HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Đức Duy

NGHIÊN CỨU ỨNG DỤNG BLOCKCHAIN CHO BÀI TOÁN THANH TOÁN PHI TIỀN MẶT TRONG LĨNH VỰC TÀI CHÍNH NGÂN HÀNG

LUẬN VĂN THẠC SỸ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – 2020

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Đức Duy

NGHIÊN CỨU ỨNG DỤNG BLOCKCHAIN CHO BÀI TOÁN THANH TOÁN PHI TIỀN MẶT TRONG LĨNH VỰC TÀI CHÍNH NGÂN HÀNG

CHUYÊN NGHÀNH: KHOA HỌC MÁY TÍNH

MÃ SỐ: 8.48.01.01

LUẬN VĂN THẠC SỸ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC

TS. ĐẶNG MINH TUẤN

HÀ NỘI – 2020

LỜI CAM ĐOAN

Tôi xin cam đoan: Khoá luận tốt nghiệp với đề tài "**NGHIÊN CỨU ỨNG DỤNG BLOCKCHAIN CHO BÀI TOÁN THANH TOÁN PHI TIỀN MẶT TRONG LĨNH VỰC TÀI CHÍNH NGÂN HÀNG**" là công trình nghiên cứu của cá nhân tôi, các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác, không sao chép của bất cứ ai.

Tôi xin chịu mọi trách nhiệm về công trình nghiên cứu của riêng mình!

Hà Nội, ngày …….

Người cam đoan

Nguyễn Đức Duy

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Viết tắt	Nguyên nghĩa
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
BCG	Boston Consulting Group
BTS	Bitshares
CorDapps	Corda Distributed Applications
CPU	Central Processing Unit
DAG	Directed Acyclic Graph
DAO	Tổ chức tự quản phân cấp thế giới
DBMS	Database Management System
DPoS	Delegated Proof-of-Stake
ECDSA	Elliptic Curve Digital Signature Algorithm
IDE	Integrated Development Environment
JDBC	Java Database Connectivity
JDK	Java Development Kit
KYC	Know your customer
OS	operating system
POA	Proof-of-Authority
POS	Proof-of-Stake
POW	Proof-of-work
RAM	Random Access Memory
RPC	Remote Procedure Call
SHA	Secure Hash Algorithm
TX	Transaction
UTXO	Unspent transaction output

DANH SÁCH BẢNG

DANH SÁCH HÌNH VẼ

MỞ ĐẦU

Trong Cách mạng công nghiệp 4.0, “blockchain” (chuỗi khối) được xem là một trong những công nghệ "then chốt" cho chuyển đổi số và xây dựng nền tảng công nghệ thông tin trong tương lai.

Với khả năng chia sẻ thông tin dữ liệu minh bạch theo thời gian thực tế, có tính bảo mật cao, công nghệ blockchain là một trong những xu hướng công nghệ đột phá, có khả năng ứng dụng rộng rãi ở nhiều ngành nghề, lĩnh vực khác nhau.

Ứng dụng công nghệ Blockchain có thể giải quyết được một số vấn đề mà hệ thống tài chính ngân hàng hiện nay đang gặp phải. Blockchain cung cấp mức độ bảo mật cao, minh bạch trong các giao dịch cũng như chi phí thấp. Hơn nữa, người dùng có thể hoàn toàn tham gia vào giao dịch mà không cần xác thực bởi bên thứ 3.

Công nghệ Blockchain thực sự mở ra tiềm năng vô cùng lớn trong lĩnh vực tài chính – ngân hàng, tác động không nho đến quy trình xác nhận giao dịch, quản lý tiền mặt, tối ưu hóa tài sản cũng như các quy trình kinh doanh khác. Công nghệ Blockchain sẽ giúp giảm thiểu thời gian từ lúc đăng ký tới lúc hoàn thành giao dịch hoặc giảm thời gian cho các giao dịch liên ngân hàng, chuyển khoản quốc tế hoặc xác nhận thông tin cá nhân.

Nhận thấy những tiềm năng to lớn của Blockchain ở hiện tại và tương lai, em quyết định lựa chọn đề tài nghiên cứu các ứng dụng của Blockchain cho bài toán thanh toán phi tiền mặt trong các hệ thống tài chính ngân hàng cho báo cáo luận văn Thạc sĩ của mình.

CHƯƠNG 1: GIỚI THIỆU CÔNG NGHỆ BLOCK CHAIN

1.1. Tổng quan về công nghệ Blockchain

1.1.1. Khái niệm

Satoshi Nakamoto (một người chưa rõ danh tính) đã xuất bản một bài báo trình bày giải pháp cho vấn đề "chi tiêu gấp đôi" đối với tiền kỹ thuật số vào năm 2008. Khi đó, ông đã tiết lộ công nghệ cơ bản được gọi là blockchain và một ví dụ về ứng dụng có thể có của blockchain dưới dạng triển khai đơn giản được gọi là "Bitcoin".

"Bitcoin" đã nhận được sự chú ý rộng rãi kể từ thời điểm đó. Cơ chế cơ bản, blockchain, cũng đã được công nhận và đã tìm thấy các ứng dụng trong các bối cảnh đa dạng. Thật vậy, thế giới đã phát hiện ra rằng các nguyên tắc của blockchain hữu ích trong nhiều bối cảnh và có thể có nhiều biến thể của việc triển khai ban đầu.

Blockchain là một công nghệ phức tạp và phát triển nhanh chóng. Phải mất nhiều trí tuệ sáng suốt trong nhiều năm phát triển, cộng với sự kết hợp của những tiến bộ trong mật mã, điện toán phân tán và kinh tế học để tạo ra công nghệ hiện tại. Blockchain được thiết kế để chống lại việc thay đổi của dữ liệu: Một khi dữ liệu đã được cập nhật trong mạng thì sẽ khó có thể thay đổi được nó. Thông tin đã lưu trong Blockchain thì không thể bị thay đổi và chỉ được bổ sung thêm khi có sự đồng thuận của tất cả các nút trong hệ thống. Ngay cả khi nếu một phần của hệ thống Blockchain sập đổ, những máy tính và nút khác sẽ tiếp tục hoạt động để bảo vệ thông tin. Đặc biệt, Blockchain có khả năng truyền tải dữ liệu mà không đòi hỏi trung gian để xác nhận thông tin. Hệ thống Blockchain bao gồm nhiều nút độc lập có khả năng xác thực thông tin.

Công nghệ Blockchain là sự kết hợp của 3 yếu tố dưới đây:

- Mật mã học: public key và hàm hash function được sử dụng để đảm bảo tính minh bạch, toàn vẹn và riêng tư.
- Mạng ngang hàng: Mỗi một nút trong mạng được xem như một client và cũng là server để lưu trữ của bản sao ứng dụng.
- Lý thuyết trò chơi: Tất cả các nút trong hệ thống đều phải tuân thủ theo luật

chơi đồng thuận (PoW, PoS, …) nhất định và được thúc đẩy bởi động lực kinh tế. Lý tưởng cơ bản của Blockchain là phi tập trung (dencentralized), nơi cộng đồng có quyền quyết định mọi vấn đề mà không cần một trung gian (như nhà nước, ngân hàng, tổ chức hành chính…). Blockchain được ví như cuốn sổ cái phân tán (distributed ledger) mã nguồn mở (open source) nơi mọi thông tin được lưu trữ minh bạch và không bị sửa đổi.

Công nghệ Blockchain là một loại chương trình để lưu, xác nhận, vận chuyển và truyền thông dữ liệu trong mạng thông qua các nút phân phối của riêng nó mà không phụ thuộc vào bên thứ ba.

Theo một cách nào đó, blockchain, với tư cách là một hệ thống phân tán, tự phụ trách chính nó. Việc tham gia vào hệ thống giao dịch vẫn bị chi phối bởi các quy tắc được xác định trong giao thức và được thực thi bởi tất cả những người tham gia. Tuy nhiên, một người tham gia trung thực sẽ đóng góp vào việc thực thi các quy tắc giao thức.

Thử nghiệm trong quản trị chuỗi cho thấy các phương pháp tiếp cận để quản lý sự phát triển của cấu trúc phần thưởng và thậm chí cả các quy tắc quản trị, đồng thời hạn chế sự phát triển của hệ thống và tránh những thay đổi lớn trừ khi hầu hết người dùng đồng ý.

1.1.2. Mạng ngang hàng (Peer to Peer Network)

Mạng ngang hàng là một kiến trúc mạng phân phối, trong đó mỗi nút tham gia (máy tính) chia sẻ tài nguyên phần cứng của nó như máy tính, dung lượng lưu trữ, liên kết mạng với nhau.

Về bản chất, hệ thống ngang hàng được duy trì bởi một mạng lưới người dùng phân tán. Mạng này thường không có quản trị viên trung tâm hoặc máy chủ vì mỗi nút lưu trữ một bản sao của các tệp và mỗi nút đóng vai trò như một máy khách và máy chủ cho các nút khác. Do đó, mỗi nút có thể tải tệp về từ các nút khác hoặc tải lên tệp cho các nút khác. Đây là điểm khác biệt giữa các mạng ngang hàng với các hệ thống máy chủ-máy khách truyền thống hơn, trong đó các thiết bị máy khách tải xuống các tệp từ một máy chủ tập trung.

Trên mạng ngang hàng, các thiết bị được kết nối chia sẻ các tệp được lưu trữ trên ổ cứng của chúng. Sử dụng các ứng dụng phần mềm được thiết kế để làm trung gian cho việc chia sẻ dữ liệu, người dùng có thể truy vấn các thiết bị khác trên mạng để tìm và tải xuống các tệp. Khi người dùng đã tải xuống một tệp, họ có thể đóng vai trò là nguồn của tệp đó.

Nói cách khác, khi một nút hoạt động như một máy khách, họ tải xuống dữ liệu từ các nút khác trên mạng. Nhưng khi họ hoạt động như một máy chủ, họ là nguồn mà các nút khác có thể tải xuống dữ liệu. Tuy nhiên, trên thực tế, các nút có thể thực hiện hai chức năng cùng một lúc (ví dụ: tải xuống dữ liệu A và tải lên dữ liệu B).Vì mỗi nút đều có chức năng lưu trữ, truyền và nhận tệp, mạng ngang hàng có xu hướng hoạt động nhanh và hiệu quả hơn khi cộng đồng người dùng của họ phát triển lớn hơn. Ngoài ra, kiến trúc phân tán của họ làm cho các hệ thống P2P có khả năng chống lại các cuộc tấn công mạng rất cao. Không giống như các mô hình truyền thống, mạng P2P không có sự hư hỏng tại một điểm. Các tài nguyên này được sử dụng để cung cấp các dịch vụ như chia sẻ nội dung và chia sẻ tập tin và có sẵn cho tất cả các nút trực tiếp mà không cần bất kỳ máy chủ trung tâm nào.

Một mạng ngang hàng đúng nghĩa thì không có khái niệm máy chủ và máy khách, hay nói cách khác, tất cả các máy tham gia đều bình đẳng như nhau và được gọi là 1 peer, là một nút mạng đóng vai trò đồng thời là máy khách và máy chủ đối với các máy khác trong mạng.

Mang ngang hàng cũng được sủ dụng để ẩn danh định tuyến lưu lượng mạng, máy tính song song, lưu trữ tập tin phân tán, chia sẻ phương tiện truyền thông. Blockchain sử dụng kiến trúc mạng P2P để đảm bảo phân tán, phân quyền mạng và không tồn tại một đơn vị kiểm soát trung tâm.

Kiến trúc ngang hàng là yếu tố cốt lõi của công nghệ blockchain - nền tảng của tiền mã hóa. Có nhiều cách để phát triển và sử dụng kiến trúc ngang hàng. Bằng cách phân tán các sổ cái giao dịch trên một mạng lớn gồm nhiều nút, kiến trúc P2P cung cấp khả năng bảo mật, phi tập trung và chống kiểm duyệt.

1.1.3. Block

Block là một đơn vị trong Blockchain, là khối xây dựng nên Blockchain bao gồm các giao dịch với dữ liệu. Một thợ đào thu thập các giao dịch của một khoảng thời gian nhất định để tạo thành một khối và tính toán hàm băm mật mã. Mã băm này phải có định dạng cụ thể như phải có 4 số 0 như trong Hình 1.1. Để có được loại mã băm này, người thợ đào phải đoán một cách ngẫu nhiên một số tùy ý đưa ra bảng băm với bốn số không hàng đầu. Số độc đoán này được gọi là số được sử dụng một lần hoặc số một lần (nonce). Ngoài ra, quá trình xác định nonce được gọi là khai thác mỏ. Một khối mẫu được thể hiện trong Hình 1.1 trong đó mỗi khối có một số block, nonce, data và hash.

Hình 1.1: Ví dụ về Block

Các giao dịch sau khi được gửi lên trên mạng lưới blockchain sẽ được nhóm vào các khối và các giao dịch trong cùng 1 khối (block) được coi là đã xảy ra cùng thời điểm. Các giao dịch chưa được thực hiện trong 1 khối được coi là chưa được xác nhận.

Mỗi nút có thể nhóm các giao dịch với nhau thành một khối và gửi nó vào mạng lưới như một hàm ý cho các khối tiếp theo được gắn vào sau đó.

Bất kỳ nút nào cũng có thể tạo ra một khối mới. Vậy, câu hỏi đặt ra là: hệ thống sẽ đồng thuận với khối nào? khối nào sẽ là khối tiếp theo?

Hình 1.2: Một chuỗi của các Blocks

Để được thêm vào blockchain, mỗi khối phải chứa một đoạn mã đóng vai trò như một đáp án cho một vấn đề toán học phức tạp được tạo ra bằng hàm mã hóa băm không thể đảo ngược.

Cách duy nhất để giải quyết vấn đề toán học như vậy là đoán các số ngẫu nhiên, những số khi mà kết hợp với nội dung khối trước tạo ra một kết quả đã được hệ thống định nghĩa. Điều này nhiều khi có thể mất khoảng một năm cho một máy tính điển hình với một cấu hình cơ bản có thể đoán đúng các con số đáp án của vấn đề toán học này.

Mạng lưới quy định mỗi khối được tạo ra sau một quãng thời gian là n phút một lần, bởi vì trong mạng lưới luôn có một số lượng lớn các máy tính đều tập trung vào việc đoán ra dãy số này. Nút nào giải quyết được vấn đề toán học như vậy sẽ được quyền gắn khối tiếp theo lên trên chuỗi và gửi nó tới toàn bộ mạng lưới.

Vậy điều gì sẽ xảy ra nếu hai nút giải quyết cùng một vấn đề cùng một lúc và truyền các khối kết quả của chúng đồng thời lên mạng lưới? Trong trường hợp này, cả hai khối được gửi lên mạng lưới và mỗi nút sẽ xây dựng các khối kế tiếp trên khối mà nó nhận được trước tiên.

Tuy nhiên, hệ thống blockchain luôn yêu cầu mỗi nút phải xây dựng trên chuỗi khối dài nhất mà nó nhận được. Vì vậy, nếu có sự không rõ ràng về việc block nào là khối cuối cùng thì ngay sau khi khối tiếp theo được giải quyết thì mỗi nút sẽ áp dụng vào chuỗi dài nhất.

1.1.4. Giao dịch

Giao dịch là một bản ghi chuyển giao tài sản (tiền tệ kỹ thuật số, đơn vị hàng tồn kho, v.v…) giữa các bên. Tương tự như vậy sẽ là một bản ghi trong một tài khoản kiểm tra cho mỗi lần tiền đã được gửi hoặc thu hồi. Bảng 1.1 cho thấy một ví dụ tiêu biểu của một giao dịch. Mỗi khối trong một Blockchain chứa nhiều giao dịch. Một giao dịch đơn lẻ yêu cầu ít nhất các trường thông tin sau, nhưng có thể chứa nhiều hơn:

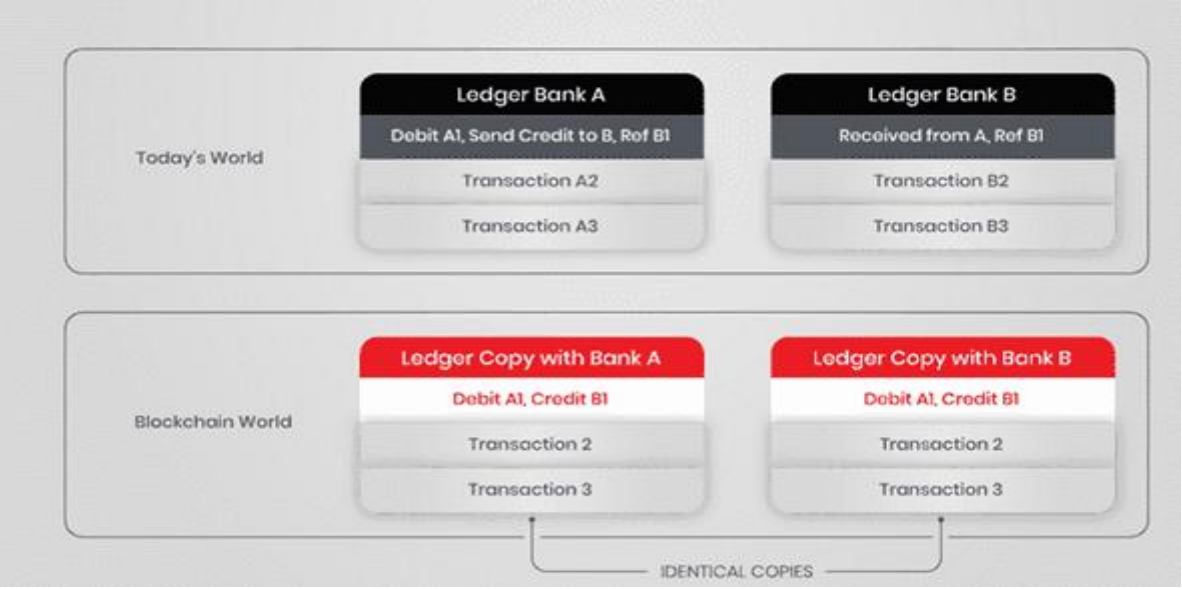
- Amount: Tổng số tiền của tài sản kỹ thuật số để chuyển.
- Input: Một danh sách các tài sản kỹ thuật số sẽ được chuyển giao (tổng giá trị bằng số tiền). Lưu ý rằng mỗi tài sản kỹ thuật số được xác định duy nhất và có thể có các giá trị khác nhau từ các tài sản khác. Tuy nhiên, không thể thêm hoặc xóa tài sản khỏi các tài sản kỹ thuật số hiện có. Thay vào đó, tài sản kỹ thuật số có thể được chia thành nhiều tài sản kỹ thuật số mới (mỗi giá trị nhỏ hơn) hoặc được kết hợp để tạo ít tài sản kỹ thuật số mới hơn (mỗi giá trị có giá trị tương ứng cao hơn).
- Output - Các tài khoản sẽ là những người nhận tài sản kỹ thuật số. Mỗi đầu ra chỉ định giá trị được chuyển giao cho (các) chủ sở hữu mới, danh tính của chủ sở hữu mới và một tập hợp các điều kiện mà chủ sở hữu mới phải đáp ứng để nhận giá trị đó. Nếu tài sản kỹ thuật số được cung cấp nhiều hơn yêu cầu, các khoản tiền bổ sung được trả lại cho người gửi (đây là một cơ chế để "thay đổi").
- ID giao dịch/Hash - Mã nhận dạng duy nhất cho mỗi giao dịch. Một số Blockchains sử dụng một ID, và một số khác sử dụng một hash của giao dịch cụ thể như là một định danh duy nhất.

