và nút kết hợp. Các chức năng tương ứng của chúng được liệt kê dưới đây:

- Các nút xác minh là các nút công chứng trong chuỗi cơ bản của InterValue. Họ xác minh tính hợp lệ của dữ liệu đến từ một số Blockchain gốc và xây dựng các khối mới trong InterValue. Các nút xác minh phải thế chấp đủ tài sản để đảm bảo rằng họ sẽ thực hiện công việc của mình
- Các nút nhận biết khối giúp các nút xác minh thu thập khối truyền thông chéo hợp lệ. Các nút này, tương tự như các trình quá trình đào trong PoW, chạy một máy khách đầy đủ của một số Blockchain gốc, xây dựng các khối mới và thực hiện các giao dịch. Sau khi nhận được khối yêu cầu giao dịch chéo, các nút nhận biết khối đóng gói các khối yêu cầu này và gửi chúng đến các nút xác minh.
- Các nút hợp nhất hoạt động giống như cổng vào giữa InterValue và các Blockchains gốc khác. Mỗi nút hợp nhất có hai hàng đợi tương ứng với các giao dịch gửi đến và các giao dịch gửi đi. Ngoài ra, các nút sáp nhập phải có một số mã của Blockchains gốc và hỗ trợ oracle chuỗi chéo.

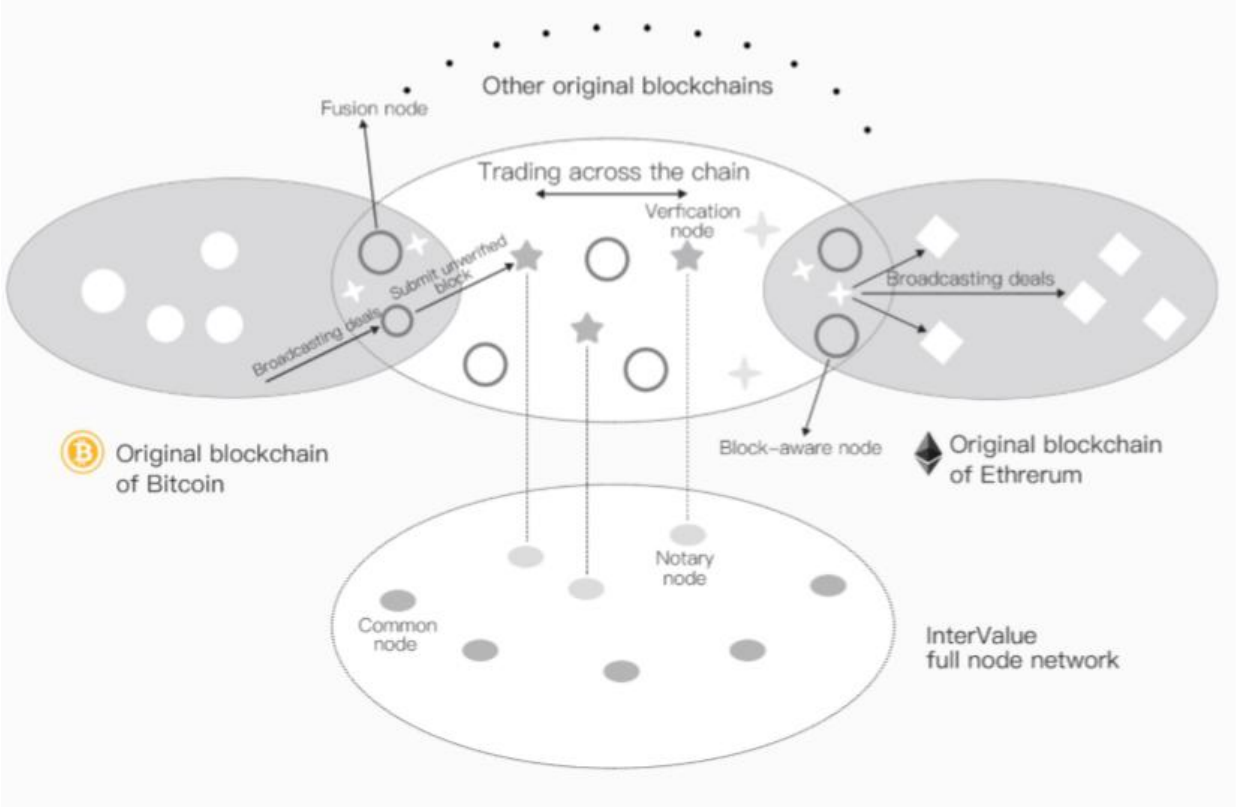


Figure 10–2: InterValue Cross–chain Technology

10.4. Trao đổi tài sản xuyên chuỗi

Để giải thích rõ ràng quá trình trao đổi tài sản xuyên chuỗi, chúng tôi lấy sự trao đổi giữa Bitcoin và Ethereum làm ví dụ. Giả sử Alice muốn chuyển đổi 1 BTC thành 10 ETH. Trong khi đó, Bob muốn chuyển đổi 10 ETH thành 1 BTC. Việc trao đổi tài sản giữa Alice và Bob được thể hiện như sau:

(1) Alice gửi 1 BTC của cô đến một tài khoản multisig của chuỗi chuyển tiếp InterValue.

(2) Nút nhận biết khối của chuỗi bitcoin chịu trách nhiệm giám sát truyền thông chéo. Sau khi nút nhận biết khối nắm bắt khối chứa giao dịch của Alice, nó đóng gói tiêu đề khối tới khối chưa được đánh dấu mới và gửi khối mới đến nút xác minh.
(3) Sau khi nút xác nhận nhận được khối mới, nó kiểm tra xem khối đã được cam kết bởi chuỗi bitcoin hay chưa. Nếu có, nút xác minh sẽ tạo một hợp đồng mới và ghi nó vào chuỗi chuyển tiếp InterValue.
(4) Bob gửi 10 ETH của mình đến một tài khoản multisig của chuỗi chuyển tiếp InterValue
(5) Nút nhận biết khối của chuỗi Ethereum chụp lại khối chứa giao dịch của Bob. Sau đó, nó gói tiêu đề khối vào khối chưa được đánh dấu mới và gửi khối mới đến nút xác minh.
(6) Sau khi nút xác nhận nhận được khối mới, nó kiểm tra xem khối đã được cam kết bởi chuỗi bitcoin hay chưa. Nếu có, nút xác minh sẽ tạo một hợp đồng mới và ghi nó vào chuỗi tiếp sức của InterValue. Trong khi đó, nút xác minh sẽ kiểm tra xem có yêu cầu trùng khớp với Bob hay không và yêu cầu của Alice.
(7) Nút xác minh tạo hai hợp đồng mới. Một là “gửi 1 BTC tới tài khoản BTC của Bob. Người kia là "gửi 10 ETH đến tài khoản eth của Alice". Hai hợp đồng được gửi đến hàng đợi của nút hợp nhất của chuỗi bitcoin và chuỗi Ethereum, tương ứng.
(8) Nút kết hợp của chuỗi bitcoin và chuỗi Ethereum đọc hàng đợi tương ứng của chúng, và gửi 1 BTC và 10 ETH cho Bob và Alice, tương ứng. Do đó, việc trao đổi tài sản xuyên chuỗi hoàn tất.

10.5. Chuyển giao tài sản xuyên chuỗi

Để giải thích rõ ràng quá trình chuyển giao tài sản xuyên chuỗi, chúng tôi lấy chuyển giao từ bitcoin sang Ethereum làm một ví dụ. Giả sử Alice muốn chuyển 1 BTC sang tài khoản eth của Bob. Chuyển giao tài sản từ Alice sang Bob được thể hiện như sau:

(1) Alice gửi 1 BTC tới nút hợp nhất của chuỗi chuyển tiếp InterValue.
(2) Nút nhận biết khối của chuỗi bitcoin chụp lại khối chứa giao dịch của Alice, nó gói tiêu đề khối vào khối chưa được đánh dấu mới và gửi khối mới tới nút xác minh.
(3) Sau khi nút xác nhận nhận được khối mới, nó thay đổi khối chứa giao dịch của Alice đã được cam kết bởi chuỗi bitcoin
(4) Dựa trên oracle chuỗi chéo, nút sáp nhập của chuỗi bitcoin trao đổi 1 BTC với lượng INVE tương ứng. Sau đó, nút sáp nhập của chuỗi bitcoin sẽ gửi INVE đến nút kết hợp của chuỗi Ethereum thông qua chuỗi InterValue.
(5) Nút xác nhận của InterValue thay đổi giao dịch giữa nút sáp nhập của chuỗi bitcoin và nút sáp nhập của chuỗi Ethereum.
(6) Dựa trên oracle cross-chain, nút kết hợp của chuỗi Ethereum trao đổi token INVE nhận được với token ETH tương ứng và gửi token ETH cho Bob.

11

Đội ngũ và chiến lược

11.1. Đội ngũ sáng lập

InterValue Foundation là một tổ chức phi chính phủ. Thông qua việc thành lập các phòng ban liên quan, Ban sáng lập cam kết phát triển InterValue và quản lý nguồn mở, xây dựng cộng đồng và thảo luận cải tiến InterValue. Hơn nữa, để làm cho dự án hoạt động tốt hơn, Ban sáng lập cũng cam kết xây dựng đội ngũ nhân viên và quan hệ đối ngoại.