Bảng 1.1: Ví dụ về 1 giao dịch

	Input	Output		Amount	Total
Transaction ID: 0xa1b2c3	Account A	Account B		0.0321	
		Account C		2.5000	
					2.531

1.1.5. Sổ cái

Sổ cái được coi là một cuốn sổ hoặc tệp tin ghi chép và tổng hợp các giao dịch. Trong suốt lịch sử, sổ ghi chép đã được sử dụng để theo dõi trao đổi hàng hoá và dịch vụ.



Hình 1.2: Sổ cái phân tán

Để có được bức tranh về trạng thái của các tài khoản tại bất kỳ thời điểm nào, người ta phải kiểm đếm tất cả các giao dịch cho đến thời điểm đó. Từng cái một, mọi bản ghi giao dịch đều thay đổi trạng thái.

Mọi giao dịch trong sổ cái đều chứa một bộ dữ liệu tùy ý, tùy thuộc vào mục đích của chúng. Trong sổ cái ghi lại các giao dịch tiền tệ, sổ cái có thể chứa các dữ liệu sau:

- Người gửi
- Người nhận
- Số tiền
- Tín dụng / Ghi nợ
- Tài liệu tham khảo

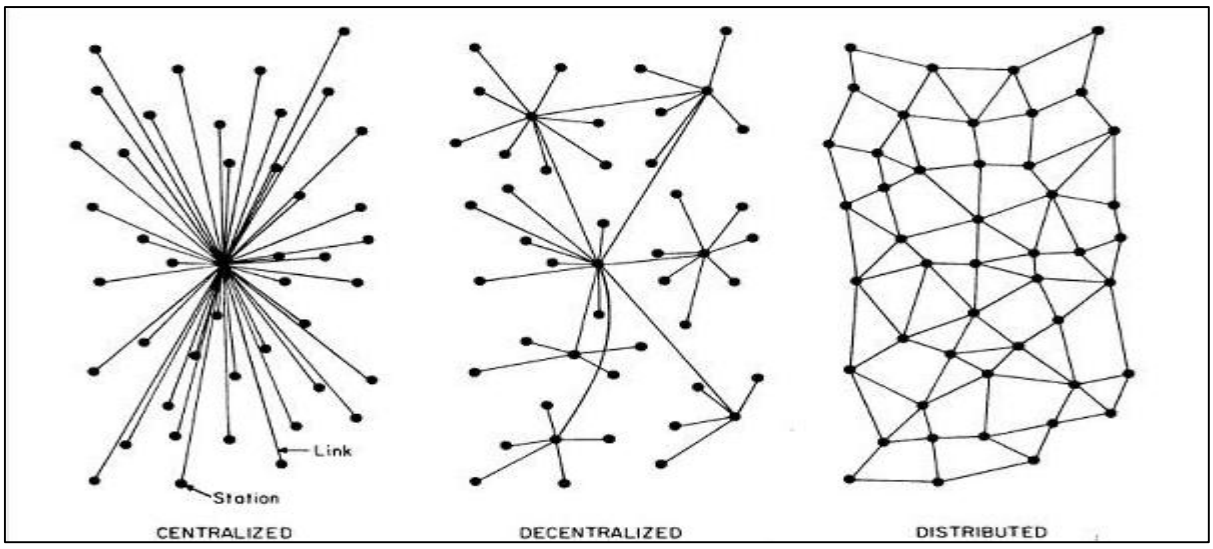
Cuối cùng, dữ liệu được ghi lại phụ thuộc vào cấu trúc và mục đích của sổ cái. Điều này sẽ quan trọng sau này, vì vậy hãy nhớ rằng các giao dịch cuối cùng là các phần dữ liệu được sắp xếp theo thứ tự thời gian.

Xem qua và xử lý từng giao dịch trong sổ cái cho phép chúng ta lấy được tất cả các loại thông tin meta. Điều này có thể bao gồm số lượng giao dịch, hoạt động trên mỗi tài khoản và tất nhiên, số dư tài khoản cá nhân. Số dư tài khoản, giống như số dư tài khoản ngân hàng của bạn, là một bản trình bày và tóm tắt trừu tượng của một danh sách các giao dịch.

Một sổ cái được thực hiện bằng cách sử dụng một Blockchain có thể giảm thiểu những vấn đề này thông qua việc sử dụng cơ chế đồng thuận phân tán. Các sổ cái Blockchain sẽ được sao chép và phân phối giữa các nút trong hệ thống.

1.1.6. Blockchain phân phối phi tập trung

Mức độ phi tập trung có ý nghĩa rất lớn đối với hoạt động của mạng. Vào năm 1964, trước những khám phá và phát triển lớn như hệ thống mã hóa khóa công khai và mạng P2P, Paul Baron đã xuất bản một bài báo về Truyền thông phân tán. Trong đó, ông đã cố gắng phân biệt giữa các mức độ phân quyền đa dạng. Mạng có thể là tập trung, phi tập trung hoặc phân tán.



Hình 1.3: Mô hình phân phối của Blockchain

Trong khái niệm của Baran về mức độ tập trung, ông đã xác định một loạt các cấu trúc liên kết mạng - tập trung và phân quyền là những thuộc tính được giới thiệu từ lâu để mô tả các hệ thống và cấu trúc phân quyền.

Blockchain là sự phân tán các nút trong mạng ngang hàng, nơi tất cả các nút có một bản sao chính xác của Blockchain. Do đó, nếu một mục trong Blockchain được sửa đổi và tái sử dụng, kết quả của mã băm sẽ trở nên khác so với các nút khác. Giao dịch này sẽ bị vô hiệu vì các nút khác sẽ làm mất hiệu lực bản sao này. Tuy nhiên, một thợ đào có thể sửa đổi một mục nhập Blockchain và tái khai thác tất cả các mục nhập băm trên các nút phân phối nếu nó có nhiều quyền lực tính toán hơn các thợ đào khác kết hợp.

1.1.7. Smart Contract

Smart Contract là một thuật ngữ mô tả khả năng tự đưa ra các điều khoản và thực thi thoả thuận của hệ thống máy tính bằng cách sử dụng công nghệ Blockchain. Các điều khoản của Smart Contract có thể coi là tương đương với một hợp đồng pháp lý và được ghi lại dưới ngôn ngữ của máy tính. Toàn bộ quá trình của Smart Contract được lập trình để thực hiện tự động và không thể có sự can thiệp từ bên ngoài.

Smart Contract được viết ra để cho phép hai bên có thể không cần xác định danh tính rõ ràng có thể giao dịch hay làm việc với nhau trên Internet mà không cần thông qua các bên trung gian. Smart Contract có tính an ninh cao, bởi vì được mã hóa và phân phối về cho các nút. Cách thức này đảm bảo không bị thất lạc hay sửa đổi mà không được cho phép.

Về cơ bản Bitcoin là nền tảng đầu tiên hỗ trợ các Smart Contract, Bitcoin là hệ thống có thể chuyển giá trị từ người này sang người khác thông qua công nghệ Blockchain. Các máy tính trong hệ thống chỉ xác nhận giao dịch hợp lệ khi đáp ứng các điều kiện trong Smart Contract. Tuy nhiên Bitcoin chỉ giới hạn ở các trường hợp sử dụng giao dịch tiền tệ mà thôi. Ngược lại, Ethereum đã cải tiến và khắc phục các hạn chế của Bitcoin và thay thế ngôn ngữ hạn chế của Bitcoin thành những ngôn ngữ cho phép các nhà phát triển viết các ứng dụng riêng của họ dựa trên việc lập trình ra các Smart Contract.

Smart Contract chỉ tự động thực hiện những điều khoản đã được lập trình sẵn từ trước khi được điều khoản đó đã đáp ứng đủ những yêu cầu cần thiết.

Đầu tiên, các điều khoản trong hợp đồng sẽ được viết bằng ngôn ngữ lập trình, sau đó được mã hóa và chuyển vào một block thuộc Blockchain. Sau khi chuyển vào block, Smart Contract này sẽ được phân phối và sao chép lại bởi các node đang hoạt động trên nền tảng đó.

Sau khi có nhận lệnh triển khai thì hợp đồng sẽ được triển khai theo đúng như điều khoản định sẵn. Đồng thời, Smart Contract cũng sẽ tự động kiểm tra quá trình thực hiện những cam kết, điều khoản được nêu trong hợp đồng.

1.2. Mật mã trong Blockchain

1.2.1. Hàm băm

Một thành phần quan trọng của công nghệ Blockchain là sử dụng hàm băm mật mã cho nhiều thao tác, chẳng hạn như băm nội dung của một khối. Hashing là phương pháp tính một đầu ra có kích thước cố định cho một đầu vào có kích thước gần như bất kỳ (ví dụ: tệp, văn bản hoặc hình ảnh). Ngay cả sự thay đổi nhỏ nhất của đầu vào sẽ dẫn đến kết quả khác biệt hoàn toàn. Bảng 1.2 cho thấy các ví dụ đơn giản về điều này. Các thuật toán băm được thiết kế theo một chiều, không thể tìm ra bất kỳ đầu vào nào có thể cho bất kỳ đầu ra được xác định trước. Các thuật toán băm cũng được thiết kế để không tìm ra hai hoặc nhiều đầu vào sản xuất cùng một đầu ra.

Một thuật toán băm được sử dụng nhiều trong công nghệ Blockchain là Thuật toán băm an toàn (SHA) với kích thước đầu ra là 256 bit (SHA-256).

Bảng 1.2: Ví dụ về đầu vào và giá trị tiêu biểu SHA-256

Input Text	**SHA-256 Digest Value**
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0x4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Vì có một số lượng lớn các giá trị đầu vào và một số hữu hạn các giá trị có thể xuất ra, nên có thể có va chạm với hash (x) = hash (y) (tức là, băm của hai đầu vào khác nhau tạo ra cùng một giá trị). Tuy nhiên, rất khó xảy ra đối với bất kỳ đầu vào x và y nào tạo ra cùng một tiêu chuẩn để có giá trị trong ngữ cảnh của hệ thống blockchain (trong trường hợp này cả hai đều là các giao dịch blockchain hợp lệ) và cũng như được tính tương đối hợp lý với nhau theo thời gian. Thuật toán băm được sử dụng (SHA-256) được cho là có khả năng chống va chạm, vì để tìm ra va chạm trong SHA-256, một người sẽ phải thực hiện thuật toán, trung bình khoảng 2^{128} lần. Công nghệ Blockchain Mã hóa bất đối xứng in lấy một danh sách các giao dịch và tạo ra một "dấu vân tay" băm cho danh sách. Bất cứ ai có cùng danh sách giao dịch đều có thể tạo ra cùng một dấu vân tay giống nhau. Nếu một giá trị trong một giao dịch trong danh sách thay đổi, thì tiêu chuẩn cho khối đó sẽ thay đổi, và sẽ dễ dàng phát hiện ngay cả một chút thay đổi nhỏ.

1.2.2. Mã hoá bất đối xứng

Mã hóa khóa bất đối xứng, là một dạng mật mã hóa cho phép người sử dụng trao đổi các thông tin mật với nhau mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai (Public Key) và khóa bí mật (Private Key).

Private Key phải được giữ bí mật tuyệt đối trong khi Public Key được phổ biến công khai. Trong 2 khóa, một dùng để mã hóa và khóa còn lại được dùng để giải mã. Điều quan trọng đối với hệ thống đó là không thể tìm ra khóa bí mật nếu chỉ biết khóa công khai.

Hệ thống mật mã hóa khóa công khai có thể sử dụng với nhiều mục đích khác nhau như:

- Mã hóa: giữ bí mật thông tin, dữ liệu và chỉ có người có khóa bí mật mới có thể giải mã được.
- Trình tạo chữ ký số: thực hiện kiểm tra một văn bản xem có phải đã được tạo với một khóa bí mật nào đó hay không.

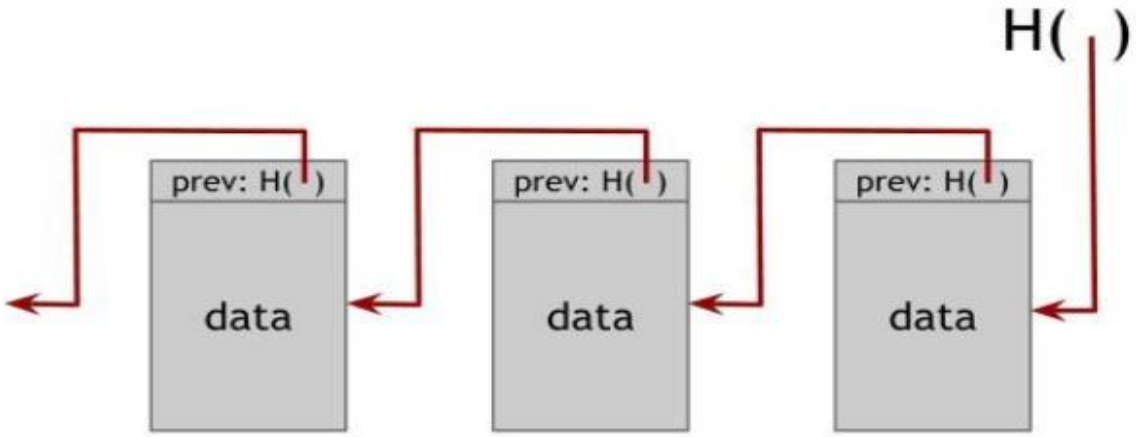
- Thỏa thuận trao đổi khóa: cho phép thiết lập khóa dùng để trao đổi thông tin mật giữa 2 bên.

Một số thuật toán mã hóa bất đối xứng phổ biến hiện nay: Mã hóa đường cong Elliptic, DSS, ElGamal, Diffie-Hellman, , Paillier, RSA (PKCS)…

1.2.3. Con trỏ băm

Con trỏ băm là con trỏ thông thường nhưng có kèm theo giá trị băm của nội dung được trỏ tới. Con trỏ băm vừa trỏ đến dữ liệu vừa lưu giá trị băm của dữ liệu đó. Con trỏ băm được sử dụng để xây dựng các cấu trúc dữ liệu tương tự các cấu trúc dữ liệu được xây dựng bằng con trỏ thông thường, ví dụ như danh sách liên kết hoặc cây nhị phân. Với giá trị băm của dữ liệu được trỏ tới, con trỏ băm giúp ta kiểm tra rằng nội dung của thông tin không bị thay đổi.

Khi sử dụng con trỏ băm thay cho con trỏ thông thường để xây dựng cấu trúc dữ liệu danh sách liên kết thì cấu trúc mới này được gọi là Blockchain. Ở cấu trúc danh sách liên kết thông thường bao gồm một chuỗi các khối (block), mỗi khối này sẽ bao gồm dữ liệu (data) và một con trỏ (pointer) chỉ về khối đằng trước trong chuỗi, đối với cấu trúc Blockchain thì con trỏ ngày được thay thế bằng con trỏ băm (hash pointer).



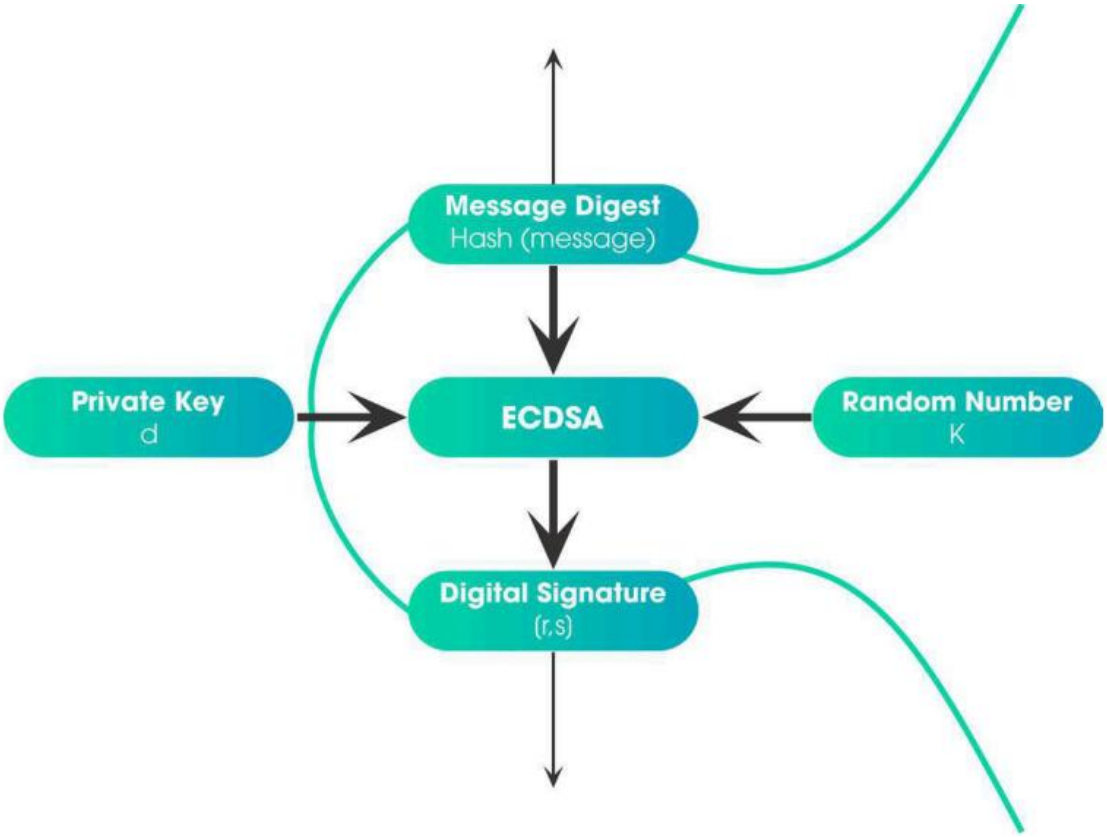
Hình 1.4: Con trỏ băm

Với Blockchain, ở mỗi block sẽ không chỉ trỏ tới block trước đó mà còn lưu giá trị băm của khối được trỏ tới, dùng giá trị băm này ta có thể kiểm tra nội dung của khối được trỏ tới không bị thay đổi.

Với cấu trúc Blockchain như vậy cho phép chỉ cần lưu giá trị của con trỏ chỉ tới khối cuối cùng (heade of the list), nhưng vẫn chắc chắn được là nội dung của cả Blockchain (các khối còn lại) là không bị thay đổi.

1.2.4. Chữ ký số

Chữ ký số là một yếu tố xây dựng khác của Blockchain. Sử dụng mật mã khoá công khai để cung cấp tính toàn vẹn, không truyền lại (nghĩa vụ của tin nhắn được gửi và nhận bởi các bên) và tính xác thực của một thông điệp và nguồn. Chữ ký số có các thuộc tính tương tự như chữ ký tay mà chỉ có thể được phát hành bởi người phát hành và được xác minh bởi những người dùng khác. Một thông điệp được kí bởi chữ ký số có thể được xác minh bởi những người dùng khác, nhưng thông điệp chỉ có thể được kí bởi chủ sở hữu chữ ký. Bên cạnh đó, chữ ký số được tạo ra bằng cách sử dụng mật mã khóa công khai. Mật mã khoá công khai hoặc mật mã bất đối xứng sử dụng khóa chính là sự kết hợp giữa khóa công khai và khóa cá nhân. Khóa cá nhân chỉ được lưu bởi chủ sở hữu trong khi khóa công khai được phân phối cho những người dùng khác. Những người dùng khác có thể mã hóa tin nhắn bằng khóa công khai của chủ sở hữu và chỉ có thể giải mã cho chủ sở hữu bằng khóa cá nhân của họ.



Hình 1.5: Thuận toán chữ ký số ECDSA

Trong đó:

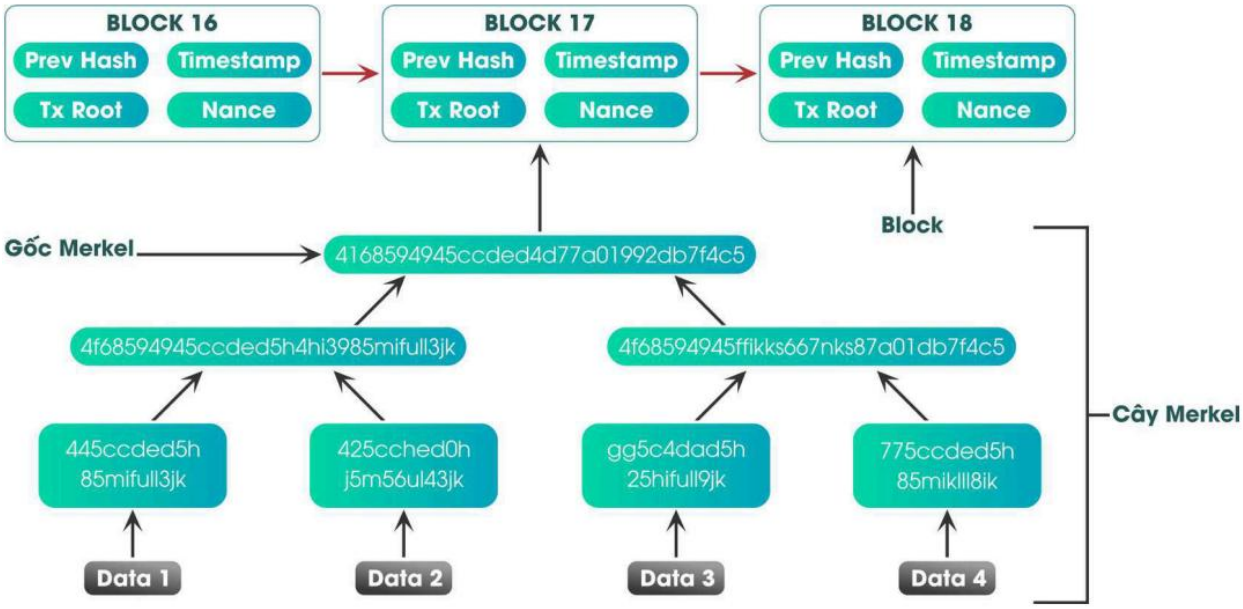
- Message Digest(hash message): Giá trị băm mã hóa của thông điệp
- Private key (d): Khóa cá nhân của người gửi
- Random Number(K): Số ngẫu nhiên K – còn gọi là số Nonce
- Digital Signature(r,s): Chữ ký số được tạo ra nhờ thuật toán ECDSA với 3 yếu tố đầu vào ở trên.

Blockchain sử dụng thuật toán chữ ký số như thuật toán chữ ký số dựa trên đường cong Elliptic (ECDSA) để tạo ra chữ ký số. Có ba bước để tạo, ký và xác nhận thông điệp có chữ ký số. Khoá bí mật (sk) và khóa công khai (pk) được tạo ra bằng phương thức tạo khóa lấy kích thước khóa làm tham số. Các sk được giữ chỉ bởi chủ sở hữu và pk được phân phối qua các nút Blockchain. Thông điệp được ký kết bằng cách sử dụng sk. Phương thức đăng nhập lấy sk và thông điệp như đầu vào và tạo ra chữ ký của thông điệp. Chữ ký này có thể được xác minh bởi các nút bằng

cách sử dụng phương pháp xác minh lấy pk, thông điệp và chữ ký làm đầu vào. Nếu kết quả trả về đúng thì thông điệp sẽ được kiểm tra nếu không nó sẽ bị vô hiệu. Do đó, khoá công khai đảm bảo thông điệp đã được tạo ra bởi chủ sở hữu chữ ký và với sự thẩm tra của thông điệp, nhận dạng người dùng được xác minh. Sử dụng Blockchain phân phối, người dùng không cần cung cấp số an sinh xã hội, số điện thoại, email cho bất kỳ máy chủ trung tâm hoặc cơ quan nào. Người dùng có thể tạo nhận dạng kỹ thuật số của mình và phân phối khóa công khai của mình tới mạng phân phối. Trong Blockchain các bản sao của tất cả các giao dịch được phân phối đến tất cả các nút, có nghĩa là một nút có thể xem tất cả lịch sử của tất cả các giao dịch. Do đó, một nút có thể quan sát lịch sử của người dùng và có thể liên kết hoặc đoán danh tính. Vì vậy, Blockchain cung cấp giả mạo hơn là ẩn danh thực.

1.2.5. Cây Merkle

Blockchain sử dụng mạng P2P, trong đó mỗi nút mạng phải có cùng một bản sao của dữ liệu và dữ liệu mới phải được truyền và kiểm tra qua mạng. Truyền và xác minh dữ liệu qua mạng P2P tốn nhiều thời gian và tốn kém về mặt tính toán. Do đó, cây Merkle được sử dụng, thay vì gửi dữ liệu chỉ băm của dữ liệu được gửi đi và người nhận kiểm tra các băm chống lại thư mục gốc của cây Merkle cho phép xác minh an toàn và xác minh các cấu trúc dữ liệu lớn hơn cũng như đảm bảo tính toàn vẹn dữ liệu. Cây Merkle là cây nhị phân của các con trỏ băm đảm bảo rằng tất cả các nút phải có cùng một dữ liệu không bị phá hoại, sửa đổi dữ liệu hợp pháp và nếu một dữ liệu bị thay đổi trong một nút, thay đổi phải được truyền đến các nút khác trong hệ thống. Cây Merkle bao gồm một số lượng lớn các khối có chứa dữ liệu hoặc các giao dịch như thể hiện trong hình. Các khối này tạo thành các lá của cây Merkle và các khối giao dịch được nhóm lại thành hai cặp, trong đó mỗi cặp có các con trỏ băm tương ứng mà cuối cùng, làm cho cấp độ tiếp theo của cây. Quá trình này được lặp lại cho đến khi khối đơn đạt được như thể hiện trong hình và khối đơn được gọi là gốc băm.



Hình 1.6: Mô hình minh họa cho cây Merkle Tree

Có bốn giao dịch TX1, TX2, TX3 và TX4 ở phía dưới cùng, bốn dữ liệu giao dịch đi qua một hàm băm để tạo ra bốn giá trị băm. Các cặp giá trị băm được kết hợp và truyền qua hàm băm tạo ra hai giá trị băm duy nhất. Hai giá trị băm này lại được kết hợp và một lần nữa truyền vào hàm băm tạo ra một giá trị băm duy nhất mà kết quả là tạo thành cây Merkle hoàn chỉnh. Cây Merkle cho phép phát hiện bất kỳ thay đổi nào đối với bất kỳ dữ liệu nào trong giao dịch khối bằng cách chạy lại quá trình giao dịch và so sánh kết quả của giá trị băm nguyên bản. Nếu một người dùng cố gắng thay đổi hoặc trao đổi một giao dịch ở phía dưới, nó sẽ gây ra những thay đổi trong giá trị băm của các nút phía trên, và như vậy sẽ hoàn toàn thay đổi gốc của cây. Nói cách khác, sự băm của khối sẽ cho kết quả là một khối mới hoàn toàn và trở thành khối không hợp lệ. Dữ liệu trong khối mới này sẽ được truyền tới các nút khác, những người dùng khác sẽ phát hiện ra thay đổi bằng cách so sánh các giá trị băm riêng của mình. Do đó, bất kì thay đổi nào với các giá trị băm của cây Merkle đều dẫn đến kết quả không hợp lệ.

1.3. Phân loại các hệ thống Blockchain

Hệ thống Blockchain thường được phân chia thành 3 loại: Public, Private và Permissioned, trong đó:

1.3.1. Blockchain công khai

Cách rõ ràng nhất để vận hành các giao thức blockchain là ở dạng công khai. Đây là công nghệ blockchain ban đầu được phát minh và vẫn được cho là được ứng dụng mạnh mẽ nhất.

Đây là loại Blockchain mà bất kỳ ai cũng có quyền đọc và ghi dữ liệu. Quá trình xác thực giao dịch trên hệ thống Blockchain này đòi hỏi phải có hàng nghìn (thậm chí nhiều hơn) nút (Node) tham gia. Vì vậy, hệ thống Blockchain này được đánh giá khá an toàn (vì chi phí để thực hiện một vụ tấn công vào hệ thống là khá cao). Điển hình cho loại Blockchain này là các đồng tiền điện tử như Bitcoin, Ethereum…

1.3.2. Blockchain bí mật

Có nghĩa là quyền truy cập được giới hạn cho các thành viên và các thành viên luôn được biết đến nhau. Những người tham gia được biết đến với nhau và họ đã quyết định cùng nhau thành lập một mạng lưới.

Người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi (quyền này thuộc về một tổ chức bên thứ 3 với độ tin cậy tuyệt đối). Bên thứ 3 có toàn quyền quyết định mọi thay đổi trên Blockchain. Thời gian xác thực giao dịch đối với Private Blockchain khá nhanh (vì chỉ cần một lượng nhỏ thiết bị tham gia vào giao dịch). Ripple là một dạng Private Blockchain, hệ thống này chỉ cần 80% các nút hoạt động ổn định là có thể tiến hành giao dịch.

Cũng có khả năng một số nút có các vai trò hoặc đặc quyền khác nhau. Những người tham gia có thể tạo ra một cấu trúc liên kết được cả hai đồng ý mà không mang lại cho bất kỳ người tham gia nào một lợi thế cụ thể không công bằng.

Mạng private Blockchain sử dụng các trạng thái được chia sẻ và bằng chứng mật mã để phát hiện và đẩy lùi các hành vi không đúng. Nó làm như vậy theo một cách độc đáo thích nghi với môi trường mà nó được thiết kế.

1.3.3. Blockchain cấp quyền

Là hệ thống đóng và chỉ dành cho những người được phép truy cập. Bất cứ ai muốn xác thực các giao dịch và/hoặc xem dữ liệu trên mạng, trước tiên phải được central authority (bộ phận trung tâm, chịu trách nhiệm quản lý chính) chấp thuận.

Nó đặc biệt hữu ích cho các ngân hàng, công ty và những tổ chức khác phải tuân thủ các quy định và không muốn mất quyền kiểm soát hoàn toàn dữ liệu.

Những lợi thế lớn của permissioned blockchain là chúng có:

- Quyền kiểm soát truy cập
- Khả năng tùy biến cao
- Thay đổi thời gian dễ dàng hơn để tuân thủ các quy định
- Hiệu quả năng lượng tốt hơn
- Khả năng mở rộng tốt hơn

Tuy nhiên, chúng cũng có những nhược điểm. Đó là:

- Tập trung hơn
- Ít minh bạch
- Dễ bị tấn công và thao túng hơn
- Dễ dàng kiểm duyệt hơn
- Khó ẩn danh hơn

1.4. Các cơ chế đồng thuận

Là một quá trình ra quyết định của nhóm trong chính các thành viên trong nhóm phát triển, và đồng ý hỗ trợ một quyết định vì lợi ích tốt nhất của toàn bộ nhóm. Đồng thuận có thể được định nghĩa một cách chuyên nghiệp như một giải pháp được chấp nhận, được hỗ trợ, thậm chí khi không phải là "sự yêu thích" của mỗi cá nhân. Sự đồng thuận được định nghĩa bởi Merriam-Webster là, đầu tiên, như là thoả thuận chung, và thứ hai là, sự đoàn kết nhóm niềm tin hoặc ý kiến.

Nói một cách đơn giản, sự đồng thuận là một cách năng động để đạt được thỏa thuận trong một nhóm. Trong khi bỏ phiếu chỉ giải quyết cho một nguyên tắc đa số mà không có bất kỳ suy nghĩ nào về cảm xúc và phúc lợi của người thiểu số, trong khi một sự đồng thuận đảm bảo rằng một thỏa thuận đạt được có thể đem lại lợi ích cho toàn bộ nhóm.

Trong một mạng lưới phân tán không có cơ quan chức năng, những người tham gia cần một quá trình để đạt được sự đồng thuận về những gì được coi là sự thật;

Từ một quan điểm lý tưởng hơn, đồng thuận có thể được sử dụng bởi một nhóm người rải rác khắp thế giới để tạo ra một xã hội bình đẳng và công bằng hơn.
Một phương pháp tạo ra sự ra quyết định đồng thuận được gọi là "cơ chế đồng thuận".

1.4.1. Đồng thuận theo bằng chứng công việc.

Trong thực tế khái niệm này xuất hiện trước cả khi tiền mã hóa ra đời. Ý tưởng này lần đầu được công bố bởi Cythia Dwork và Moni Naor vào năm 1993, tuy nhiên cho đến năm 1999, cụm từ này mới được hình thành.

Satoshi Nakamoto, tác giả của Bitcoin, người đầu tiên đã đã vượt qua được vấn đề của Blockchain bằng cách sử dụng bằng chứng minh về công việc.

Việc đề xuất sử dụng Proof-of-Work còn nhằm mục đích đề phòng một thế lực có thể nắm trong tay quyền kiểm soát cả một hệ thống. Cách giải quyết vấn đề đồng thuận này không chỉ đơn thuần bằng cách sử dụng phương pháp mật mã mà còn có sự kết hợp của phần cứng máy tính.
Khi một block mới được tìm thấy, nó sẽ được công bố trên toàn mạng để các node khác kiểm tra. Nếu mọi tính toán, giao dịch trong block đó chính xác, các node sẽ cập nhật vào bản sao blockchain (Iedger — số cái) đang lưu trữ cục bộ tại node đó. Vấn đề mâu thuẫn xảy ra là vì khoảng cách địa lý, có thể gây ra hiện tượng cùng một thời điểm các node sẽ lưu trữ hai hoặc nhiều hơn các phiên bản blockchain không đồng nhất. Ví dụ, các nước ở châu Mỹ đang có chuỗi blockchain là ...P —>A, còn các nước châu Á có chuỗi blockchain là ...P —›B.