Cấu trúc tổ chức của InterValue Foundation được thể hiện trong Hình 11-1.

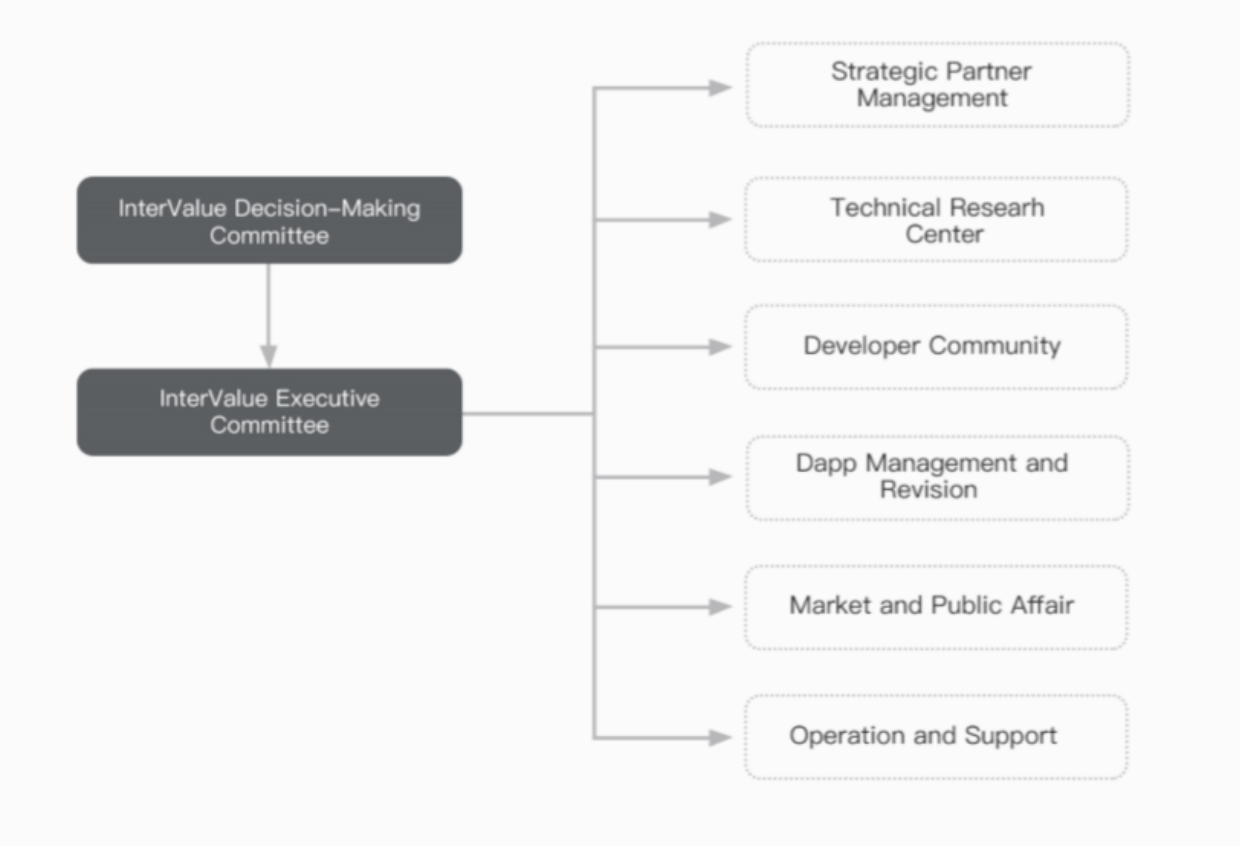


Figure 11-1: The Organization Structure of InterValue Foundation

Ban điều quyết InterValue (InterValue Decision-Making Committee): chịu trách nhiệm quản lý và ra quyết định các vấn đề chính, bao gồm phát triển các hướng chiến lược quan trọng của InterValue, bổ nhiệm và miễn nhiệm các thành viên ủy ban điều hành, bầu lãnh đạo Ban điều hành và người đứng đầu các phòng ban. Các thành viên của ban này được bổ nhiệm trong thời hạn ba năm và có thể được bầu lại, và Ban sẽ có một chủ tịch. Các thành viên đầu tiên của ủy ban ra quyết định sẽ được bỏ phiếu bởi nhóm sáng lập InterValue và các đại diện ủy ban, trong đó có luân chuyển hàng năm.

Ban điều hành InterValue (InterValue Executive Committee): chịu trách nhiệm quản lý công việc của từng bộ phận, chẳng hạn như xây dựng nền tảng mở mạng lưới tiêu thụ, quy tắc giám sát, phân tích mục tiêu của ủy ban ra quyết định, thực hiện và giám sát công việc của từng bộ phận. Trách nhiệm cụ thể của ban điều hành InterValue được thể hiện như sau:

- **Quản lý đối tác chiến lược**(Strategic Partner Management): Quản lý đối tác chiến lược và điều phối tài nguyên đối tác
- **Trung tâm nghiên cứu kỹ thuật (Technical Research Center)**: Chịu trách nhiệm phát triển các giao thức công nghệ cơ bản, thiết kế và phát triển hệ thống blockchain, kiểm tra, lặp lại, phát triển các tiêu chuẩn, v.v.

- **Cộng đồng nhà phát triển (Developer Community):** Cung cấp cho nhà phát triển giáo dục, đào tạo, hỗ trợ kỹ thuật và các dịch vụ khác. Đồng thời, nó chạy cộng đồng để cung cấp một nền tảng cho phát triển và truyền thông.
- **Quản lý và Kiểm toán Dapp (DApp Management and Audit):** Chịu trách nhiệm kiểm tra tất cả các DApp đã tham gia InterValue để đảm bảo tuân thủ DApp trên nền tảng InterValue, có lợi cho nền tảng hệ sinh thái y tế
- **Thị trường và các vấn đề công cộng (Market and Public Aairs)**: Bao gồm phát triển thị trường, người dùng nuôi dưỡng và quản lý các vấn đề công
- **Hoạt động và Hỗ trợ(Operation and Support)**: Bao gồm quản lý thêm bốn phòng ban, chẳng hạn như nhân sự, pháp lý, nhân sự và các phòng ban hành chính. Bộ phận tài chính chịu trách nhiệm về việc sử dụng và xem xét tài liệu, hội thảo pháp lý chịu trách nhiệm tuân thủ của nền tảng, cũng như chuẩn bị và xem xét các tài liệu khác nhau, để ngăn chặn các loại rủi ro pháp lý khác nhau. tiền lương và công tác hành chính hàng ngày.

11.2. Thành viên nhóm phát triển

Đối với các thành viên mới gia nhập nhóm sau này, chúng tôi sẽ cập nhật danh sách bên dưới.

 Barton Chao	Giám đốc điều hành, phó giám đốc Xidian University blockchain ứng dụng và phòng thí nghiệm kiểm tra, nhà nghiên cứu nổi tiếng của Trung tâm nghiên cứu blockchain Đại học Chiết Giang. Học viên ngành công nghiệp Blockchain, Tiến sĩ, chuyên gia cao cấp về P2P, mật mã, an ninh mạng và Blockchain. Ông là một nhà phát triển tiên phong của Blockchain từ năm 2009. Công việc chính của ông bao gồm nghiên cứu các công nghệ cơ bản của Blockchain, kết hợp blockchain với ngành công nghiệp và áp dụng công nghệ Blockchain trong bối cảnh ứng dụng thực tế. Kể từ khi ông đã lên kế hoạch và phát triển một số dự án liên quan đến Blockchain, ông có hiểu biết sâu sắc và kinh nghiệm thực tế phong phú của nguyên tắc kỹ thuật của blockchain, công nghệ cơ bản, giao thức tầng giữa, ứng dụng trên chuỗi, cảnh ứng dụng, xu hướng phát triển và v.v.

 Leo Cheung	CTO, Tiến sĩ, học giả của Đại học Khoa học & Công nghệ Hồng Kông. Lĩnh vực nghiên cứu chính của ông là tính toán P2P, quản lý dữ liệu lớn, phân tích thông minh, học tập sâu và vv. Ông đã xuất bản hơn 30 bài báo cấp cao, 4 chuyên khảo và đã dẫn đầu và tham gia 10 dự án nghiên cứu khoa học cấp cao. Ông đã tham gia vào thiết kế cấu trúc của hệ thống P2P và có hiểu biết sâu sắc về cấu trúc lớp kép của cấu trúc liên kết P2P.
 Roger Max	Kiến trúc sư trưởng, Tiến sĩ, được dành riêng cho máy tính phân tán, điện toán đám mây và học máy. Anh ấy đã xuất bản hơn 20 giấy tờ cấp cao trong và ngoài nước. Trong lĩnh vực tính toán phân tán, ông có một sự hiểu biết sâu sắc về khả năng mở rộng, độ tin cậy và độ đàn hồi của các hệ thống phân tán. Trong lĩnh vực blockchain, ông có một sự hiểu biết sâu sắc và kinh nghiệm thực tế cho nguyên tắc và công nghệ blockchain.
 Andy Tang	InterValue Eco Construction Leader, Ph.D., hướng nghiên cứu chính về học máy, xử lý thông tin thông minh, hệ thống thông tin, đã xuất bản hơn 10 bài báo. Từ lâu nó đã được tham gia vào các hệ thống thông tin quy mô lớn và phát triển ứng dụng phân tán, và có kinh nghiệm phong phú về sản phẩm và thiết kế hệ thống phức tạp. Từ năm 2015, ông đã tham gia vào công nghệ BlockChain và ứng dụng liên quan đến BlockChain, và có một sự hiểu biết sâu sắc về hệ sinh thái blockchain.

 Storm Zhang	Thạc sĩ kỹ thuật, lập trình viên cao cấp, chuyên gia công nghệ Blockchain. Ông đã làm việc trong Bộ phận cổng nghệ hệ thống của IBM và Sở dữ liệu lớn của Sina trong nhiều năm, và có trải nghiệm phát triển Hadoop và Map Reduce mở rộng. ông đã tiếp xúc với Bitcoin từ năm 2013, và ông đã quen thuộc với nguyên tắc cryptocurrency và chương trình docking cửa hàng cho Exchange Wallet. Ông là giám đốc kỹ thuật Go của Renrenbao. Hiện tại, ông đang tập trung vào sự chỉ đạo của các hợp đồng thông minh và các ứng dụng Blockchain.

 Scott Guo	COO, Ông làm việc cho VIEDA, Red Net, Alibaba và Tencent làm Giám đốc tiếp thị. 14 năm kinh nghiệm trong hoạt động sản phẩm và dịch vụ Internet. Trong mười năm qua, đã được cam kết với Internet và dữ liệu lớn và trí thông minh trong lĩnh vực nghiên cứu và ứng dụng. Trong 10 năm qua, anh ta đã phụ trách và tham gia vào các dự án phát triển hệ thống quy mô lớn như chính phủ và các doanh nghiệp lớn. Ông có chính phủ mạnh mẽ và kinh nghiệm hợp tác và dịch vụ doanh nghiệp lớn. Ông chịu trách nhiệm về tổ chức bộ phận kế hoạch và tiếp thị thương hiệu tổng thể của công ty. Ông có kỹ năng nắm bắt các cơ hội thị trường, duy trì độ nhạy thị trường, triển khai hợp lý các mối quan hệ nội bộ và bên ngoài. Ông chịu trách nhiệm xây dựng, kiểm soát, điều chỉnh và sửa đổi các chiến lược. Căn cứ vào vị trí thương hiệu và đặc điểm công nghiệp của công ty, Ông đề xuất một phương pháp hợp tác sáng tạo khác với mô hình truyền thống và cuối cùng thực hiện nó một cách hợp lý và hiệu quả.
 Isda Chen	Lãnh đạo Quan hệ Nhà đầu tư, Thạc sĩ. Làm việc cho AVIC International Holding và Youe Data là đại diện của công ty cả ở nước ngoài và trong nước. Xây dựng kết nối với chính quyền địa phương và phát triển thị trường. Phát triển và thực hiện một số dự án của chính phủ. Gần đây, dành riêng cho ngành công nghiệp Big Data và Blockchain. Với tầm nhìn quốc tế và kinh nghiệm sâu sắc trong hợp tác chính phủ.

11.3. Cố vấn Dự án

Danh sách cố vấn dự án sẽ được cập nhật liên tục

 Allen Wu	Ông Wu đã tích lũy được nhiều kinh nghiệm trong phát triển sản phẩm phần mềm, nghiên cứu và phát triển công nghệ và quản lý đội ngũ. Ông từng là một trong những nhà lãnh đạo chính của Ủy ban Công nghệ Sản phẩm của Tập đoàn Alibaba và Kiến trúc sư trưởng của Yahoo Trung Quốc. Trước đó, ông đã tham gia lãnh đạo một số phần mềm hệ thống, thương mại điện tử và các dự án Internet di động tại IBM, Silicon Valley và Tổng công ty Internet Bắc Kinh. Đồng thời, ông cũng là một chuyên gia cao cấp trong các thuật toán thông minh nhân tạo, NPL, và cơ sở dữ liệu phân tán.

Daxue Li

Ông Li có sự hiểu biết độc đáo và kinh nghiệm hiệu quả về công nghệ và hoạt động của Internet. Các chuyên gia thiết kế kiến trúc kỹ thuật và quản lý đội ngũ kỹ thuật. Ông gia nhập hệ thống nghiên cứu và phát triển kỹ thuật của JingDong trong năm 2008 và để cho doanh nghiệp của JingDong đạt được thời gian tăng trưởng gấp 10.000 lần theo sự phát triển của công nghệ. Năm 2015, ông thành lập công nghệ kỹ thuật số Magcloud, cho phép công ty trở thành một công ty hợp tác công nghệ với cốt lõi của blockchain, và trở thành một nhà lãnh đạo ngành công nghiệp một cách nhanh chóng.

Năm 2005, ông được Hội đồng Nhà nước tặng thưởng là “Công nhân mẫu quốc gia”; Vào năm 2012, ông được vinh danh là “Con số hàng đầu của Zhongguancun”; Năm 2014, ông được vinh danh là “CTO nổi tiếng nhất năm 2014”; Năm 2016, ông được chọn “Quy trình công nghiệp dữ liệu lớn hàng đầu Trung Quốc 100”; và vinh danh "Lãnh đạo kỹ thuật nhất" của China Internet Weekly vào năm 2017.

Xinwen Jiang

Giáo sư tại Khoa Khoa học Máy tính thuộc Đại học Quốc gia về Công nghệ Quốc phòng (Trung Quốc) và tại Khoa Kỹ thuật Máy tính của Đại học Tương Đàm (Trung Quốc). Nghiên cứu của ông chủ yếu tập trung vào tính toán phức tạp và thuật toán mã hóa. Ông đã chủ trì Quỹ khoa học quốc gia của Trung Quốc cũng như các tổ chức cấp quốc gia khác và đã tham gia vào hơn 10 dự án khoa học cấp quốc gia. Ông đã giành được một giải thưởng, hai giải nhì, và một giải ba tại Bộ Khoa học và Công nghệ Trung Quốc, đã xuất bản hai cuốn sách, một luận án và hơn 40 bài nghiên cứu trên các tạp chí khoa học. Tác phẩm của ông về vấn đề cơ bản và phức tạp nhất trong mật mã, “P so với NP”, mang lại một số tiến bộ và nhận được rất nhiều sự chú ý.

Các bài giảng dài hạn của ông bao gồm, trong số những thứ khác, “Tính phức tạp”, “Mật mã ứng dụng”, “Logic toán học”, “Thiết kế và phân tích thuật toán”. Song song với việc giảng dạy, ông đã khám phá thực tiễn xây dựng kỷ luật và lý thuyết về các nguyên tắc giáo dục, nhận được giải thưởng cho những thành tựu của ông ở cấp quốc gia. Ông đã xuất bản gần 10 tài liệu nghiên cứu về giảng dạy trong các tạp chí như Giáo dục máy tính. Ông đã nhận được giải thưởng Tài năng Quân sự hai lần.

 Zhiqi Han	Ông Han là thành viên của Hiệp hội Doanh nhân trẻ Bắc Kinh, UCSI MBA. Ông thành lập Stanley Ventures vào năm 2007 và đã phục vụ nhiều công ty Internet quy mô lớn trong nước, như Sohu, Sina và Fenzong. Anh ấy đã giúp hoàn thành nhiều vụ sáp nhập và mua lại. Là một trong những tổ chức FA sớm nhất ở Trung Quốc, ông đã tiếp tục phục vụ cho một số công ty Internet, chẳng hạn như Du lịch Tuniu, Nha khoa Jiamei, Bảo vệ Môi trường Lvchuang, vv và tổng số tiền vượt quá 100 triệu đô la Mỹ. Từ năm 2013, ông Han bắt đầu đầu tư vào tiền kỹ thuật số và đã tham gia vào hơn 50 dự án Token, chẳng hạn như EOS, Mạng Kyber, Mạng Raiden, SmartMesh, MeshBox, Trạng thái, Bluzelle, Tezos, Tinh vân, Tenx, 0x, v.v.
 Leo Li	Đối tác sáng lập của Whales Capital. Leo nhận bằng tiến sĩ bằng về vi điện tử từ Học viện Khoa học Trung Quốc và bằng cử nhân về kỹ thuật y sinh từ Đại học Beihang. Trước đây anh đã làm việc cho Trung Quốc Ngân hàng phát triển liên doanh Capital, Tsinghua Holdings Capital, Prometheus Capital và Delong Capital. Leo đã tích lũy được nhiều kinh nghiệm trong mười năm qua trong đầu tư cổ phần tư nhân. Ông chủ yếu tập trung vào TMT và Blockchain.
 Bill Dai	Đối tác của Trung tâm quản lý tài sản Bắc Kinh DeTai JiuFang và Trợ lý Chủ tịch của Jide Holding Co., Ltd. Giám đốc Hiệp hội cổ phần tư nhân Zhongguancun. Ông là giám đốc điều hành của Quỹ đầu tư chứng khoán Internet năng lượng cao Wuxi Aerospace, Phó chủ tịch của Công ty TNHH Quản lý vốn Bắc Kinh Junyuan và nhà đầu tư chính của Datang Huayin Electricity Co., Ltd. Ông có hơn 10 năm đầu tư và quản lý kinh nghiệm và thành thạo trong đầu tư cổ phần tư nhân và đầu tư công nghiệp. Ông đã quen thuộc với đầu tư chứng khoán và hợp tác kinh doanh, hiểu đầu tư vào bất động sản, tương lai và các dẫn xuất tài chính, và quen thuộc với quản lý chiến lược của các công ty và quản lý các công ty niêm yết và doanh nghiệp nhỏ.