Việc mining (đào) lúc này vẫn diễn ra bình thường. Sau đó, một block X mới được tìm thấy từ một node ở khu vực châu Á đang lưu trữ chuỗi hiện tại là ...P —>B, và chuỗi blockchain sẽ được cập nhật lại là ... P—>B —X. Khi blockchain mới này được thông báo đến các node ở khu vực châu Mỹ, lúc này sẽ có sự mâu thuẫn xảy ra là xuất hiện 2 chuỗi không đồng nhất là chuỗi ...P —A và chuỗi ... P —>B —X. Theo luật quy định của Proof-of-Work, chuỗi blockchain nào dài hơn thì sẽ thành chuỗi chính. Do đó, các node ở châu Mỹ phải cập nhật lại chuỗi blockchain mới là ... P —>B —>X. Khi đó sự thống nhất của chuỗi blockchain trên hệ thống được đảm bảo.
Vấn đề cốt lõi của thuật toán đồng thuận theo bằng chứng công việc là phải sử dụng

một nguồn tài nguyên máy tính lớn và cần thiết nhiều năng lượng điện cung cấp cho hệ thống máy tính nhằm có được đáp án tối ưu. Nếu nhìn về khía cạnh sinh thái thì điều này hoàn toàn không có lợi chút nào. Các thợ đào phải sử dụng quá nhiều năng lượng và gây ảnh hưởng xấu đến môi trường. Để đào được Bitcoin (hoặc các đồng coin sử dụng thuật toán đồng thuận theo bằng chứng công việc) thợ đào cần phải có một số lượng lớn sức mạnh tính toán, nhiều hơn sức mạnh mà một máy tính bình thường đang có. Điều này sẽ khiến cho cộng đồng các thợ đào gom cụm lại với nhau hình thành nên các mining-pool. Những thợ đào nhỏ lẻ sẽ không cạnh tranh được với các thợ đào lớn hơn, tạo ra sự độc quyền trong khai thác từ các nhóm thợ đào lớn. Vì với sức mạnh tính toán lớn hơn thì xác suất tìm ra đáp án đúng và nhanh hơn thợ đào nhỏ lẻ rất nhiều.

Đồng thuận theo bằng chứng công việc và blockchain chứng minh rằng một tập hợp các nút không biết hoặc nhất thiết phải tin tưởng lẫn nhau có thể tạo thành một sự đồng thuận về một tập hợp các sự kiện. Các quy trình đơn giản của Bitcoin, tức là logic kinh doanh, thực thi một cách đáng tin cậy trên một nền tảng phân tán vì sự đồng thuận không quan tâm đến các yếu tố đầu vào khỏi các nút tấn công hoặc trục trặc.

Lịch sử được chia sẻ đáng tin cậy, trạng thái được chia sẻ và các quy trình hóa chặt chẽ mà không cần một người lưu giữ sổ cái tập trung đã truyền cảm hứng cho suy nghĩ mới về cách xây dựng hệ thống cho ngành dịch vụ tài chính được quản lý.

1.4.2. Đồng thuận theo bằng chứng cổ phần.

Cơ chê đông thuận theo bằng chứng cổ phần được nêu ý tưởng lần đầu tiên trên diễn đàn bitcointalk.org vào năm 2011, đồng coin đâu tiên sử dụng thuật toán đông thuận này là Peercoin cùng với ShadowCash, NXT, BlackCoin, NuShares / NuBits, Qora và Nav Coïn vào năm 2012.

Cơ chế đồng thuận theo bằng chứng cổ phần cũng có chung một mục đích với đồng thuận theo bằng chứng công việc là cung cấp phương thức đồng thuận cho mạng lưới blockchain và chăn chặn hiện tượng lặp chi. Tuy nhiên chúng khác nhau ở cách vận hành do đồng thuận theo bằng chứng cổ phần không có câu đố toán học nào để

giải quyết như đồng thuận theo bằng chứng công việc, thay vào đó người ta tạo khối dựa vào cổ phần. Ví dụ một người trữ được 100 coin trong ví, người khác trữ được 1000 coin, thì người giữ 1000 coi có xác suất được chọn làm người xác nhận cao gấp 10 lần trong việc tạo ra khối mới. Về bản chất sẽ không có coin nào sinh ra thêm, tất cả coin được tạo ra ngay từ ban đầu. Thuật toán đồng thuận theo bằng chứng cổ phần hoạt động khi một thợ đúc góp cổ phần của mình vào để xác minh cho 1 khối dao dịch, việc này khá đơn giản và không yêu cầu cấu hình phần cứng máy tính mạng. Quy mô khai thác sẽ tỉ lệ tuyến tính với số lượng cổ phần sở hữu. Điều này giúp khuyến khích cộng đồng tham gia vào việc xác nhận giao dịch, tang khả năng phân quyền và dân chủ.

1.4.3. Ủy nhiệm đồng thuận theo bằng chứng cổ phần.

Một phần mở rộng của thuật toán bằng chứng cổ phần được gọi là bằng chứng cổ phần được ủy quyền (DPoS).

Cơ chế đồng thuận này được khởi xướng bởi Daniel Larimer nhà sáng lập của Bitshares (BTS) đồng thời ông cũng là giám đốc công nghệ của EOS. 1.4.3. Ủy nhiệm đồng thuận theo bằng chứng cổ phần là cách thức để gia tăng tốc độ giao dịch và tạo khối của mạng lưới mà vẫn không ảnh hưởng đến "cấu trúc phần thưởng khuyến khích phi tập trung" cơ bản của blockchain. Trong cơ chế đồng thuận theo bằng chứng cổ phần cơ bản, người dùng có thể đặt số coin của họ vào việc staking do đó họ có quyền xác thực các giao dịch, đúc ra khối mới và tìm kiếm các phần thưởng khuyến khích liên quan. Còn ủy nhiệm đồng thuận theo bằng chứng cổ phần là một biến thể của đồng thuận theo bằng chứng cổ phần nhằm mục đích tìm kiếm cách thức đạt được sự đồng thuận trong mạng lưới một cách hiệu quả hơn.

Người dung bỏ phiếu chọn ra các chứng nhân, là các người dùng tin tưởng bầu chọn bở các người dung khác, để thực hiệc việc xác minh các giao dịch. Các nhân chứng hang đầu là những người thu được nhiều phiếu bầu nhất và sẽ có quyền xác minh các giao dịch cho hệ thống.

1.4.4. Đồng thuận theo bằng chứng ủy quyền.

Cơ chế đồng thuận đồng thuận theo bằng chứng ủy quyền được giới thiệu lần đầu tiên bởi dự án cùng tên là POA Network (tên trước đó là Oracle Network). Hiện

nay việc xây dựng một dịch vụ/ứng dụng trên một blockchain công khai (publie blockchain) gặp phải hai vấn đề lớn là rào cản kỹ thuật khi tham gia vào mạng lưới và chỉ phí đầu vào đề tham gia tương đối cao, nên nhiều doanh nghiệp nhỏ và vừa sẽ bị loại khỏi việc ứng dụng và hưởng lợi từ công nghệ blockchain. Với mong muốn khắc phục tình trạng trên, dự án này sử dụng thuật toán đồng thuận theo bằng chứng ủy quyền nhằm mục tiêu đơn giản hóa quá trình khởi tạo và thực thi các ứng dụng phi tập trung (DApp). đồng thời tăng tốc độ, nâng cao tính bảo mật và giảm chỉ phí với mức phí phải chăng (những ưu điểmtrước đây chỉ xuất hiện trên các private blockchain) để tạo điều kiện dễ dàng hơn cho các doanh nghiệp này tiếp cận với công nghệ blockchain.

Đồng thuận theo bằng chứng ủy quyền là một cơ chế được dùng để kiểm định và xác nhận giao dịch bằng những node có bằng chứng nhân thân tốt (không có hành vi sai trái nào trước đó), hoặc có địa vị/danh tiếng nhất định trong mạng lưới, nghĩa là các node này đều phải có đăng ký danh tính rõ ràng tuân theo một số yêu cầu về xác minh bản thân, đòi hỏi phải có địa chỉ chứng thực và không có bất cứ lý lịch xấu nào trong quá khứ. Điều này giảm thiểu những tác động tiêu cực từ các node xấu đem lại và đảm bảo cho kết quả cuối cùng là hợp lệ, chính xác, không chịu sự thâu tóm hoặc can thiệp của bắt kì ai. Cơ chế đồng thuận theo bằng chứng ủy quyền chỉ sử dụng danh tính người dùng làm căn cứ duy nhất để xác minh quyền xác nhận ra block giao dịch mới mà không cần đến những thuật toán "đào/đúc".

Hay nói cách khác, trong cơ chế theo bằng chứng cổ phần, cổ phần (stake) được đo lường bằng giá trị tiền tệ (số lượng coin mà người tham gia staking sỡ hữu) thì khái niệm cổ phần (stake) trong cơ chế đồng thuận theo bằng chứng ủy quyền chính là "danh tính" của người xác nhận giao dịch. "Danh tính" ở đây phải có sự trùng khớp giữa "định danh cá nhân của người xác nhận giao dịch" với "tài liệu thông tin nhân thân được phát hành chính thức trên hệ thống" là của cùng một người, mọi người dùng của mạng lưới đều biết chắc chắn rằng người thực hiện xác nhận các giao dịch chính xác là người đại diện cho ai. "Thông tin định danh — indentity" được xem là một loại "cỗ phần — stake" và chúng có tính "khan hiếm độc nhất" bởi vì một người chỉ có thể có một "danh tính thực" duy nhất.

Người dung chỉ cần cung cấp danh tính và thuật toán của hệ thống sẽ tự động thực hiện toàn bộ quá trình cấp quyền, tích lũy điểm uy tín cho đến quá trình thực hiện giao dịch.

1.5. Phương thức hoạt động của Blockchain

Phương thức hoạt động của Blockchain gồm có 5 bước: Định nghĩa giao dịch, xácthực giao dịch, tạo khối, xác nhận khối, chuỗi khối.

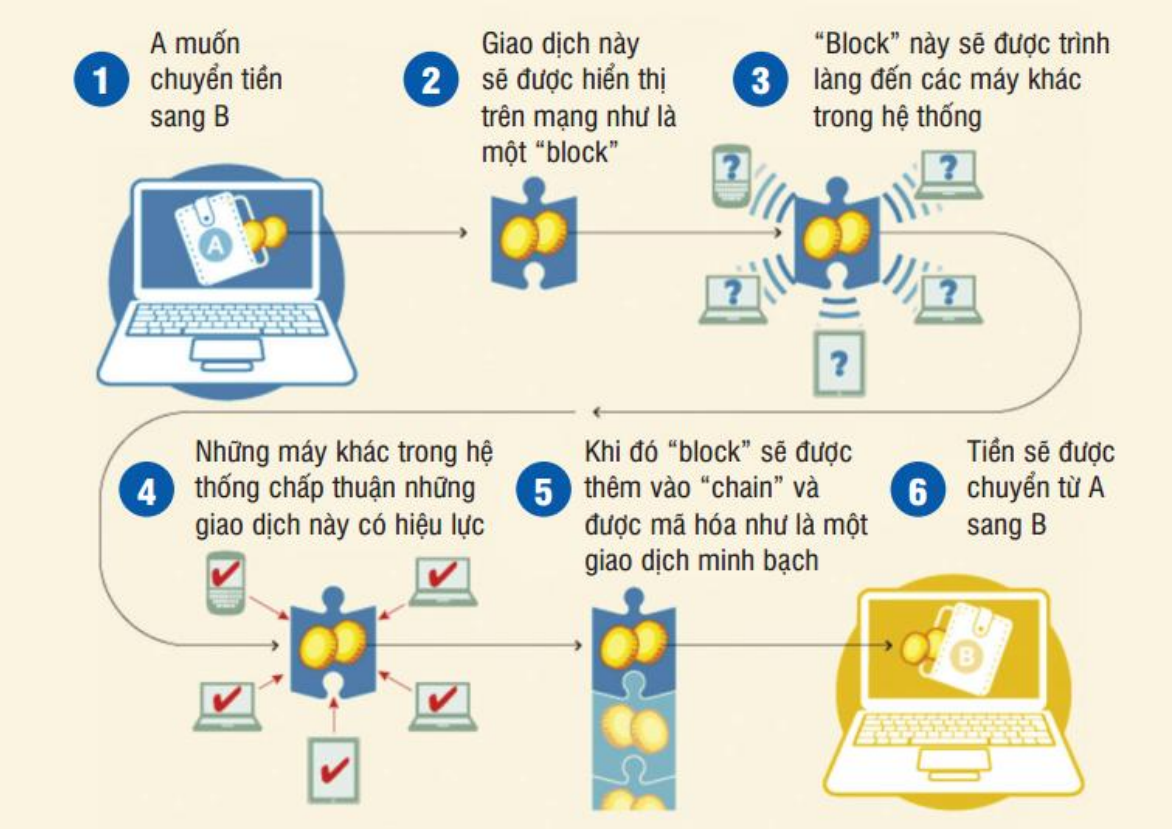
Định nghĩa giao dịch là mô hình của giao dịch được xác định trước bởi mạng lưới Blockchain, gồm chữ ký số của người gửi, trọng tải của giao dịch, khóa công khai của người nhận được kí kết mật mã với khóa kĩ thuật số được bảo vệ bởi người gửi.

Xác thực giao dịch là quá trình mà các nút xác nhận nếu một tài khoản A có tài sản, đủ số dư tài sản để thực hiện giao dịch.

Tạo khối là quá trình tạo ra khối bởi các nút từ các mỏ giao dịch, nơi giao dịch được nhóm lại với nhau dựa trên thời gian tạo.

Xác nhận khối là quá trình xác nhận xem khối có hợp lệ không bằng cách kiểm tra PreHash và Nonce.

Chuối khối là quá trình bổ sung khối cho Blockchain một khi các nút đạt được sự đồng thuận.



Hình 1.7: Cách hoạt động của Blockchain

Một ví dụ về cách hoạt động của công nghệ Blockchain được thể hiện như trong hình. Trong đó user A chuyển một tài sản kỹ thuật số sang User B, tài sản có thể là tiền hoặc hợp đồng thông minh. Đầu tiên cả hai người dùng tạo nhận dạng số, có thể gọi đây là một chiếc ví Blockchain riêng của mỗi người dùng. A cần khóa cá nhân của mình và khóa công khai của B để tạo ra một giao dịch. A nhận khoá công khai của B bằng cách quét mã QR của B hoặc B gửi khoá công khai tới A thông qua email. A tạo ra giao dịch được ký kết với khóa cá nhân của mình và phát sóng vào mạng lưới Blockchain. Các nút trong mạng lưới xác nhận giao dịch và xác minh tính xác thực của A. Nếu xác nhận thất bại, giao dịch bị loại bỏ, còn nếu xác nhận thành công nó sẽ được nhóm lại cùng với giao dịch đang chờ xử lý từ các mỏ giao dịch và một khối mới sẽ được tạo ra. Khối này được truyền đến các nút khác và một khi đạt được sự đồng thuận thì khối sẽ được thêm vào chuỗi Blockchain trở thành vĩnh viễn.

Cuối cùng, giao dịch được xác nhận và tài sản được chuyển từ A sang B. Ngoài ra, tùy thuộc vào mạng lưới Blockchain, có thể mất 2 phút đến 10 phút để các giao dịch được xác nhận. Ví dụ: Bitcoin 4.1 mất trung bình 10 phút trong khi Ethereum 4.3 mất 2 phút để xác định các giao dịch.

1.8. Ưu nhược điểm của công nghệ Blockchain

1.8.1. Ưu điểm

- Tính minh bạch: Công nghệ Blockchain mang đến nhiều bước tiền trong việc cải thiện tính minh bạch.
- Tính phi tập trung: Các hệ thống được xây dựng dựa trên công nghệ Blockchain có thể hoạt động trên mạng lưới máy tính phi tập trung, từ đó giảm thiểu các rủi ro bị tấn công, thời gian chết trên máy chủ và gây thất thoát dữ liệu.
- Loại bỏ đơn vị trung gian: Các hệ thống được xây dựng dựa trên công nghệ Blockchain cho phép có thể loại bỏ các đơn vụ trung gian liên quan đến hoạt động lập hồ sơ, ghi chép dữ liệu và chuyển giao tài sản.
- Sự tin cậy: Các hệ thống xây dựng dựa trên công nghệ Blockchain làm gia tăng niềm tin giữa các bên giao dịch nhờ tính minh bạch được cải thiện và mạng lưới phi tập trung và đồng thời loại bỏ được các đơn vị trung gian không cần thiết.
- Tiết kiệm chi phi: Sổ cái thiết lập trên nền tảng Blockchain cho phép loại bỏ đơn vị trung gian và các lớp xác nhận trong giao dịch. Các giao dịch dù cần nhiều sổ cái riêng biệt, đều có thể thiết lập trên một sổ cái chung, từ đó giảm thiểu chi phí kiểm nhận, xác thực và thẩm tra một giao dịch.
- Độ bảo mật: Dữ liệu nhập vào Blockchain sẽ không thể sửa đổi, qua đó tránh được tình trạng gian lận qua việc ngụy tạo giao dịch và giả mạo lịch sử dữ liệu. Các giao dịch đưa vào Blockchain sẽ tạo nên một lịch sử hoạt động rõ rang minh bạch từ điểm khởi đầu của Blockchain, cho phép dễ dàng thẩm tra và kiểm kê mọi giao dịch
- Công nghệ dễ tiếp cận: Cùng với tiềm năng ứng dụng rộng rãi, công nghệ Blockchain còn giúp việc tạo lập các ứng dụng dễ dàng hơn, nhờ các bước tiến hiện nay như nên tảng Ethereum, mà không cần phải đầu tư quá nhiều vào cơ sở

hạ tầng. Các ứng dụng phi tập trung, các hợp đồng thông minh và nền tảng Ethereum.