 Wenli Su	Ông làm việc trong một ngân hàng đầu tư lớn ở Bắc Mỹ với việc sáp nhập và tổ chức lại doanh nghiệp hơn mười năm. Ông có nhiều kinh nghiệm trong việc mua lại các công ty niêm yết, tiếp quản thù địch, mua lại tài sản, tái cấu trúc nợ của công ty, và đánh giá giá trị của công ty và tài sản. Ông cá nhân thống trị và tham gia vào một số mười tỷ trường hợp sáp nhập. Là một người ủng hộ blockchain, ông V đã tham gia vào một số dự án blockchain.
 Yugui Wang	Ông là giám sát viên hiện tại của Ngân hàng Minsheng và là giám đốc không điều hành kể từ khi thành lập Ngân hàng Minsheng. Ông là tổng giám đốc của Hiệp hội bảo hiểm lẫn nhau của chủ tàu Trung Quốc và đã dẫn dắt công ty trở thành công ty lớn nhất thế giới và là cổ đông sáng lập của Ngân hàng Minsheng. Ông từng là giám đốc điều hành của Hiệp hội Luật Hàng hải Trung Quốc, Hiệp hội Thương mại Dịch vụ Trung Quốc, Giám đốc Công ty TNHH Chứng khoán Minsheng, giám sát Công ty Chứng khoán Haitong, và trọng tài của Ủy ban Trọng tài Hàng hải Quốc tế Trung Quốc. Ông Wang là giám đốc và giám sát của Ngân hàng Everbright Trung Quốc và là luật sư bán thời gian của Công ty Luật Bắc Kinh Jingwei.
	Giám đốc điều hành của Ngân hàng Đầu tư Chứng khoán Thương nhân Trung Quốc.

 Lizhi Ran	Người sáng lập Roots Capital, 2015 Zhongguancun, nhà đầu tư thiên thần xuất sắc, thành viên của đảo Zhenghe. Ông đã tham gia đầu tư mạo hiểm và đầu tư cổ phần tư nhân trong hơn 10 năm. Ông từng là phó chủ tịch điều hành của Qingke Group và giám đốc điều hành của Qingke Capital, bộ phận ngân hàng đầu tư của Tập đoàn Qingke. Qingke Group là một nhà cung cấp dịch vụ tích hợp nổi tiếng của Trung Quốc trong khu vực VC / PE. Anh đã tham gia gần 20 đầu tư và giao dịch tài chính cho các công ty internet (ví dụ: Mạng Baihe, Mạng Ganji và Siku Luxury, vv) và thành lập một số công ty, như thương hiệu sô cô la ma thuật Amovo và Business State. Sau khi xây dựng Qiyuan Captital, ông dẫn đầu đầu tư của hàng chục công ty, chẳng hạn như Công nghệ Xiaoneng, SENSORO Yunzi, Redu Medium và Yami, vv Ông cũng là giám đốc của nhiều công ty Internet nổi tiếng trước IPO (ví dụ: Siku Luxury).
 Junmin Zhou	Đồng sáng lập Công ty TNHH Tư vấn Deya Village Manangment Consulting (Bắc Kinh), Phó Tổng thư ký Phòng Thương mại và Công nghệ tại Liên đoàn Công nghiệp và Thương mại Thượng Hải và Trưởng ban đặc biệt Blockchain, đồng sáng lập Hiệp hội cựu sinh viên Thượng Hải 985. Ông có hơn mười năm kinh nghiệm quản lý và phát triển sản phẩm CNTT và tám năm kinh nghiệm đầu tư tài chính trong các lĩnh vực tài chính, truyền thông và internet. Ông là một quản lý sản phẩm cao cấp và đã làm việc trong các công ty CNTT nổi tiếng như Beida Fangzheng và Baoxin Software và các xe khối cao cấp như Viện nghiên cứu chiến lược quốc gia.
 Jun Sun	Yalian Advisory Group President, chuyên gia tư vấn cấp cao về quản lý tài chính / giảng viên cao cấp của Trung tâm đào tạo Ủy ban điều tiết ngân hàng Trung Quốc. Ông đã làm việc cho các tổ chức tài chính lớn trong nước và quốc tế các tổ chức tiêu chuẩn hóa nổi tiếng và đã dẫn dắt nhóm của ông thành công trong việc cung cấp dịch vụ tư vấn và đào tạo cho các nhà quản lý và gần một trăm tổ chức tài chính. Ông cũng đã tham gia với tư cách là giảng viên trong nhiều buổi đào tạo của các ngân hàng quy trình và các quy ước vốn mới do Ủy ban điều tiết ngân hàng Trung Quốc nắm giữ. Ông là một trong những người soạn thảo chính của nhiều nguyên tắc quy định của Ủy ban điều tiết ngân hàng Trung Quốc.

 Hui Wang	Zhong Yu Capital đồng sáng lập, giám đốc kiểm soát rủi ro chính. Ông là giám đốc độc lập của Huajing Securities, một thành viên chuyên gia của Ủy ban Kiểm toán Trách nhiệm Kinh tế của Viện Kế toán Công chứng Bắc Kinh, và là thành viên của Viện Kế toán Công chứng Bắc Kinh. Ông từng là đối tác của Reanda Certifed Public Accountants, bộ kiểm soát tài chính của công ty niêm yết NASDAQ và giám đốc China Huajing Electronics Group.
 Gaoqiang Li	Sáng lập đối tác và CEO của BenRui Capital. Ông có nhiều năm kinh nghiệm trong lĩnh vực đầu tư và quản lý. Ông có một sự hiểu biết mạnh mẽ về đầu tư cổ phần tư nhân và chứng khoán thị trường thứ cấp. Ông đã tham gia vào sự hợp tác của nhiều công ty Internet lớn. Ông đã biết Bitcoin từ năm 2010 và đã giúp tài trợ cho một số dự án blockchain và quá trình đào mỏ kể từ năm 2016.

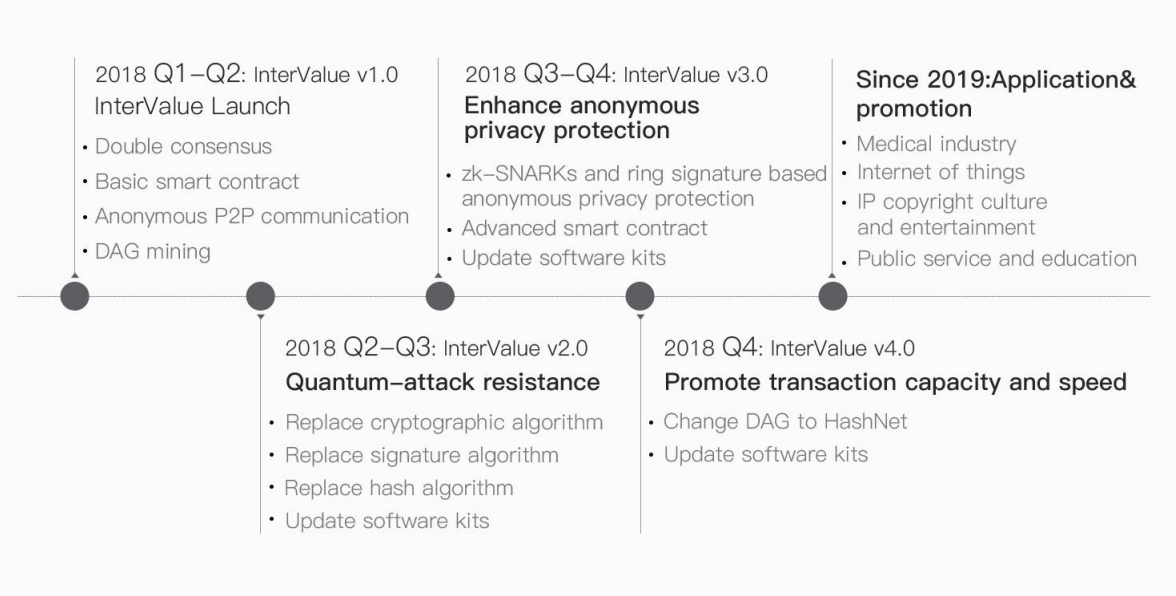
11.4. Tổ chức cố vấn

Danh sách đối tác chiến lược sẽ được cập nhật liên tục.

- **Roots Cap:** Quỹ đầu tư thiên thần hàng đầu của Trung Quốc tập trung vào các ngành công nghệ mới nổi như big data, nâng cao trải nghiệm khách hàng, dịch vụ doanh nghiệp, phần cứng thông minh (VR / AR). Họ đã đầu tư thành công vào hàng chục dự án VC đầu tiên, bao gồm big data, thương mại điện tử, phần cứng thông minh, du lịch trực tuyến, nâng cấp tiêu dùng và giải trí văn hóa, v.v. trong đó 80% dự án nhận được một vòng đầu tư mới.
- **BenRui Capital**: Được thành lập và thành lập bởi các chuyên gia kỹ thuật blockchain, các nhà đầu tư chuyên nghiệp và các học viên của VC / PE, tập trung vào đầu tư theo hướng công nghệ trong lĩnh vực blockchain.
- **Whales Capital**: Một quỹ đầu tư mạo hiểm chuyên nghiệp mà chủ yếu tập trung vào Blockchain. Tìm kiếm các công ty hoặc dự án với thị trường lớn, công nghệ hàng đầu và đội ngũ tài năng. Tin tưởng vào đầu tư giá trị và đầu tư trao quyền.
- **Genesis Capital**: Tập trung vào ngành công nghiệp blockchain và cam kết quá trình đào các dự án tốt nhất trong giai đoạn đầu. Đây là một trong 5 quỹ tiền tệ mật mã hàng đầu tại Trung Quốc. Nó đã đầu tư khoảng 50 dự án liên quan đến blockchain.
- **Obsidian capital** : Tổ chức đầu tư mạo hiểm nổi tiếng châu Âu

Các đối tác chiến lược khác bao gồm: CryptoLaboratory , OKCrypto , BigcoinCapital , EYUCaptial , ReexionCapital , HelloCaptial , StarwinCapital , SkylineCapital, Cloud Chain Capital, v.v.

11.5. Roadmap



Lộ trình của InterValue bao gồm hai giai đoạn: giai đoạn phát triển và giai đoạn thành phẩm. Sau bốn lần nâng cấp lặp lại trong giai đoạn phát triển, InterValue sẽ được định hình phù hợp với tầm nhìn của chúng tôi và đi vào giai đoạn sản xuất.

- 2018 Q1-Q2: Chúng tôi sẽ phát hành InterValue 1.0 và các bộ phần mềm của nó. Phiên bản này hỗ trợ quá trình đào DAG, đồng thuận kép, giao tiếp P2P ẩn danh và hợp đồng thông minh.
- 2018 Q2-Q3: Chúng tôi sẽ phát hành InterValue 2.0 bằng cách thay đổi biểu đồ DAG của các phiên bản trước thành HashNet, sẽ nâng cao năng lực của InterValue và tăng tốc độ giao dịch lên hàng trăm nghìn TPS.
- 2018 Q3-Q4: Chúng tôi sẽ phát hành InterValue 3.0 giúp tăng cường bảo vệ quyền riêng tư ẩn danh của phiên bản 2.0 bằng cách sử dụng bằng chứng không có kiến thức.
- 2018 Q4: Chúng tôi sẽ phát hành phần mềm InterValue 4.0 và bộ phần mềm của nó. Phiên bản này được đánh dấu bằng sức đề kháng tấn công lượng tử bằng cách thay thế thuật toán mã hóa, thuật toán chữ ký và thuật toán băm trong phiên bản trước.
    - Từ sự phát hành của InterValue 1.0 vào năm 2018, chúng tôi sẽ áp dụng nền tảng InterValue trong một số cảnh ứng dụng, chẳng hạn như ngành y tế, internet, IP, văn hóa và giải trí, dịch vụ công cộng, giáo dục vv. Chúng tôi sẽ khám phá việc áp dụng InterValue với cộng đồng và mở rộng các lĩnh vực ứng dụng của nó.

12

Token

12.1. Token tiện ích (token utility)

InterValue đặt mục tiêu xây dựng một công nghệ nền tảng Blockchain 4.0 toàn diện và đầy đủ tính năng, hỗ trợ các tổ chức thương mại và các cơ quan chính phủ xây dựng Blockchain công cộng, Blockchain liệp hợp và Blockchain riêng để đáp ứng các yêu cầu và đặc tính kinh doanh tương ứng của họ. Để hỗ trợ Blockchain công cộng, InterValue giới thiệu chính sách token trong lớp khuyến khích để hỗ trợ các kế hoạch đồng thuận linh hoạt. Token nội vi INVE kích thích cộng đồng duy trì Blockchain công khai của InterValue và phát triển DApps, sau đó là làm tăng giá trị của Blockchain công khai InterValue và thúc đẩy mạng lưới InterValue. Trong Blockchain công cộng InterValue, các tiện ích của token INVE được liệt kê dưới đây:

- Kích thích đa số người dùng giao dịch tài sản của họ trong mạng InterValue để kiếm phí giao dịch và phí công chứng, giúp cải thiện tính bảo mật của mạng InterValue; Hỗ trợ quá trình đào bằng cách bổ sung các nút giao dịch và các nút công chứng;

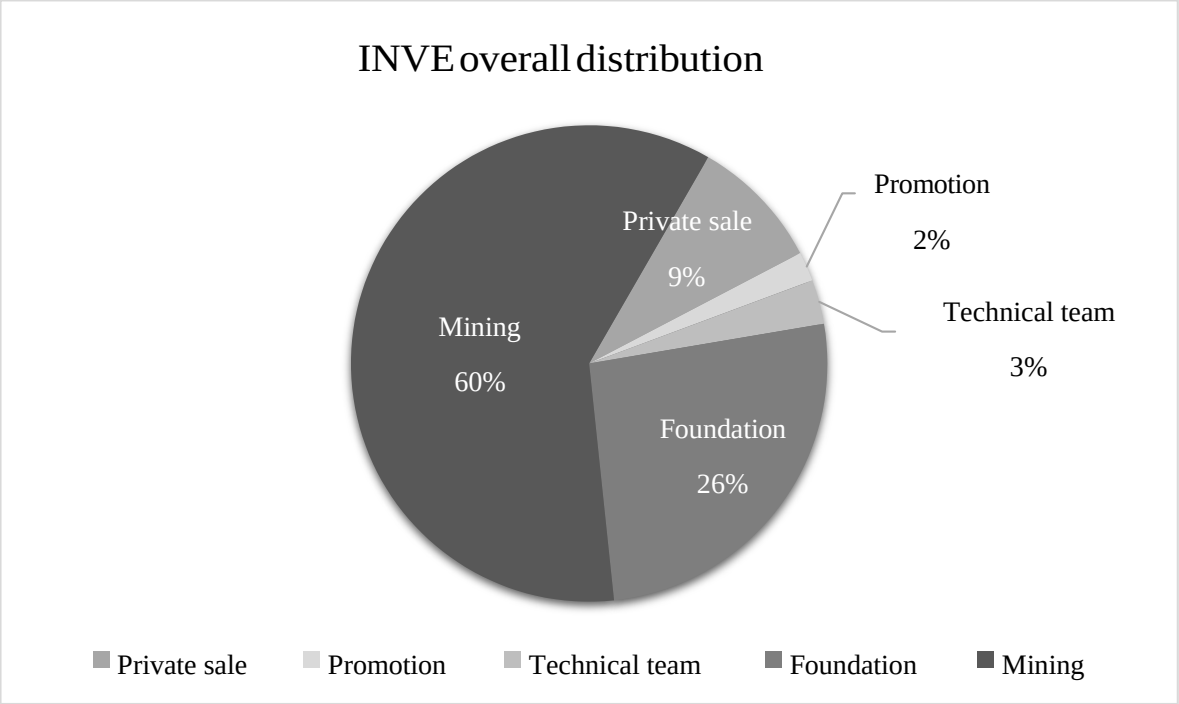
- Được sử dụng để đo lường công bằng để thực hiện kiến trúc đồng thuận kép được đề xuất trong InterValue: Sự đồng thuận DAG cơ bản và sự đồng thuận BA-VRF trong giai đoạn phát triển ban đầu; Sự đồng thuận của HashNet và sự đồng thuận của BA-VRF ở giai đoạn sau;
- Hỗ trợ hệ sinh thái của InterValue để thực hiện hợp đồng thông minh tiên tiến, cung cấp các chương trình chống gian lận để ngăn chặn "bom logic" khỏi ảnh hưởng tới hiệu quả mạng;
- Đóng vai trò của tiền tệ cơ bản trong hệ sinh thái của InterValue, vốn là token của DApp với các tính năng tương ứng và đặt nền tảng thanh khoản tài sản;
- Hành động như phí ký quỹ để quản lý DApp của Blockchain công cộng InterValue và cải thiện mức độ phổ biến của DApps;
- Được sử dụng để phát triển các chức năng mạng bổ sung và cải thiện khả năng mở rộng của nền tảng.

12.2. Phát hành token (token issuance)

INVE là tên viết tắt của token cơ bản của InterValue, và nó bằng 10^{18} Atom, tức là, 1 INVE = 10^{18} Atoms

Atom là đơn vị nhỏ nhất của token INVE, và nó cũng được sử dụng làm phí giao dịch cho hợp đồng thông minh tiên tiến và giao dịch qua chuỗi hợp đồng thông minh.