- Tiềm năng ứng dụng rộng: Đa phần mọi giá trị đều có thể có thể được lập hồ sơ dựa trên Blockchain và nhiều công ty trong nhiều lĩnh vực công nghệ đã phát triển các hệ thống dựa trên công nghệ Blockchain

1.8.2. Nhược điểm

- **Tấn công 51%**

Một cuộc tấn công 51% có thể xảy ra nếu có một đơn vị kiểm soát hơn 50% sức mạnh băm của mạng lưới. Điều này sẽ cho phép đơn vị này phá vỡ mạng lưới bằng cách cố ý ngăn chặn hoặc sửa đổi việc đặt các giao dịch.

Mặc dù về mặt lý thuyết là có thể xảy ra, nhưng thực tế là chưa bao giờ có cuộc tấn công 51% thành công nhắm vào blockchain Bitcoin. Khi mạng lưới phát triển lớn hơn, bảo mật sẽ tăng lên và rất khó có khả năng có thợ đào nào đó sẽ đầu tư số tiền và tài nguyên lớn để tấn công Bitcoin nên tốt hơn cả là thợ đào sẽ hành động trung thực để nhận thưởng. Ngoài ra, một cuộc tấn công 51% thành công sẽ chỉ có thể sửa đổi các giao dịch gần đây nhất trong một khoảng thời gian ngắn vì các khối được liên kết thông qua các bằng chứng mật mã (để thay đổi các khối cũ hơn, sức mạnh tính toán sẽ là không tưởng). Ngoài ra, blockchain Bitcoin rất linh hoạt và sẽ nhanh chóng thích ứng như là một phản ứng trước một cuộc tấn công.

- **Sửa đổi dữ liệu**

Một nhược điểm khác của các hệ thống blockchain là một khi dữ liệu đã được thêm vào blockchain thì việc sửa đổi là rất khó. Mặc dù tính ổn định là một trong những lợi thế của blockchain, nhưng nó không phải lúc nào cũng tốt. Việc thay đổi dữ liệu hoặc mã blockchain thường rất phức tạp và thường cần có một hard fork, trong đó một chuỗi sẽ bị bỏ và một chuỗi mới được đưa lên.

- **Chìa khóa cá nhân**

Blockchain sử dụng mật mã chìa khóa công khai (hoặc bất đối xứng) để cung cấp cho người dùng quyền sở hữu đối với các đơn vị tiền điện tử của họ (hoặc bất kỳ dữ liệu blockchain nào khác). Mỗi tài khoản blockchain (hoặc địa chỉ) có hai chìa khóa tương

ứng: một chìa khóa chung (có thể chia sẻ) và một chìa khóa cá nhân (cần được giữ bí mật). Người dùng cần chìa khóa cá nhân để truy cập vào tiền của họ, nghĩa là tự họ đóng vai trò như một ngân hàng. Nếu người dùng mất chìa khóa cá nhân, tiền sẽ bị mất và không thể làm gì hơn được nữa.

- **Không hiệu quả**

Lý do là vì đào có tính cạnh tranh cao và cứ sau mười phút lại có một người chiến thắng nên công sức của các thợ mỏ khác sẽ bị lãng phí. Khi các thợ mỏ liên tục cố gắng tăng sức mạnh tính toán, họ sẽ có cơ hội tìm được lời giải hợp lệ cao hơn. Do đó các tài nguyên được sử dụng bởi mạng lưới Bitcoin đã tăng đáng kể trong vài năm qua, và hiện tại lượng điện tiêu thụ dành cho bitcoin đã vượt qua nhiều quốc gia, chẳng hạn như Đan Mạch, Ireland và Nigeria.

- **Lưu trữ**

Các sổ cái Blockchain có thể phát triển rất lớn theo thời gian. Blockchain Bitcoin hiện cần khoảng 200 GB dung lượng lưu trữ. Tốc độ tăng kích thước hiện tại của blockchain có vẻ như vượt xa tốc độ tăng dung lượng lưu trữ của các ổ đĩa cứng. Mạng lưới có nguy cơ mất các node nếu kích thước của sổ cái là quá lớn để các cá nhân tải xuống và lưu trữ.

Kết chương

Chương này đã tìm hiểu một số khái niệm cơ bản về công nghệ Blockchain, những thành phần cơ bản cấu tạo nên công nghệ Blockchain như hàm băm, chữ ký số, các cơ chế đồng thuận và cách hoạt động của công nghệ này. Những lợi ích của công nghệ Blockchain là không thể phủ nhận. Tuy nhiên đây là một công nghệ mới và để hoàn thiện được các đặc tính của công nghệ này là cả một bài toán lâu dài. Chương 2 sẽ đi vào tìm hiểu, nghiên cứu nền tảng Corda R3. Một nền tảng hỗ trợ mạnh mẽ việc xây dựng ứng dụng cho doanh nghiệp.

CHƯƠNG 2: NGHIÊN CỨU NỀN TẢNG CORDA R3

2.1. Nền tảng Corda R3

2.1.1. Giới thiệu nền tảng Corda R3

R3 (R3 LLC) là một công ty công nghệ blockchain doanh nghiệp. Nó dẫn đầu một hệ sinh thái gồm hơn 300 công ty cùng nhau xây dựng các ứng dụng phân tán trên Corda (được gọi là CorDapps) để sử dụng trên các ngành công nghiệp như dịch vụ tài chính, bảo hiểm, y tế, tài chính thương mại và tài sản kỹ thuật số.

R3 có trụ sở tại thành phố New York. Nó được thành lập vào năm 2014 bởi David E Rutter. CTO hiện tại là Richard G. Brown.

Corda là một nền tảng sổ cái phân tán (distributed ledger). Được quản lý bởi tổ chức R3, Corda hướng đến mảng doanh nghiệp với các ứng dụng tài chính, thương mại, bảo hiểm, y tế, chuỗi cung ứng v..v, được xây dựng nhằm giảm thiểu các trở ngại trong giao dịch thương mại. Corda được xây dựng dựa trên công nghệ DLT (distributed-ledger-technologies) hay còn gọi là công nghệ sổ cái phi tập trung, mà ứng dụng điển hình là công nghệ Blockchain.

Corda là một blockchain được cấp phép (permissioned blockchain) được kiểm soát và phát triển bởi R3 và các tổ chức tham gia vào giao dịch.

Corda cũng có thể ứng dụng trong xây dựng các nền tảng KYC (Know your customer) nhận dạng, xác minh danh tính khách hàng, đồ vật. Hiện nay, Corda đang được tập trung nghiên cứu tại các doanh nghiệp cần đến nghiệp vụ chứng thực số như: bảo hiểm, ngân hàng, tổ chức tín dụng, sản xuất và thương mại, vv.. một nền tảng để tạo khả năng tương tác trong cài đặt doanh nghiệp. Khả năng mở rộng ấn tượng, quyền riêng tư của giao dịch, tính nhất quán của trạng thái và tính linh hoạt của quy trình làm việc phù hợp với nhiều loại hình doanh nghiệp bao gồm thị trường vốn, tài trợ thương mại, nhận dạng kỹ thuật số, bảo hiểm, chăm sóc sức khỏe, chính phủ, chuỗi cung ứng và viễn thông.

Corda được xây dựng nhằm mục đích ghi lại, quản lý và đồng bộ hóa các dữ kiện được chia sẻ bởi những bên tham gia. CorDapps, là những ứng dụng có thể được xây dựng trên Corda, mô hình hóa chặt chẽ các quy trình kinh doanh bắt đầu với sự tồn tại của các ràng buộc. Ở Corda, các hợp đồng thực hiện các thỏa thuận pháp lý. Corda

giúp thực hiện các hợp đồng bằng cách dễ dàng thực hiện các quy trình kinh doanh như thu thập các phê duyệt và chữ ký cần thiết sẽ tạo, thực hiện và giao dịch các thỏa thuận ràng buộc.

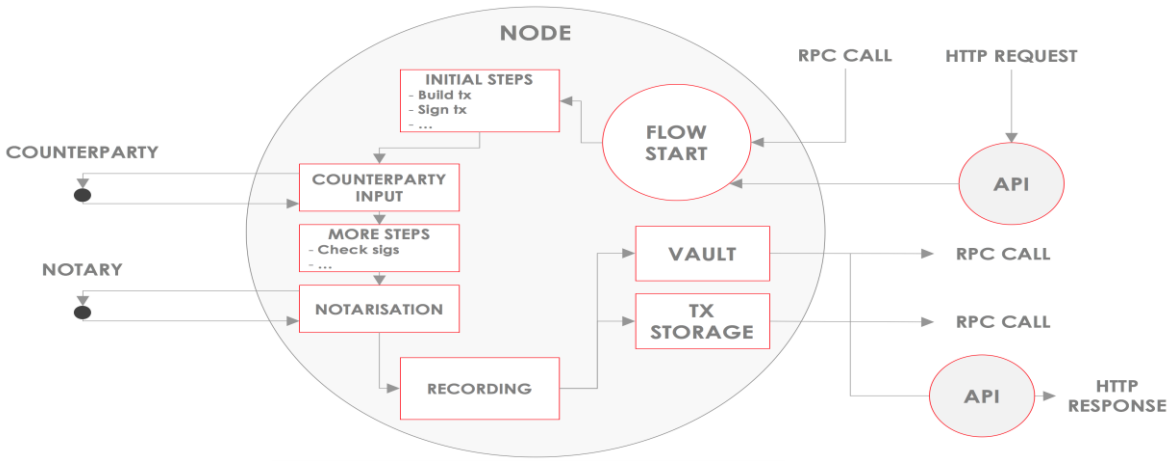
Corda hỗ trợ nhiều cơ sở dữ liệu quan hệ khác nhau, chỉ cần kết nối thông qua JDBC (Java Database Connectivity).

Ngoài việc hỗ trợ các cơ sở dữ liệu khác nhau, Corda linh hoạt trong việc sử dụng thuật toán đồng thuận. Corda không có hệ thống đồng thuận cố định, nó sử dụng Notary services nhằm kiểm chứng giao dịch, tránh trường hợp double spending. Mạng Corda có thể có một hoặc nhiều Notary services, mỗi Notary services sử dụng các thuật toán đồng thuận khác nhau.

Với Corda, mỗi tổ chức duy trì một sổ cái ghi lại các thỏa thuận và vị trí pháp lý của công ty với các đối tác. Rất nhiều hoạt động giữa các doanh nghiệp liên quan đến việc điều tiết lịch sử và sự kiện khác nhau. Sự không nhất quán là không thể tránh khỏi do sự trùng lặp của các quá trình phức tạp. Điều này dẫn đến việc giải quyết tranh chấp tốn kém hơn nữa, bản thân nó dễ xảy ra sai sót và tốn kém.

2.1.2. CorDapp

CorDapps (Corda Distributed Applications) là các ứng dụng phân tán chạy trên nền tảng Corda. Mục tiêu của CorDapp là cho phép các nút đạt được thỏa thuận về các bản cập nhật cho sổ cái. Chúng đạt được mục tiêu này bằng cách xác định các luồng mà chủ sở hữu nút Corda có thể gọi qua RPC:



Hình 2.1: Luồng xử lý trong CorDapp

CorDapps có dạng một tập hợp các tệp JAR chứa các định nghĩa lớp được viết bằng

Java hoặc Kotlin.

Các định nghĩa lớp này thường sẽ bao gồm các phần tử sau:

- Flow: Xác định một quy trình để nút chạy, thường là để cập nhật sổ cái
- States: Xác định các sự kiện mà thỏa thuận đạt được.
- Contracts: Xác định những gì cấu thành một bản cập nhật sổ cái hợp lệ
- Services: Cung cấp các tiện ích tồn tại lâu dài trong nút
- Serialisation whitelists: Danh sách hạn chế những loại nút của sẽ nhận được.

Mã nguồn của CorDapp được chia thành một hoặc nhiều mô-đun, mỗi mô-đun sẽ được biên dịch thành một JAR riêng biệt. Kết hợp cùng với nhau, các JAR này đại diện cho một CorDapp duy nhất. Thông thường, một CorDapp chứa tất cả các lớp cần thiết để nó được sử dụng độc lập. Tuy nhiên, một số CorDapp chỉ là thư viện cho các CorDapp khác và không thể chạy độc lập.

Mô hình chung cần phải có:

- Một mô-đun chỉ chứa các hợp đồng hoặc trạng thái của CorDapp, cũng như bất kỳ phụ thuộc bắt buộc nào.
- Mô-đun thứ hai chứa các lớp còn lại phụ thuộc vào các hợp đồng hoặc trạng thái này

2.1.3. Các thiết lập cài đặt môi trường cơ bản để phát triển CorDapp

- Cài đặt Java 8 JDK: Cài đặt Java 8 JDK. Corda yêu cầu ít nhất phiên bản 8u171, nhưng hiện không hỗ trợ Java 9 trở lên cho phiên bản Corda này.
- Cài đặt IntelliJ IDEA: IntelliJ là một IDE hỗ trợ mạnh mẽ cho việc phát triển Kotlin và Java.
- Cài đặt Git: Sử dụng Git để lưu trữ CorDapp mẫu và cung cấp quyền kiểm soát các phiên bản.
- Cài đặt Gradle.

2.1.4. So sánh Corda với các nền tảng khác

Corda được tạo ra từ quá trình làm việc sâu rộng với các công ty tài chính, ngân hàng và được thiết kế với các yêu cầu của họ. Tuy nhiên, thiết kế đó cũng được lấy cảm hứng từ các nền tảng trước đó.

Bảng 2.1: So sánh Corda với một số nền tảng khác

Tiêu chí	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**	**R3 Corda**
Ngôn ngữ lập trình	C++	Solidity(JavaScript, C++, Python)	Golang, Java	Kotlin, JVM platform
Quản trị	Không	Không	Linux	R3 consortium
Hợp đồng thông minh	Có	Không ràng buộc sổ cái	Không ràng buộc sổ cái	Ràng buộc sổ cái
Thuật toán đồng thuận	Phân tán, cổ phần	Cổ phần, công việc	Byzantine	Notary nodes
Khả năng mở rộng	Có	Có	Có	Có
Tiền tệ	BTC	Ether	Không có	Không có

2.2. Đặc trưng và triết lý của Corda

2.2.1. Tính cấp quyền

Tính riêng tư của mạng Corda: Corda là một mạng cấp quyền (giống như Hyperledger Fabric hay Quorum). Các node tham gia vào mạng cần được cấp phép và định danh đầy đủ.

Ở Corda, có một quy trình kết nạp mạng chính xác. Một tác nhân trên mạng Corda được đại diện bởi một nút. Các nút được biết đến với nhau và hệ thống được thiết kế để từ chối các nút trái phép.

Khi các node bên ngoài muốn tham gia vào mạng Corda, Node đó sẽ cần phải xác thực với DoorMan (tạm dịch là người giữ cửa). Node mới sẽ được tham gia vào mạng khi được DoorMan verified và accept.

2.2.2. Hợp đồng thông minh trong Corda R3.

Corda cũng có smart contract như các nền tảng khác như Ethereum, Hyperledger Fabric hay Quorum. Tuy nhiên, smart contract của Corda có chút khác biệt so với các nền tảng trên.

Tất cả nội dung, nghiệp vụ, logic trong smart contract của các nền tảng như Ethereum hoàn toàn do lập trình viên quy định. Do đó, nó khá free style, không thực sự giống so với các hợp đồng pháp lý truyền thống.

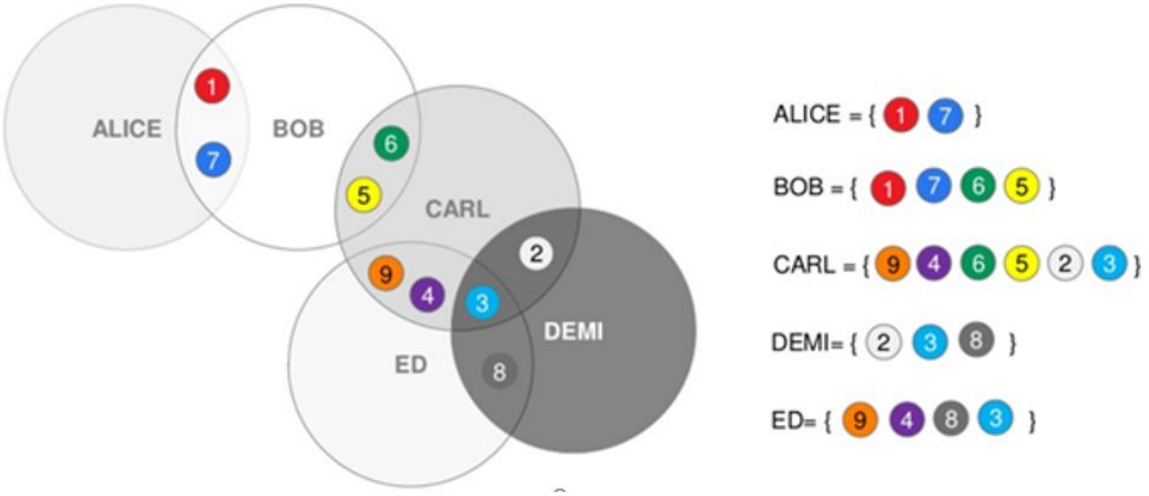
Corda khác biệt ở chỗ nó tập trung vào ngôn ngữ pháp lý, quy trình kinh doanh, cách giải quyết các thỏa thuận tranh chấp và mối quan tâm cụ thể của các doanh nghiệp. Trong các nền tảng blockchain nêu trên Code là luật (Code is Law) thì Corda hướng tới triết lý Luật là luật (Law is Law).