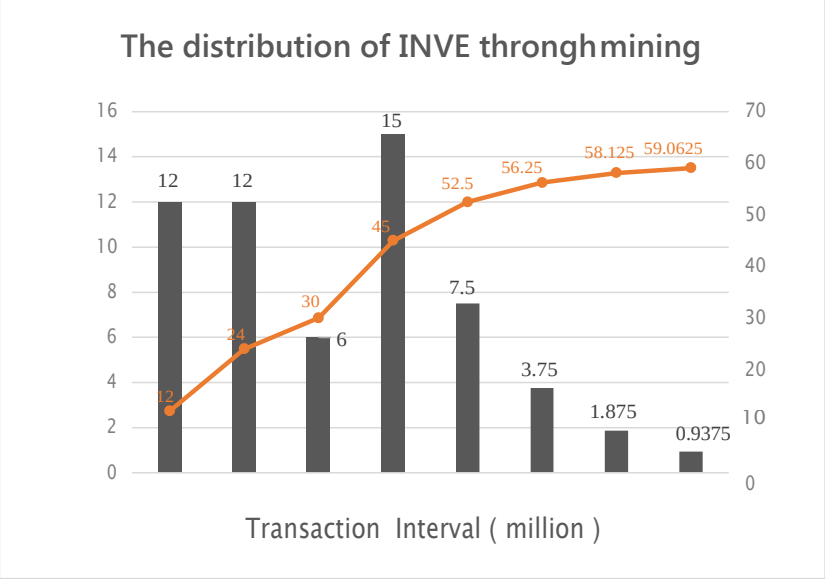
Tổng số token INVE là 10 tỷ, trong đó 6 tỷ được phát hành như phần thưởng đào thông qua quá trình đào DAG và phần còn lại được dành riêng cho nền tảng, phát triển dự án, xúc tiến dự án và xây dựng nhóm. Dự án gây quỹ được lên kế hoạch để khởi chạy trên Ethereum trong quý 1 năm 2018, và các token ERC20 đã được phát hành có thể được chuyển đổi thành token INVE theo tỉ lệ 1: 1 khi chuỗi chính của InterValue được ra mắt lần đầu. Sự sắp xếp phân phối tổng thể INVE và phân phối token INVE dự trữ được thể hiện trong hình 12-1.



Người dùng thông thường cần gửi giao dịch qua các nút đầy đủ của địa phương.

Để ngăn chặn người dùng độc hại có các cuộc tấn công DDoS độc hại, người dùng thông thường phải thực hiện phép tính POW ở mức độ thấp trước khi bắt đầu một giao dịch. Sau đó, nó sẽ gửi giao dịch đến nút đầy đủ cục bộ để xử lý. Nếu giao dịch là một giao dịch cross-sharding, nó cần được tiếp tục gửi đến toàn bộ nút. Các nút đầy đủ và các nút đầy đủ của địa phương tham gia vào sự đồng thuận xác minh xem liệu giá trị băm của giao dịch có đáp ứng được độ khó quá trình đào hay không. Sau khi giao dịch được xác minh và ổn định, nút đầy đủ cục bộ và nút đầy đủ (trong trường hợp giao dịch xuyên tạc) gửi giao dịch có thể nhận được một số lượng mã INVE tương ứng làm phần thưởng quá trình đào. Để thưởng cho đóng góp của các nút đầy đủ và các nút đầy đủ địa phương để giúp đạt được sự đồng thuận trên toàn bộ mạng, 6 tỷ thẻ INVE được tạo thông qua quá trình đào làm phần thưởng.

Figure 12–2: The Distribution of INVE through Mining Reward



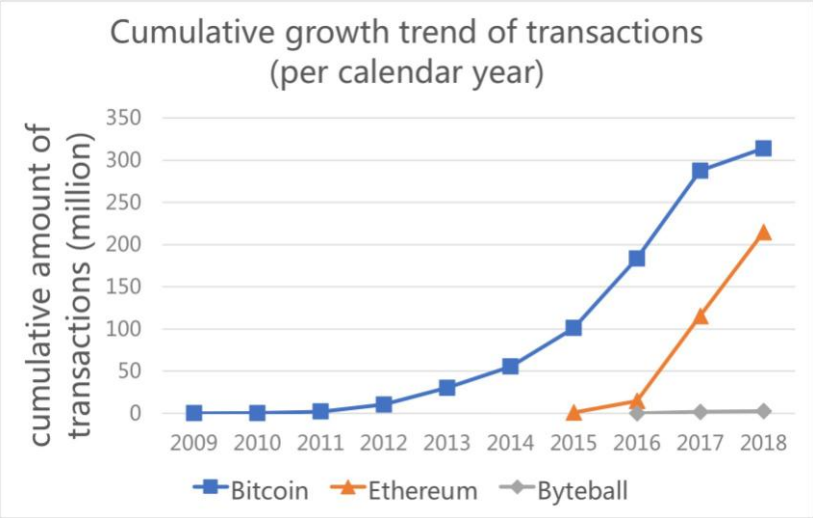
Sáu tỷ token INVE được phát hành theo lô cho người dùng thông thường khi phần thưởng quá trình đào giảm theo số lượng lô. Các lô này được chia cho số lượng giao dịch được ưu tiên. Một người dùng bình thường gửi một giao dịch bao gồm trong đợt thứ hai (bao gồm 200 triệu giao dịch đầu tiên với tổng khối lượng phát hành $S1$ = 1,2 tỷ đồng) sẽ nhận được 6 mã INVE như phần thưởng quá trình đào, 3 mã INVE khi giao dịch của bạn rơi vào lô thứ hai (phạm vi từ giao dịch 200 triệu đến giao dịch 600 triệu và tổng khối lượng phát hành $S2$ = 1,2 tỷ) và 1,5 mã INVE khi giao dịch của anh rơi vào bồn thứ ba (phạm vi từ giao dịch 600 triệu đến giao dịch 1 tỷ và tổng khối lượng phát hành $S3$ = 0,6 tỷ đồng). Lô thứ tư và các lô tiếp theo được chia cho mỗi 1 tỷ giao dịch. Một người dùng bình thường có thể nhận được 1.5 token / giao dịch INVE làm phần thưởng quá trình đào trong đợt thứ tư và phần thưởng quá trình đào sẽ giảm liên tục xuống một nửa trong các đợt tiếp theo. Sự phân bố của INVE thông qua quá trình đào (lấy 6 tỷ giao dịch đầu tiên làm ví dụ) được thể hiện trong Hình 12-2.

$$\text{Total mining reward} = S_1 + S_2 + S_3 + \lim_{n\to\infty} \sum_{i=4}^{i=n} s_i$$

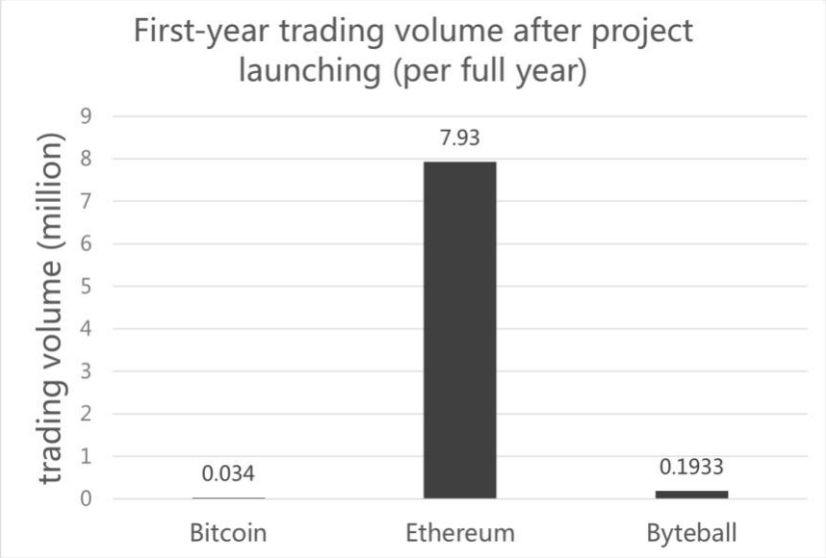
$$= 3 \text{ Billion} + S_4/(1-q)$$

$$= 6 \text{ Billion}(S_4 = 1.5 \text{ Billion}, q = 0.5)$$

Việc thiết lập chu kỳ phân phối phần thưởng quá trình đào (chia cho số giao dịch) xem xét toàn bộ lợi thế của cấu trúc dữ liệu chuỗi DAG được sử dụng bởi dự án InterValue trong tốc độ hội tụ giao dịch và lợi thế sau phát triển của dự án (tức là chấp nhận khái niệm dự án và sự trưởng thành của cộng đồng).



Hình 12-3: Xu hướng tăng trưởng tích lũy của các giao dịch (Bitcoin, Ethereum và Byteball)



Hình 12-4: Khối lượng giao dịch trong năm đầu tiên sau khi triển khai dự án （Bitcoin, Ethereum và Byteball）

- **Ưu điểm của tốc độ xác nhận giao dịch :** Nếu không xem xét lợi thế của phát triển sau, khối lượng giao dịch mà dự án có thể hoàn thành trong một đơn vị thời gian chủ yếu được xác định bởi tốc độ giao dịch của giao dịch. Bitcoin và Byteball là các dự án tiên phong của cấu trúc dữ liệu blockchain chuỗi đơn và cấu trúc dữ liệu chuỗi DAG, tương ứng, và chúng không có lợi thế sau phát triển trong các loại công nghệ blockchain tương ứng của chúng. Như thể hiện trong hình 12-3, sự tăng trưởng tích lũy của giao dịch Bitcoin và Byteball tăng rất chậm trong ba năm đầu tiên sau khi dự án ra mắt, nhưng số lượng giao dịch được thực hiện bởi dự án Byteball trong năm đầu tiên cao hơn đáng kể so với Bitcoin (Theo thể hiện trong hình 12-4), trong đó cho thấy rằng việc sử dụng cấu trúc dữ liệu chuỗi DAG để cải thiện tốc độ kết nối giao dịch có lợi cho việc

cải thiện khối lượng giao dịch của dự án. Do đó, dự án InterValue của chúng tôi có lợi thế vốn có trong việc tăng khối lượng giao dịch.