Lấy ví dụ nho nhỏ về giao dịch tiền mặt, smart contract trong corda sẽ được viết để kiểm tra xem giao dịch có đúng hay không? Chẳng hạn như tổng giá trị input bằng tổng giá trị output. Nó tương tự như vai trò của kế toán, kiểm toán vậy. Nếu không thỏa mãn các điều kiện, giao dịch sẽ bị smart contract reject.

2.2.4. Mạng ngang hàng

Mạng P2P của Corda không có việc boardcast thông tin hay giao dịch cho toàn mạng. Thông tin, giao dịch chỉ được trao đổi bởi các bên tham gia. Ví dụ nếu Alice giao dịch với Bob, thì chỉ Alice và Bob biết về nó, và có thể thêm bên cơ quan quản lý.

Không như Ethereum, Bitcoin hay phần nào là Hyperleder Fabric. Dữ liệu trên sổ cái của mạng Corda không đồng bộ ở tất cả các Node. Ví dụ được mô tả trong hình bên dưới, Alice chỉ giao dịch với Bob, nên dữ liệu, trạng thái về các giao dịch giữa Alice và Bob chỉ được lưu trữ ở sổ cái của 2 bên. Ngược lại, Alice cũng không biết được về các giao dịch giữa Bob với Carl, Card với ED, v..v



Hình 2.2: Mô tả lưu trữ giao dịch mạng ngang hàng trên Corda

Mạng Corda được thiết kế để mở rộng quy mô. Quá trình hoàn tất giao dịch được thiết kế để chạy nhanh nhất có thể khi mạng và phần cứng cơ bản cho phép. Quá trình hoàn thiện không bị ràng buộc về mặt logic bởi cơ chế tạo nhịp độ hoặc nhu cầu thu thập thỏa thuận rộng rãi như được tìm thấy trong các mạng blockchain đạt được sự đồng thuận. Nếu Alice và Bob đồng ý rằng giao dịch đã được hoàn tất và các quy trình khác nhau hoàn thành thì đó là giao dịch cuối cùng.

2.2.4. Hàng đợi thông điệp

Corda sử dụng AMQP (Advanced Message Queuing Protocol) thông qua TLS để truyền thông điệp trong mạng. AMQP chạy bất đồng bộ, chịu tải tốt, đảm bảo về việc gửi, lưu giữ thông điệp và hoạt động mà không cần kết nối liên tục. Khi node ngoại tuyến, thông điệp được xếp thành hàng đợi và gửi đi khi node online.

2.2.5. UTXO

Corda sử dụng mô hình UTXO cho các giao dịch giống như Bitcoin. Output của giao dịch này sẽ là Input cho giao dịch kế tiếp.

Ví dụ: Alice có 10$, Alice muốn chuyển cho Bob 1$. Đầu vào của giao dịch sẽ là Alice has got $10, đầu ra của giao dịch là Alice has got $9 và Bob has got $1. Khi giao dịch hoàn tất, input sẽ được đánh dấu là Historic (không thể sử dụng làm đầu vào cho các giao dịch tiếp theo).

Việc sắp xếp sai các giao dịch là điều không thể xảy ra vì mỗi giao dịch phụ thuộc vào sự tồn tại của các trạng thái đến trước đó và chỉ có thể được thực hiện một lần. Cơ cấu này giải quyết gọn gàng vấn đề chi tiêu gấp đôi trong khi đặt ra những yêu cầu tối thiểu cho quá trình đồng thuận.

2.3. Các khái niệm quan trọng trong Corda

2.3.1. Các trạng thái

Tổng hợp của tất cả các state được nắm giữ bởi tất cả các nút của mạng là "distributed ledger state". Không có sổ cái trung tâm và không phải tất cả các nút đều biết tất cả các trạng thái, vì vậy sổ cái tổng thể mang tính chủ quan từ quan điểm của từng người tham gia. Hầu hết các trạng thái được tìm thấy trong ít nhất hai nút khác nhau.

Trạng thái là dữ liệu được lưu trong sổ cái của một hay nhiều node trong 1 thời điểm nhất định, trạng thái tại thời điểm đó là không thể thay đổi (immutable).

Trạng thái không thế sửa đổi trực tiếp, thay vào đó trạng thái sẽ được lưu thành mỗi chuỗi (gọi là State sequences). Các trạng thái cũ sẽ được đánh dấu là Historic.

2.3.2. Các giao dịch

Giao dịch chỉ việc tiêu thụ các trạng thái và tạo ra các trạng thái mới. Các giao dịch chỉ có hoàn thành toàn bộ hoặc không có hiệu lực. Trong Corda một giao dịch tham chiếu trạng thái đầu vào hiện tại và trạng thái đầu ra trong tương lai. Giao dịch chưa được các bên chấp nhận được gọi là giao dịch đề xuất.

Giả sử Alice sẽ gửi tất cả $ 10 cho Bob. Một giao dịch có thể tham chiếu trạng thái đầu vào "Alice có 10 đô la" và trạng thái đầu ra "Bob có 10 đô la". Giao dịch tiêu tốn "Alice có $ 10" để trở thành trạng thái lịch sử. Nó là một phần của quá khứ và nó giải thích lịch sử của tài khoản Alice. Nó đã biến mất vì Alice đã gửi nó cho Bob. Lúc này tiền đã được đổi chủ.

2.3.9. Nodes

Corda node là môi trường chạy máy ảo Java (Java Virtual Machine run-time), mỗi node trong mạng đều có cho mình một định danh riêng.

Các thành phần chính trong kiến trúc của một Corda node:

Persistence layer làm nhiệm vụ lưu trữ dữ liệu gồm có 2 phần:

Vault, lưu trữ trạng thái của sổ cái (hiện tại và historic)

Storage service, nơi lữu trữ các giao dịch.

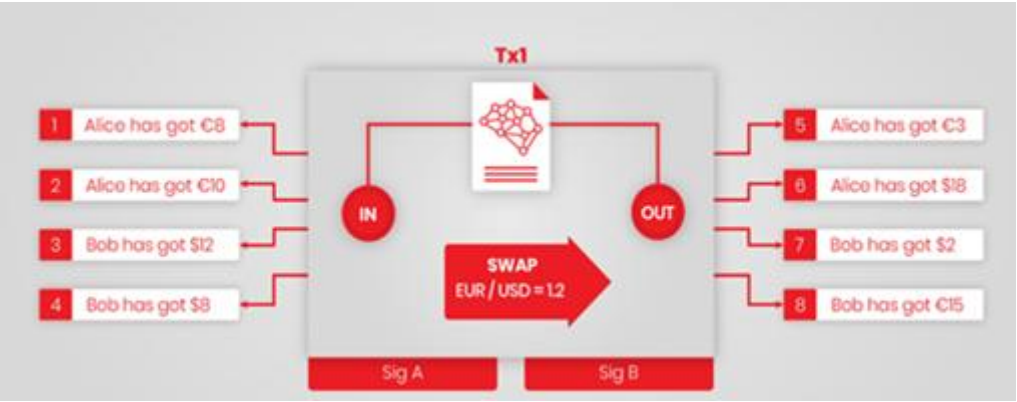
Network interface thực hiện việc tương tác với các nodes khác trong mạng.

RPC interface có chức năng tương tác với các thành phần khác trong node.

Service Hub là nơi trung gian để tương tác với các services trong mạng (oracles, notary)

2.3.3. Commands

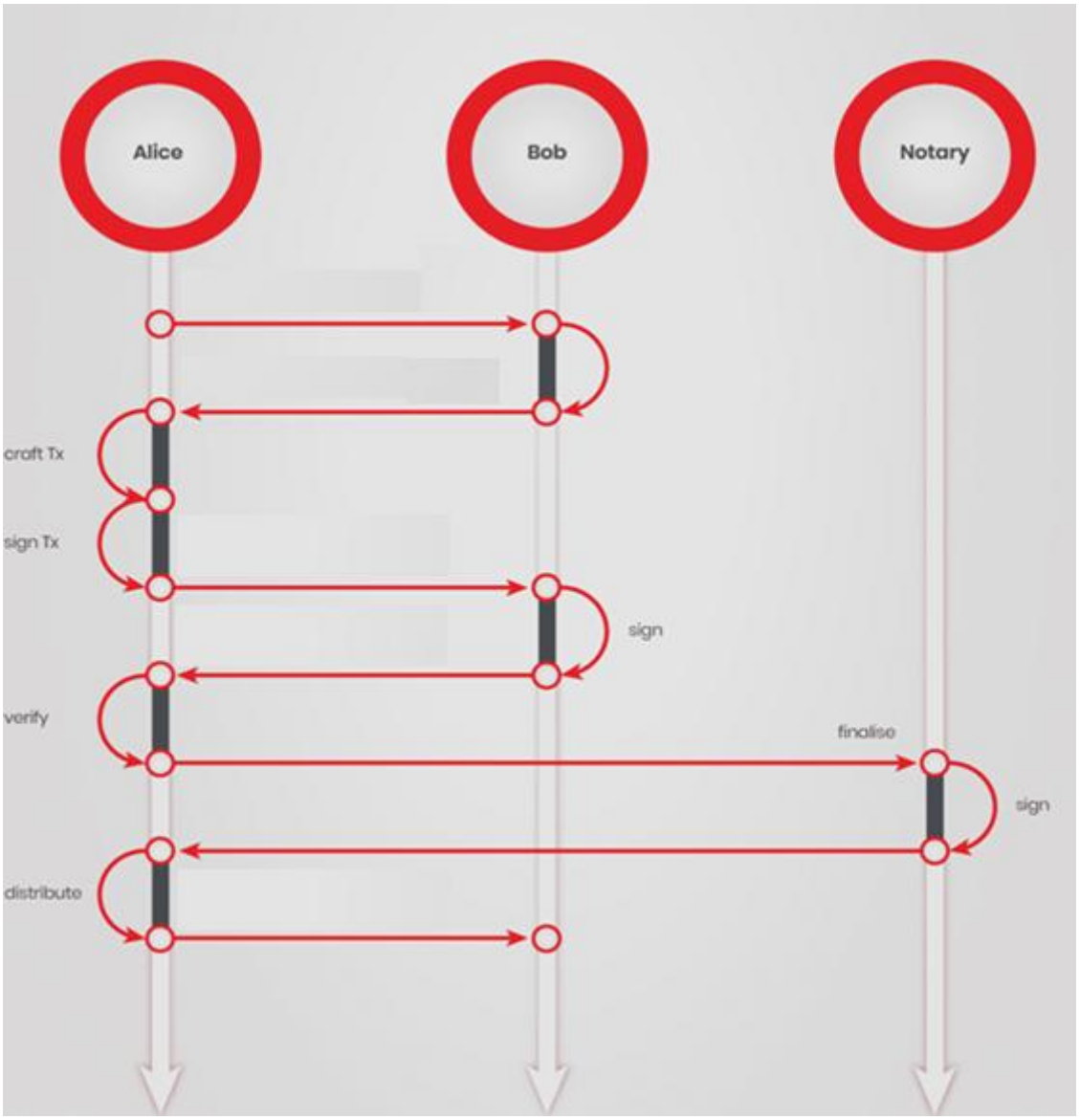
Có nhiều hình thức giao dịch khác nhau. Không chỉ là chuyển tiền mà có thể là đổi tiền, hủy tiền, vv... Commands là khái niệm gắn liền với 1 giao dịch trong Corda nhằm mô tả rõ mục đích của giao dịch đó.



Hình 2.7: Commands

2.3.4. Flows

Flows là một chuỗi các bước để một node biết cách cập nhật trạng thái của sổ cái, chẳng hạn như phát hành một tài sản hoặc thực thi một giao dịch. Chẳng hạn, Flow của node gửi giao dịch và node nhận giao dịch sẽ khác nhau. Corda cung cấp Flow Library để các node có thể implement tùy thuộc vào từng trường hợp.



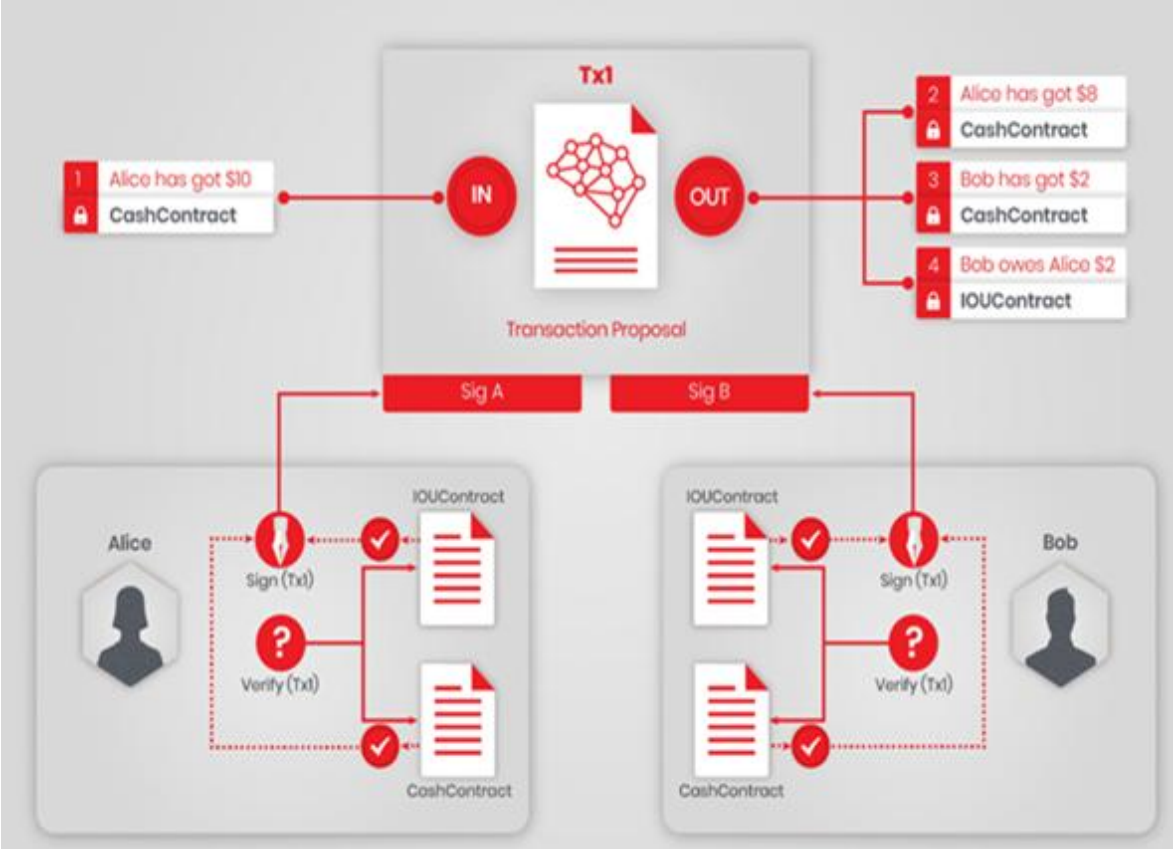
Hình 2.8: Ví dụ đơn giản về Corda Flow

2.3.5. Các cơ chế đồng thuận

Để được lưu vào sổ cái, giao dịch phải đạt được Validation Consensus lẫn Uniqueness Consensus.

Validation Consensus

Validation consensus là quá trình đồng thuận nhằm đảm bảo cho giao dịch đều được ký bởi tất cả các bên tham gia cũng như input, output của giao dịch thỏa mãn logic trong hợp đồng thông minh.



Hình 2.9: Luồng xác thực giao dịch

Uniqueness Consensus

Uniqueness consensus có mục đích nhằm ngăn chặn việc double-spends (lặp chi) được cung cấp bởi Notary Services.

Lấy ví dụ Bob có 1.000.000$ trong tài khoản. Bob tạo 2 giao dịch

Chuyển 1.000.000$ cho Charlie để đổi lấy 800.000£

Chuyển 1.000.000$ cho Dan để đổi lấy 900.000€

Vấn đề ở đây là 2 giao dịch của Bob hoàn toàn thỏa mãn Validation Consensus, chỉ với 1.000.000$ Bob có thể gian lận và thu về gấp đôi số tiền ban đầu.

Để ngăn chặn điều đó, mọi giao dịch được đề xuất cần thỏa mãn yêu cầu rằng không có bất kỳ input nào trong giao dịch đã được sử dụng ở một giao dịch khác.

2.3.6. Notary Services

Notary Services là một dịch vụ trong mạng Corda có chức năng chống double spends. Notary Services có thể bao gồm 1 hay nhiều node, mỗi node có thể chạy các thuật toán đồng thuận khác nhau.

Khi một peer gửi giao dịch đến Notary Services, có 2 trường hợp có thể xảy ra. Nếu trạng thái của input đã có trong Notary Map thì service sẽ throw exception. Nếu trạng thái input chưa được ghi nhận là đã sử dụng thì Notary Services sẽ ký và xác nhận giao dịch.

2.3.7. Time-windows

Đúng như tên gọi (cửa sổ thời gian), time-windows là khái niệm trong các giao dịch, áp dụng với các giao dịch cần được thực hiện trong một khoảng thời gian nhất định.

Time-windows có 3 khoảng là trước, trong và sau. Các bên tham gia có thể quy định khoảng thời gian mà giao dịch cần được thực hiện.