- **Lợi thế hậu phát triển :** Lợi thế hậu phát triển của dự án có vai trò quan trọng trong việc tăng khối lượng giao dịch. Như thể hiện trong hình 12-3, Ethereum kế thừa Bitcoin, đã tận dụng lợi thế hậu phát triển của dự án để đạt được tốc độ tăng trưởng tương đương với Bitcoin trong ba năm đầu tiên sau khi dự án ra mắt. Ngoài ra, trong năm đầu tiên sau khi phát hành dự án, khối lượng giao dịch được hoàn thành bởi Ethereum cao hơn 2 lần so với khối lượng giao dịch của Bitcoin. Do đó, lợi thế hậu phát triển trong sử dụng cấu trúc dữ liệu chuỗi DAG khiến InterValue có tiềm năng lớn trong việc tăng khối lượng giao dịch.

Tính đến lợi thế về hai khía cạnh trên, với việc Ethereum đã hoàn thành hơn 200 triệu giao dịch trong vòng chưa đầy ba năm sau khi dự án được tung ra, chúng tôi dự đoán rằng dự án InterValue của chúng tôi có khả năng hoàn thành một tỷ giao dịch trong vòng một năm sau khi khởi chạy dự án.

13

Hiện trạng kinh doanh

13.1. Cạnh tranh kỹ thuật

- Bitcoin là dự án đại diện cho Blockchain 1.0. Cơ sở hạ tầng của nó, được gọi là Blockchain, là một cuốn sổ tài khoản chia sẻ để thực hiện truyền thông giá trị theo thể thức ngang hàng. Tác động tiềm năng của Blockchain đối với tài chính và các ngành khác thậm chí có thể tương đương với việc phát minh ra sổ kế toán kép
- Ethereum là dự án đại diện cho Blockchain 2.0. Nó là một hệ thống mã nguồn mở Blockchain cơ bản được thực hiện với hợp đồng thông minh. Hàng trăm Dapp đã được triển khai trên Ethereum. Tuy nhiên, dự án như CryptoKitties cho thấy sự bất lợi của thông lượng giao dịch và tốc độ xác nhận giao dịch của Ethereum.
- EOS là bản sản phẩm tiêu chuẩn của Ethereum. Mục tiêu cuối cùng của nó là trở thành một hệ điều hành blockchain. Nó cung cấp cho các nhà phát triển nhiều chức năng cơ bản, chẳng hạn như cơ sở dữ liệu, cài đặt đặc quyền tài khoản, lịch thực hiện, xác thực, truyền thông mạng, v.v.
- IOTA là tiền điện tử của Internet vạn vật IOT. Để cải thiện thông lượng giao dịch của Blockchain, nó thiết kế cuốn sổ tài khoản phân tán dựa trên DAG, được gọi là Tangle. Mục tiêu của nó là đạt được một mạng micropayment toàn cầu trong ngành công nghiệp IoT
- ByteBall là một hệ thống phân quyền và cho phép lưu trữ chống giả mạo cho bất kỳ dữ liệu nào. Các đơn vị lưu trữ của ByteBall kết nối với nhau. Mỗi giá trị chứa một hoặc nhiều giá trị băm của các đơn vị lưu trữ trước đó, được sử dụng để kết hợp đơn vị lưu trữ trước đó và xây dựng một phần đơn đặt hàng giữa các đơn vị lưu trữ. Tất cả các đơn vị lưu trữ tạo thành một DAG.

Bảng 13-1: Lợi thế kỹ thuật của InterValue

	BTC	ETH	EOS	IOTA	ByteBall	InterValue
Node Type	Global Node, Light Node	Global Node, Light Node	Global Node, Light Node	Global Node, Light Node	Global Node, Light Node	Confirm Node, Full Node, Local Full Node, Light Node, Tiny Node
Anonymity of P2P Network	No	No	No	No	No	Yes
Consensus	POW	Dagger POW	DPOS	Weighted POW	12 Notary	HashNet BA-VRF
Anti-quantum Attack	No	No	No	Partial	No	Yes
Privacy Protection	No	No	No	No	No	Zero Knowledge Proof of Privacy Protection
Smart Contract	No	Turing Complete	Turing Complete	No	Declarative Contract	Declarative Contract and AdvancSed Turing Complete
Transaction Speed	7TPS	30TPS	3300TPS	1000TPS	100TPS	>100000TPS
Price Scheme	Transaction Fee &Mining	Transaction Fee &Mining	Transaction Fee &Mining	No Transaction Fee	Transaction Reference &Notarization	Transaction Reference &Notarization & Mining
Application	Few	Hundreds	Exploit	Exploit	Exploit	Massive applications in future

13.2. Cạnh tranh ở cấp độ công ty

- Công ty công nghệ JingTong: Đây là một công ty của Trung Quốc trong lĩnh vực nghiên cứu về công nghệ cơ bản của Blockchain. Đội ngũ cốt lõi của nó bao gồm các kỹ sư Blockchain trong thung lũng silicon và Trung Quốc. Trong năm 2014, công ty phát hành nền tảng cơ bản cho các ứng dụng kinh doanh. Cho đến nay, công ty đã phát triển một số DApps trong các lĩnh vực khác nhau, chẳng hạn như tài chính, đi du lịch, thành phố thông minh, hậu cần, y học, và vv

- Ripple: Ripple được thành lập vào năm 2013. Nó cung cấp giải pháp cân bằng tài chính toàn cầu. Giải pháp cho phép sự cân bằng giữa các ngân hàng theo cách ngang hàng, thay vì thông qua các ngân hàng proxy, điều này làm cho việc chuyển tiền nhanh chóng và giảm đáng kể chi phí cân đối. Ripple coin một lần là đồng tiền kỹ thuật số có giá trị đứng thứ 2 (3) trên toàn cầu, và nó là mô hình đầu tiên kết hợp chặt chẽ giữa đồng tiền kỹ thuật số và ứng dụng kinh doanh.

- Circle: Circle được thành lập vào năm 2013. Sản phẩm của nó chứa thanh toán bitcoin và thanh toán xã hội. Công ty có một đội ngũ hoàn chỉnh và khác biệt. Người sáng lập có kinh nghiệm thành công trong lĩnh vực xây dựng công ty, phần mềm, truyền thông và thông tin liên lạc nền tảng.

Bảng 13-2: Lợi thế của công ty về InterValue

	JingTong Technology	Ripple	Circle	Hedera Hashgraph	InterValue
Roadmap	Blockchain commercial platform in various fields	Bank balance	Digital coin payment	Blockchain platform in various fields	Public chain 、Blockchain browser 、Blockchain Wallet 、Commercial platform in various fields
Applicatio n	Business &Non-business	Finance	Digital coin	Business &Non-business	Digital coin& Business &Non-business
Advantage	Professional team, Intervene in various fields	Professio nal team, High entry barrier	Professional team, Rich Experience, Abundant funds	Professional team, High creativity	Professional team, Rich Experience, High creativity
Vision	Trust ecological builder	Global uniform payment standard	Rebuild global payment network	Build the trust layer of the Internet	Build global value network

14

Nguy cơ

Đầu tư vào tài sản Crypto có nhiều rủi ro lớn. Các nhà đầu tư cần phải hiểu đầy đủ các rủi ro này và tự chịu trách nhiệm về rủi ro đó.

- **Thông tin công bố không đầy đủ**

Cho đến ngày xuất bản báo cáo bạch này, INVE vẫn đang được phát triển. Các công nghệ cốt lõi của nó như thuật toán mã hóa, mạng truyền thông, sự đồng thuận, có thể được cập nhật thường xuyên. Báo cáo bạch này chứa tổng quan cơ bản về INVE, nhưng nó không hoàn toàn hoàn chỉnh. Nền tảng có thể cập nhật và cải tiến dự án theo thời gian dựa trên những thay đổi về công nghệ hoặc cho các mục đích cụ thể. Quỹ không thể và không có nghĩa vụ thông báo cho nhà đầu tư trong thời gian thực về tất cả các chi tiết của quy trình phát triển INVE. Việc tiết lộ thông tin không đầy đủ là không thể tránh khỏi và hợp lý.

- **Giám sát**

Tài sản mã hóa đã được giám sát bởi nhiều cơ quan quản lý quốc gia do những rủi ro cao. Quỹ có thể nhận được yêu cầu, thông báo, cảnh báo, đơn đặt hàng hoặc phán quyết từ các nhà quản lý trong quá trình bán hàng và thậm chí có thể được yêu cầu chấm dứt hoạt động bán hàng. Việc giám sát có thể ảnh hưởng rất lớn đến sự phát triển, tiếp thị, quảng cáo của INVE. Vì các quy tắc giám sát có thể thay đổi bất cứ lúc nào, phụ cấp giám sát của INVE ở bất kỳ quốc gia nào có thể là tạm thời. Ngoài ra, INVE có thể được coi là hàng hóa ảo, tài sản kỹ thuật số hoặc tiền tệ chứng khoán. Do đó, INVE có thể bị cấm giao dịch hoặc giữ ở một số quốc gia.

- **Lỗi dự án**

INVE vẫn đang được phát triển. INVE có thể không thành công hoặc dừng vì bất kỳ lý do gì. Những lý do chính bao gồm: buộc phải chấm dứt bởi các nhà quản lý, quỹ tiềm ẩn, và những thách thức kỹ thuật không thể vượt qua. token INVE có thể không được gửi cho nhà đầu tư do lỗi dự án.

- **Quỹ bị đánh cắp**

Ai đó có thể cố gắng ăn cắp quỹ ICO của nhóm sáng lập và điều đó sẽ ảnh hưởng lớn đến sự phát triển của INVE. Mặc dù nền tảng sẽ thích ứng với giải pháp an toàn nhất để bảo vệ quỹ ICO. Tuy nhiên, một số trộm cắp trên mạng vẫn còn khó khăn để ngăn chặn hoàn toàn.

- **Lỗ hổng mã nguồn**

Mặc dù nền tảng này sẽ mời nhóm bảo mật hàng đầu kiểm tra mã nguồn của INVE, không ai có thể đảm bảo rằng mã nguồn là hoàn hảo. Có thể có một số lỗi, lỗi hoặc lỗ hổng bảo mật khiến người dùng không thể sử dụng một số chức năng. Hơn nữa, những lỗ hổng này gây nguy hiểm cho sự sẵn có, sự ổn định, hoặc an toàn và tiêu cực ảnh hưởng đến giá trị của INVE. Quỹ sẽ hợp tác với cộng đồng INVE để tối ưu hóa và cải thiện tính bảo mật của mã nguồn.

- **Nâng cấp mã nguồn**

Vì mã nguồn của INVE là mã nguồn mở và được nâng cấp liên tục, không ai có thể dự đoán hoặc đảm bảo kết quả chính xác trong khi nâng cấp. Do đó, việc nâng cấp mã nguồn có thể dẫn đến kết quả không lường trước được hoặc không lường trước được, điều này có thể ảnh hưởng lớn đến hoạt động và giá trị của INVE.

- **DdoS**

INVE có thể bị tấn công DDoS, điều này làm cho hệ thống INVE không hoạt động. Bên cạnh đó, giao dịch có thể được ghi vào INVE HashNet với độ trễ hoặc thậm chí không thể thực hiện được.

- **Không đủ khả năng của các nút**

Sau khi hệ thống INVE trực tuyến, các giao dịch sẽ tăng lên rất nhiều. Nếu yêu cầu xử lý cao hơn khối lượng công việc của hệ thống INVE, nó có thể gây ra sự thất bại của INVE. Trong trường hợp xấu nhất, bất kỳ ai cũng có thể mất token INVE của họ. Hơn nữa, các rollback hoặc hardfork của INVE có thể được kích hoạt, gây nguy hiểm cho tính khả dụng, ổn định, hoặc an toàn của INVE.

- **Token INVE bị lấy đi khi chưa được phép**

Kẻ tấn công có thể giải mã hoặc tấn công tài khoản của nhà đầu tư. Do đó, anh / cô ấy có thể xác nhận token INVE của nạn nhân. Đó là, các thẻ INVE được mua bởi nạn nhân có thể được gửi đến kẻ tấn công. Mỗi nhà đầu tư phải bảo vệ tài khoản của mình. Có một số mẹo: (1) Cài đặt phần mềm chống vi-rút, (2) Sử dụng mật khẩu bảo mật cao, (3) Không mở hoặc trả lời bất kỳ email tung hứng nào, và (4) Lưu trữ thông tin tài khoản và khóa riêng ở nơi an toàn.

- **Mất khóa riêng**

Mỗi nhà đầu tư phải giữ chìa khóa riêng của ví tiền INVE một cách an toàn. Nếu nhà đầu tư mất hoặc phá hủy khóa riêng, thì nền tảng không thể giúp nhà đầu tư xác nhận token INVE.

- **Phân chia hệ thống hay fork**

INVE là một dự án nguồn mở được cộng đồng hỗ trợ. Mặc dù nền tảng có một số điểm yếu trong cộng đồng INVE, nền tảng không thể kiểm soát hoàn toàn sự phát triển và thị trường của INVE. Bất kỳ ai cũng có thể phát triển và nâng cấp INVE mà không có bất kỳ quyền nào của người khác. Khi một phần người dùng chấp nhận quảng cáo chiêu hàng hoặc nâng cấp INVE, nó sẽ gây ra một hardfork. Hơn nữa, theo lộ trình, nền tảng sẽ làm một hardfork. Về mặt lý thuyết, INVE Hashnet có thể chia rẽ nhiều lần. Trong trường hợp xấu nhất, các nhánh này có thể phá hủy tính bền vững của hệ thống INVE.

- **Thiếu độ thu hút**

Giá trị của INVE phụ thuộc vào mức độ phổ biến của Blockchain INVE. Nền tảng không đảm bảo rằng INVE sẽ phổ biến trong một thời gian ngắn. Trong trường hợp xấu nhất, INVE chỉ thu hút một vài người sử dụng, dẫn đến giá token uyên thâm và phát triển sự phát triển của INVE. Bên cạnh đó, nền tảng không chịu trách nhiệm về việc vô hiệu hóa hoặc ảnh hưởng đến giá thị trường của INVE.

- **Không đủ lượng lưu hành**

INVE không thuộc về bất kỳ người, tổ chức, ngân hàng, quốc gia, tổ chức, tiểu bang hoặc tiểu bang nào khác, cũng không được hỗ trợ bởi bất kỳ tài sản hoặc tín dụng nào. Giao dịch của INVE chỉ dựa trên sự đồng thuận giữa các nhà đầu tư. Không ai có thể đảm bảo giá lưu thông hoặc giá thị trường của INVE. Nếu chủ sở hữu muốn bán INVE của họ, họ cần phải tìm người mua phù hợp. Bên cạnh đó, Có thể không có trao đổi hoặc các thị trường khác để giao dịch INVE.

- **Biến động Giá token**

Trong thị trường mở, giá của mã hóa-token biến động rất nhiều. Sự biến động gây ra bởi sự thay đổi của thị trường, chính sách pháp lý, công nghệ, bảo vệ trao đổi, và vv Nền tảng không chịu trách nhiệm về giao dịch của INVE trên thị trường thứ cấp. Rủi ro giao dịch INVE được thực hiện bởi các đại lý.

- **Cạnh tranh**

Giao thức cơ bản của INVE dựa trên giao thức nguồn mở. Không ai sở hữu bản quyền hoặc các quyền khác của mã nguồn. Vì vậy, mọi người có thể sao chép, thiết kế, sửa đổi và nâng cấp mã nguồn để phát triển một giao thức, hệ thống hoặc nền tảng ảo cạnh tranh hơn. Trong trường hợp này, sản phẩm cạnh tranh trong tương lai có thể vượt qua hoặc thậm chí thay thế INVE, và điều này không thể được kiểm soát bởi nền tảng. Bên cạnh đó, một số nền tảng hiện có như IOTA và ByteBall đã trở thành đối thủ cạnh tranh của INVE. Có lẽ có nhiều đối thủ cạnh tranh hơn trong tương lai. Nền tảng không thể loại bỏ sự xuất hiện của các đối thủ cạnh tranh.

References

[1] Bitcoin Computation Waste, http://gizmodo.com/the-worlds-most-powerful -computer-network-is-being-was-50403276. 2013.

[2] Bitcoinwiki. Proof of Stake. http://www.Blockchaintechnologies.com/ Blockchain-applications. Aug 2017.

[3] Coindesk.com. Bitcoin: A Peer-to-Peer Electronic Cash System.

[4] http://www.coindesk.com/ibm-reveals-proof-concept-Blockchain-powered-internet-things/ Nov 2017.

[5] Ethereum. Ethereum. https://github.com/ethereum/. Nov 2017.

[6] IOTA. https://github.com/iotaledger/. As of 10 Nov 2017.

[7] Byteball. Byteball. https://github.com/byteball/. Sep 2017.

[8] Bernstein, Daniel J, et al. High-speed high-security signatures. Journal of Cryptographic Engineering 2.2(2012), 77-89.

[9] M. Castro and B. Liskov. Practical Byzantine Fault Tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, Louisiana, USA,1999, pp. 173-186.

[10] Biryukov, Alex, and D. Khovratovich. Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. Network and Distributed System Security Symposium 2016.

[11] Gilad Y, Hemo R, Micali S, et al. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. The Symposium 2017, 51-68.

[12] C. Decker and R. Wattenhofer. Information Propagation in the Bitcoin Net- work. 13-th IEEE Conference on Peer-to-Peer Computing, 2013.

[13] D. Dolev and H.R. Strong. Authenticated algorithms for Byzantine agreement. SIAM Journal on Computing 12 (4), 656-666.

[14] A. Kiayias, A. Russel, B. David, and R. Oliynycov..Ouroburos: A provably secure proof-of-stake protocol. Cryptology ePrint Archive, Report 2016/889, 2016. http://eprint.iacr.org /2016/889.

[15] S. King and S. Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof- of-Stake, 2012.

[16] S. Micali, M. Rabin and S. Vadhan. Verifable Random Functions. 40th Foun- dations of Computer Science (FOCS), New York, Oct 1999.

[17] Directed acyclic graph: https://en.wikipedia.org/wiki/Directed_acyclic_graph