Notary Services sẽ kiểm tra thời gian và reject các giao dịch có thời gian đã bên ngoài time-windows được quy định.

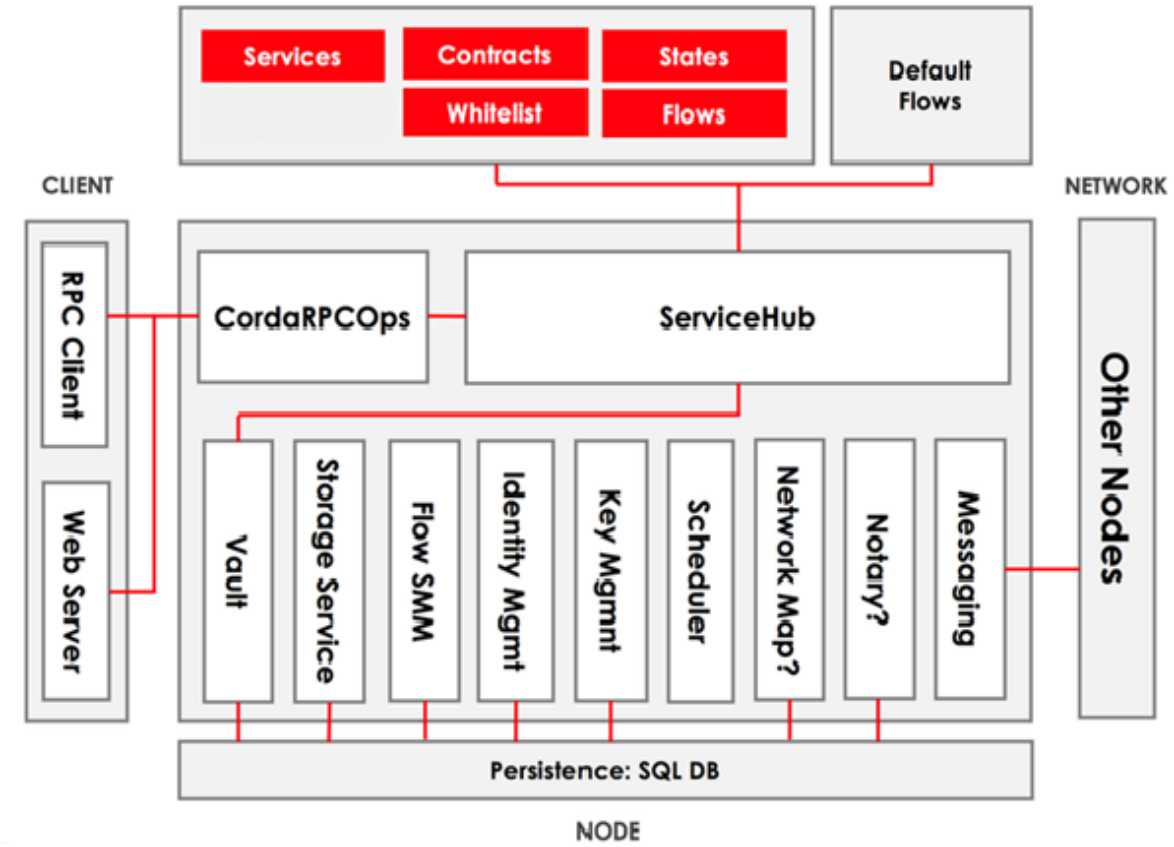
2.3.8. Oracles

Oracles trong Corda cũng có ý nghĩa tương tự như Oracles trong các nền tảng blockchain khác như Ethereum, Cosmos, vv… là dịch vụ cung cấp dữ liệu bên ngoài cho mạng (ví dụ như tỷ giá tiền tệ).

2.3.10. The service hub

Các chức năng cụ thể mà service hub cung cấp:

- Thông tin về các node khác trên mạng và các dịch vụ chúng cung cấp.
- Truy cập vào nội dung của vault và storage service.
- Truy cập và tạo ra các cặp public-private key của node.
- Thông tin về chính node chứa service hub.
- Thời gian.

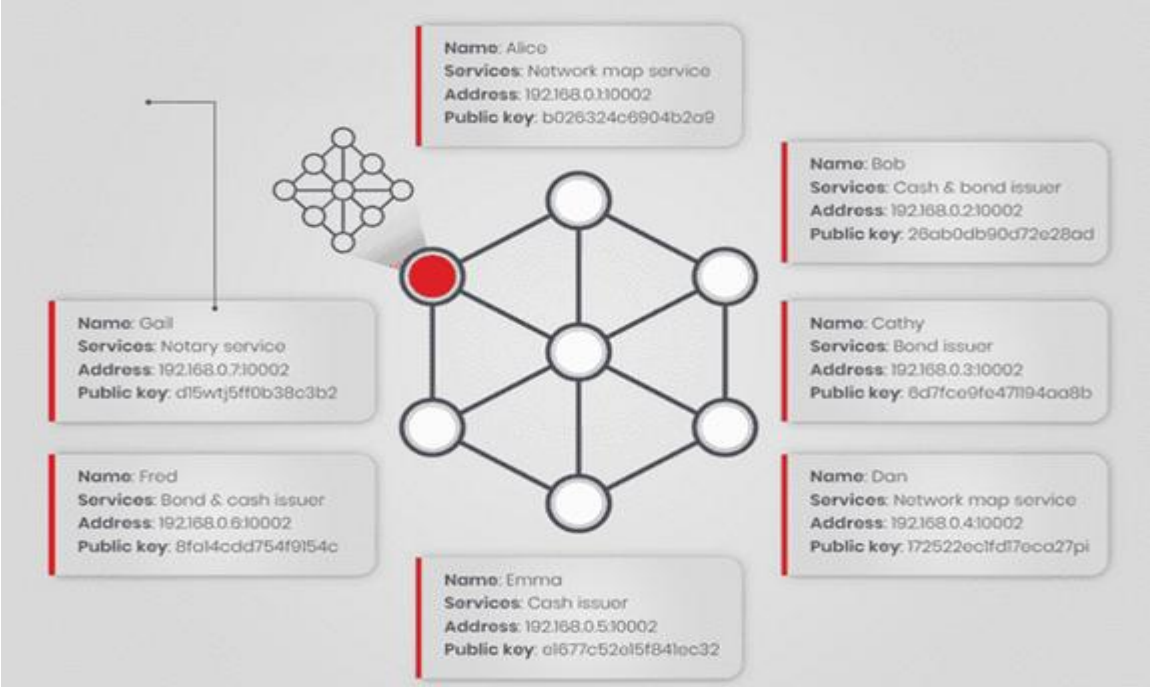


Hình 2.11: ServiceHub

2.3.12. Mạng Corda

Mạng Corda là một đồ thị được kết nối đầy đủ. Cũng như hai hoặc nhiều người tham gia ngang hàng có những vai trò đặc biệt quan trọng tạo nên một quá trình triển khai hoàn chỉnh.

- Một người gác cửa cung cấp việc cấp phép và ký chứng chỉ cho mạng được cấp phép
- Oracles
- Dịch vụ bản đồ một mạng
- Một hoặc nhiều Notary Services



Hình 2.12: Corda Network

Kết chương

Corda là một tập hợp các dữ kiện được chia sẻ không đồng đều giữa các thành phần trong mạng trên cơ sở định danh rõ ràng, một cơ sở dữ liệu phi tập trung được thiết kế để sử dụng trong môi trường doanh nghiệp. Nó cho phép một tập dữ liệu nhất quán được phân cấp giữa nhiều nút phân tán lẫn nhau, với các hợp đồng thông minh chạy trên JVM cung cấp định nghĩa điều khiển truy cập và lược đồ. Hệ thống quản lý danh tính đảm bảo rằng các bên luôn biết ai họ đang tương tác với. Các công chứng viên đảm bảo tính nhanh nhạy của thuật toán đối với các hệ thống đồng thuận phân tán và hệ thống hoạt động mà không cần khai thác hoặc chuỗi của các khối.

Kiến trúc và lựa chọn chiến lược của Corda hướng đến việc ghi lại và thực hiện các thỏa thuận tài chính bao gồm ba tầm nhìn chính: thứ nhất, các hồ sơ do hệ thống này quản lý sẽ chỉ có thể truy cập được đối với các tác nhân có lợi ích hợp pháp trong tài sản và thỏa thuận mà họ quản lý. Thứ hai, hành vi của các thỏa thuận do hệ thống quản lý sẽ được mô tả trong mã máy tính đề cập rõ ràng và đạt được tính hợp pháp của nó từ văn bản pháp lý bổ sung. Và cuối cùng, để đạt được sự chấp nhận rộng rãi trong cộng đồng tài chính, các phần của hệ thống phải và sẽ phải mở: mã nguồn mở, quy trình phát triển mở, các tiêu chuẩn công nghiệp và công nghệ mở.

CHƯƠNG 3: ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN TRONG GIAO DỊCH CHUYỂN TIỀN LIÊN NGÂN HÀNG

3.1. Đặt vấn đề

Theo nghiên cứu của Boston Consulting Group (BCG), gần 53 tỷ USD đã được dành cho các công ty fintech và hiện có khoảng 3.500 công ty Fintech trên thế giới. Những công ty này hỗ trợ rất nhiều ngành nghề, trong đó lĩnh vực tài chính - ngân hàng được hưởng lợi nhiều nhất.

Fintech trong lĩnh vực tài chính - ngân hàng kết nối người cho vay với người đi vay, thanh toán hóa đơn bằng một ứng dụng trên smartphone, quản lý danh mục đầu tư bằng robot tự động... Rõ ràng, Fintech đang thay đổi diện mạo ngành tài chính - ngân hàng.

Theo khảo sát của PwC đầu năm 2020, tỷ lệ khách hàng sẵn sàng hợp tác với các công ty fintech trong lĩnh vực thanh toán chiếm 84%, ngân hàng điện tử chiếm 68%, tài chính cá nhân là 60%, cho vay cá nhân chiếm 56%, tiếp theo đó là tiết kiệm, bảo hiểm và quản lý tài sản.

Một số nhà phân tích tài chính tin rằng, trong tương lai không xa, blockchain sẽ thay thế các hệ thống chuyển khoản ngân hàng hiện tại.

Các ngân hàng thường là đối tượng áp dụng công nghệ thông tin sớm nhất và họ đã làm rất tốt trong việc tự động hóa các quy trình thủ công trước đây và số hóa các quy trình vật lý trước đây.

Theo một cuộc khảo sát của Công ty Tư vấn Accenture, hơn một nửa các nhà quản lý hàng đầu hiện nay thừa nhận rằng blockchain đóng một vai trò quan trọng trong sự thành công của các ngân hàng cũng như công ty tài chính. Các ngân hàng trên toàn thế giới sẽ tiết kiệm được 20 tỷ USD vào năm 2022 nhờ áp dụng công nghệ blockchain.

Công nghệ Blockchain đang thực sự mở ra một tiềm năng rất lớn trong lĩnh vực tài chính – ngân hàng, nó có tác động to lớn đến quy trình xác nhận giao dịch, quản lý tiền mặt, tối ưu hóa tài sản cũng như các quy trình kinh doanh khác. Công nghệ blockchain sẽ giúp giảm thiểu thời gian từ lúc đăng ký tới lúc hoàn thành giao dịch

hoặc giảm thời gian cho các giao dịch liên ngân hàng, chuyển khoản quốc tế hoặc xác nhận thông tin cá nhân.

Trong bối cảnh này, công nghệ blockchain có thể cung cấp các lựa chọn khả thi và hiệu quả hơn cho ngành công nghiệp chuyển tiền.

3.1.1. Xác định bài toán

Dịch vụ chuyển tiền tại Việt Nam được định nghĩa tại Khoản 7 Điều 3 Thông tư 46/2014/TT-NHNN hướng dẫn về dịch vụ thanh toán không dùng tiền mặt do Thống đốc Ngân hàng Nhà nước Việt Nam ban hành như sau:

Dịch vụ chuyển tiền là việc tổ chức cung ứng dịch vụ thanh toán thực hiện theo yêu cầu của bên trả tiền nhằm chuyển một số tiền nhất định cho bên thụ hưởng. Bên thụ hưởng có thể là bên trả tiền. Dịch vụ chuyển tiền bao gồm dịch vụ chuyển tiền qua tài khoản thanh toán và không qua tài khoản thanh toán của khách hàng.

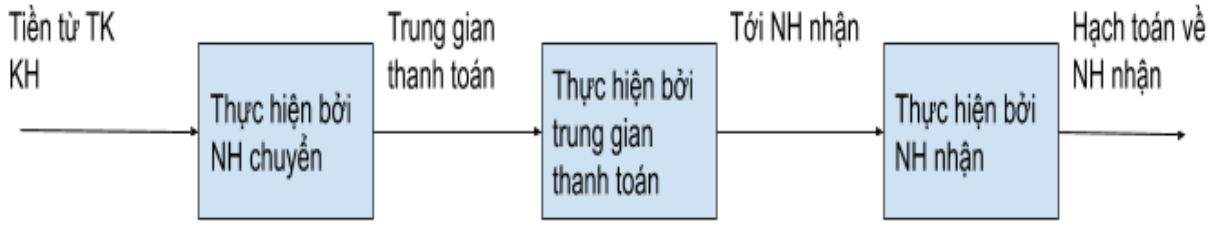
Các bên tham gia trong phương thức chuyển tiền

Người trả tiền – người mua, người mắc nợ – hoặc người chuyển tiền – người đầu tư, kiều bào chuyển tiền về nước, người chuyển kinh phí ra nước ngoài – là người yêu cầu ngân hàng chuyển tiền ra nước ngoài.

Người hưởng lợi – người bán, chủ nợ, người tiếp nhận vốn đầu tư – hoặc là người nào đó do người chuyển tiền chỉ định.

Ngân hàng chuyển tiền là ngân hàng ở nước người chuyển tiền.

Ngân hàng đại lý của ngân hàng chuyển tiền là ngân hàng ở nước người hưởng lợi.



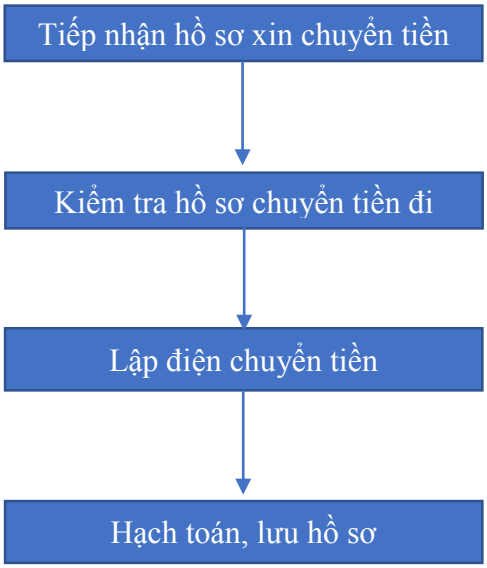
Hình 3.1: Tổng quan luồng chuyển tiền liên ngân hàng

Các nghiệp vụ ngân hàng chuyển tiền

Đối với ngân hàng có hai nghiệp vụ chuyển tiền đi và chuyển tiền đến.

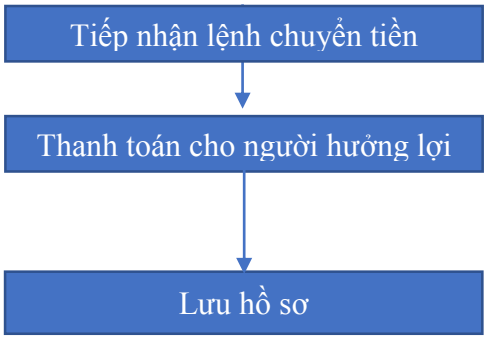
Khi chuyển tiền đi, nghiệp vụ ngân hàng diễn ra theo 4 b ước: (1) tiếp nhận hồ sơ

xin chuyển tiền; (2) Kiểm tra hồ sơ chuyển tiền đi; (3) Lập điện chuyển tiền và (4) Hạch toán – Lưu hồ sơ. (Hình 4.2.)



Hình 3.2: Nghiệp vụ chuyển tiền đi

Khi chuyển tiền đến, ngân hàng thực hiện thanh toán theo ba bước: (1) Tiếp nhận lệnh chuyển tiền; (2) Thanh toán cho người hưởng lợi và (3) Lưu hồ sơ. (Hình 4.3.)



Hình 3.3: Nghiệp vụ nhận tiền

Theo thông tin trên ngân hàng nhà nước, các hình thức chuyển tiền trực tuyến hiện tại: Nếu chia theo yếu tố trong hay ngoài ngân hàng, có 2 hình thức:

- Chuyển tiền tới một tài khoản cùng ngân hàng, còn gọi là chuyển khoản nội bộ. Với hình thứ này, tiền sẽ "nổi" trên tài khoản người nhận "real time", việc xử lý sẽ nhanh hơn do giao dịch được thực hiện trong hạ tầng nội bộ của ngân hàng, ít xảy ra lỗi, nếu có lỗi sẽ xử lý quyền lợi cho khách hang nhanh chóng hơn

- Chuyển tiền sang một ngân hàng khác, còn gọi là chuyển khoản liên ngân hàng. Với hình thức này, ngân hàng nguồn sẽ gọi sang các bên trung giang như NAPAS, Viettel, BIDV, VNPay, NHNN… là các đơn vị có kết nối đến nhiều ngân hàng hoặc xây dựng kết nối trực tiếp đến các ngân hàng thụ hưởng tại Việt Nam thông qua internet.

Nếu chia theo yếu tố thời gian, có 2 hình thức:

- Chuyển khoản liên ngân hàng nhanh, hay còn gọi là chuyển tiền 247. Khi chuyển tiền online sang ngân hàng khác qua internet banking, hầu hết các trường hợp có thể chọn hình thức chuyển tiền nhanh. Còn tại sao chuyển khoản nhanh lại gọi là chuyển khoản 247? Vì tiền sẽ tới tài khoản người nhận ngay lập tức, bất kể bạn thực hiện lệnh chuyển tiền lúc nửa đêm hay ngày nghỉ lễ.
- Chuyển khoản liên ngân hàng thường (Chuyển tiền CITAD): Khi chuyển tiền thường, người chuyển sẽ phải đợi một thời gian để tiền tới tài khoản người nhận. Nếu bạn thực hiện lệnh chuyển tiền trong giờ hành chính ngày làm việc, tiền sẽ tới trong vòng một vài giờ. Nếu lệnh được thực hiện ngoài giờ hành chính, hoặc vào ngày nghỉ, lễ, tiền sẽ tới tài khoản người nhận vào sáng ngày làm việc tiếp theo.

Bài toán đặt ra ở đây là các ngân hàng sẽ phải xây dựng 1 hạ tầng và 1 nguồn nhân lực khổng lồ để duy trì và vận hành hệ thống chuyển tiền này.

3.1.2. Cách tiếp cận và giải pháp.

Việc ứng dụng công nghệ Blockchain vào việc chuyển tiền liên ngân hàng trên thế giới đã được ứng dụng khá rộng rãi, có nhiều giải pháp, hệ thống Blockchain được đưa ra.

Mục tiêu chính của việc ứng dụng chuyển tiền qua Blockchain là để đơn giản hóa toàn bộ quy trình, gỡ bỏ các bên trung gian không cần thiết. Việc này sẽ giúp việc chuyển tiền thực hiện được dễ dàng và gần như ngay lập tức.

Khác với các dịch vụ mạng truyền thống, mạng Blockchain không cần dựa vào quá trình phê duyệt giao dịch chậm chạp do phải đi qua một hoặc nhiều bên trung gian và cần nhiều thao tác thủ công. Thay vào đó việc sử dụng hệ thống Blockchain có thể

thực hiện các giao dịch tài chính trên toàn thế giới dựa trên một mạng lưới phân tán gồm nhiều máy tính. Điều này có nghĩa là một số máy tính tham gia vào quá trình kiểm tra và xác thực các giao dịch và quá trình này có thể được thực hiện theo cách thức phi tập trung và bảo mật. So với hệ thống ngân hàng truyền thống, công nghệ blockchain có thể mang lại các giải pháp thanh toán nhanh chóng và đáng tin cậy hơn với chi phí thấp hơn nhiều.

Corda R3 là một framework Blockchain cung cấp giải pháp thích hợp cho vấn đề này.

3.2. Xây dựng hệ thống

3.2.1. Môi trường phát triển và công cụ

Hệ thống Blockchain được xây dựng và triển khai trên máy tính có cấu hình phần cứng như sau:

Bảng 3.1: Cấu hình phần cứng hệ thống

STT	**Nội dung**	**Thông số kỹ thuật**
1	CPU	Intel(R) Core (TM) i5-7400 CPU @ 3.00GHz (4 CPUs), ~3.0GHz
2	RAM	16384MB RAM
3	Hard Disk	240 GB SSD
4	OS	Windows 10 Pro 64-bit (10.0, Build 19041) (19041.vb_release.191206-1406)

Và thông tin các phần mềm:

Bảng 3.1: Các phần mềm hệ thống

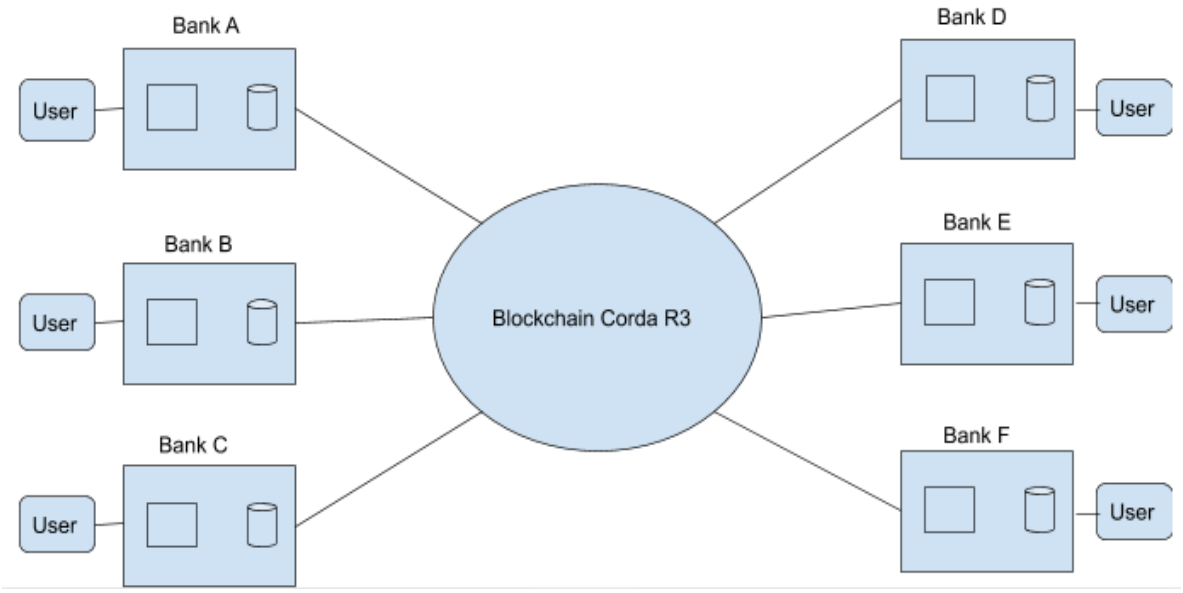
Phần mềm	Ghi chú
Oracle JDK	version 8u171 hoặc cao hơn
IDE	IntelliJ IDEA, visual code,
Git	source control
Gradle	
Docker	

H2 database	DBMS
PHP	
Bootstrap	
Spring Boot servers	

3.2.2. Kiến trúc hệ thống

Hệ thống chuyển tiền liên ngân hàng qua Blockchain Corda R3 trong nghiên cứu này được xây dựng cơ bản dựa trên 3 yếu tố chính:

- Mạng lưới Blockchain Corda R3
- Hệ thống các ngân hàng có các node trong Blockchain
- Người dùng thuộc các ngân hàng đó.



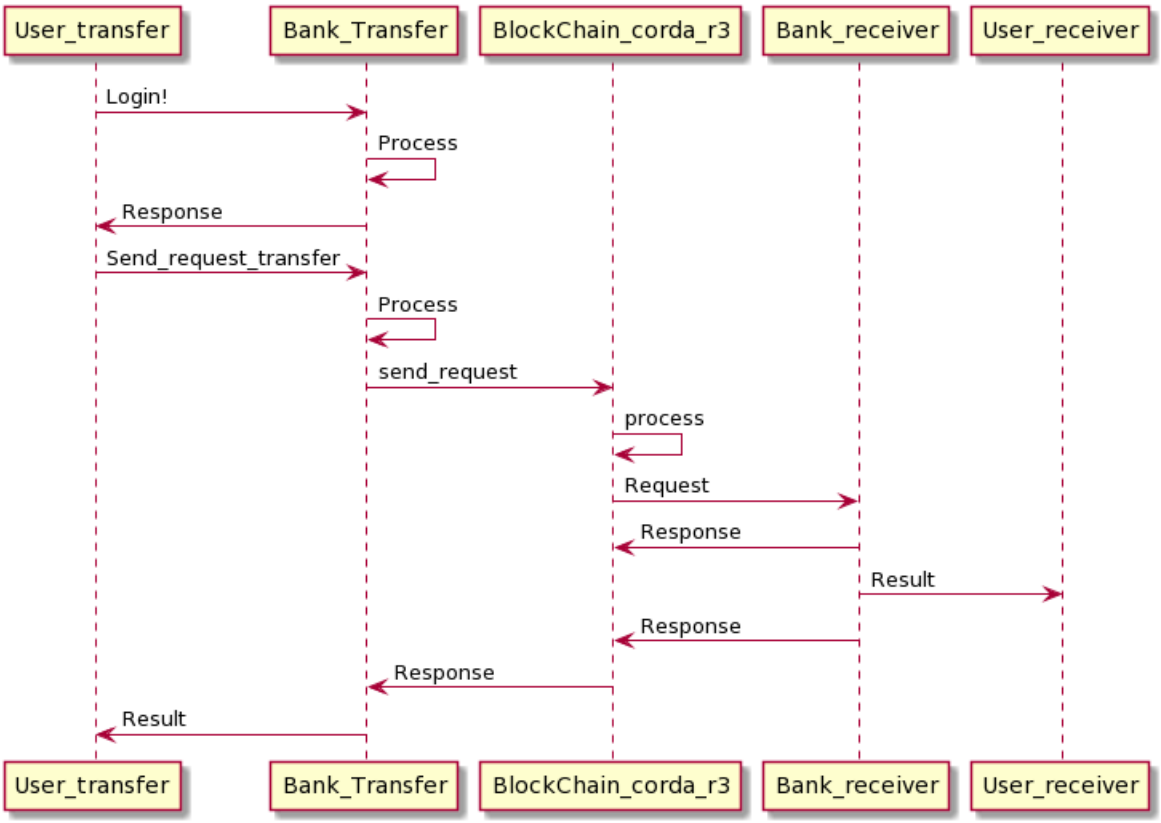
Hình 3.4: Mô hình chuyển tiền liên ngân hàng qua Blockchain Corda R3

Qua đó, mọi giao dịch thực hiện chuyển tiền từ User của Bank sau khi chuyển đi và trước khi chuyển đến đều được xử lý trên hệ thống Blockchain và trả ra kết quả cuối, kết quả này một lần nữa được ghi nhận lại trên Bank, người dùng có thể thực hiện truy vấn kết quả này thông qua việc xây dựng các Business được xây dựng phía từ phía các Bank.

3.2.3. Đặc tả chức năng

Hệ thống chuyển tiền qua Blockchain được xây dựng bởi các ngân hàng thành viên

và cụm server Blockchain tương tác kết quả qua nhau bằng API.



Hình 3.5: Luồng giao dịch chuyển tiền giữa 2 user khác Bank thông qua Blockchain Corda R3

Mô tả các bước:

Bước 1: User_transfer thực hiện login vào hệ thống Bank_transfer

Bước 2: Bank_transfer trả về kết quả login: Thành công hoặc thất bại.

Bước 3: Nếu kết quả login là thành công User_transfer thực hiện lệnh chuyển tiền sang Bank_transfer, Bank_transfer thực hiện xử lý các business như lưu DB, kiểm tra so sánh số dư… nếu kết quả xử lý ok, gửi request vào blockchain.

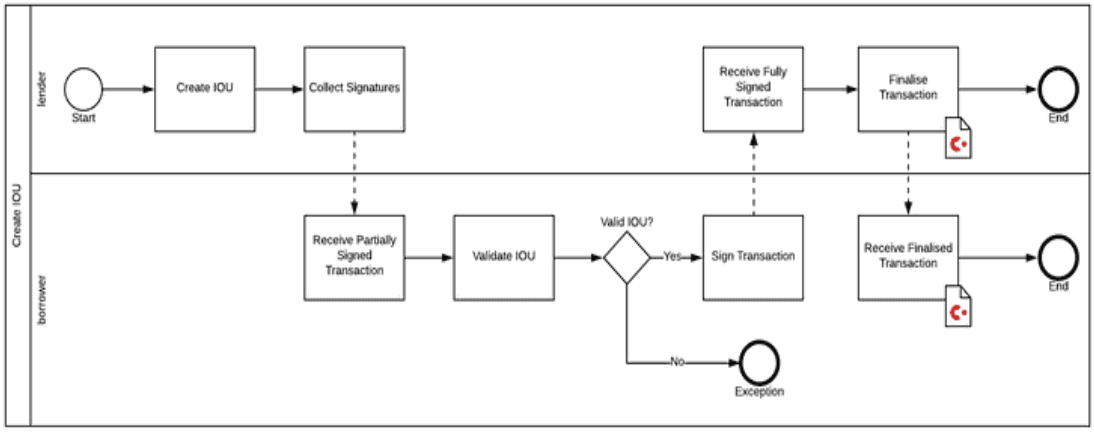
Bước 4: Hệ thống Blockchain xử lý giao dịch, gửi kết quả cho Bank_receiver, Bank_receiver xử lý cộng tài khoản cho User_receriver và trả kết quả cho Blockchain.

Bước 5: Blockchain trả kết quả cuối cho Bank_transfer.

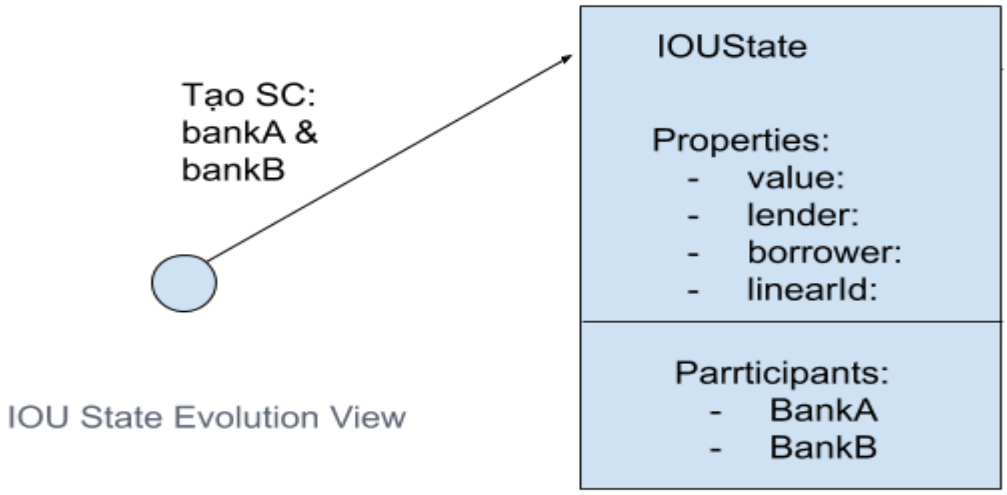
Luồng xử lý nội bộ trong Blockchain Corda R3:

Trong hệ thống Blockchain Corda R3 có thể có từ 2 đối tác trở lên, lender và borrower, để 1 giao dịch hoàn thành, cả 2 đối tác cần phải đồng thuận và đề xuất giao

dịch. Để đạt được sự đồng thuận này, quy trình phải trải qua một số bước và cả hai đều cần phải thực hiện ký. Họ muốn đạt được sự đồng thuận và đạt được sự phát triển trạng thái này:



Hình 3.5: Luồng xử lý nội bộ Blockchain Corda R3



Hình 3.8: Quá trình đồng thuận và đề xuất giao dịch của các bên

3.2.4. Cài đặt hệ thống

Phần cài đặt hệ thống Blockchain Corda:

Bước 1: Mở cửa sổ Terminal của Window tại thư mục chứa Project Corda

Bước 2: Chạy lệnh *gradlew.bat deployNodes* để deployNodes

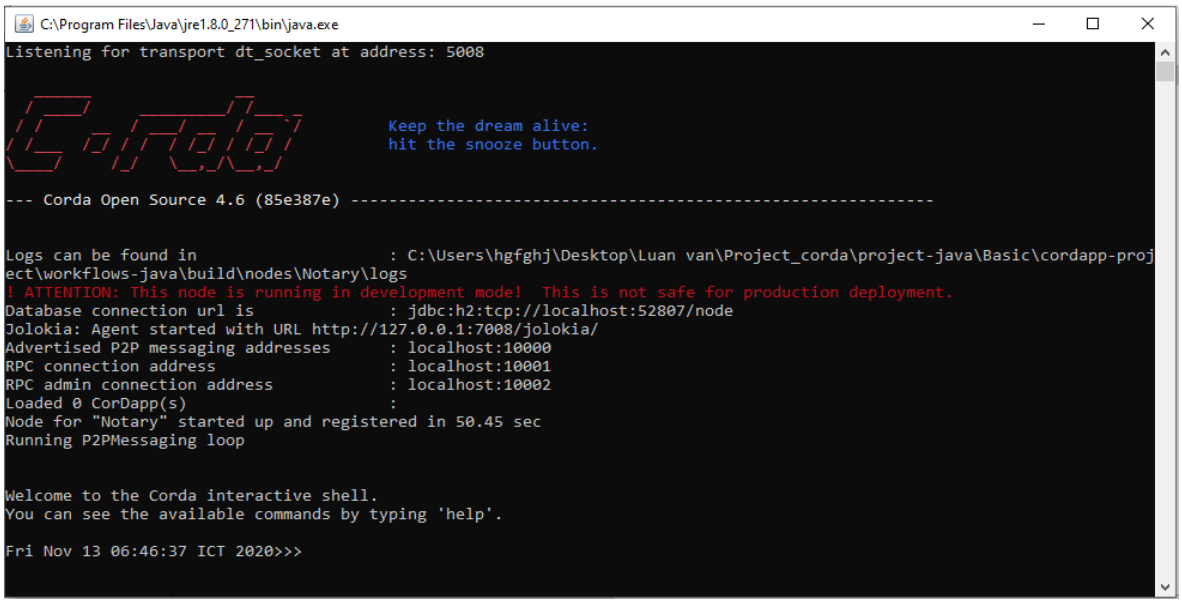
Bước 3: Sau khi build thành công thực hiện chạy CorDapp bằng câu lệnh:

call workflows-java\build\nodes\runnodes.bat

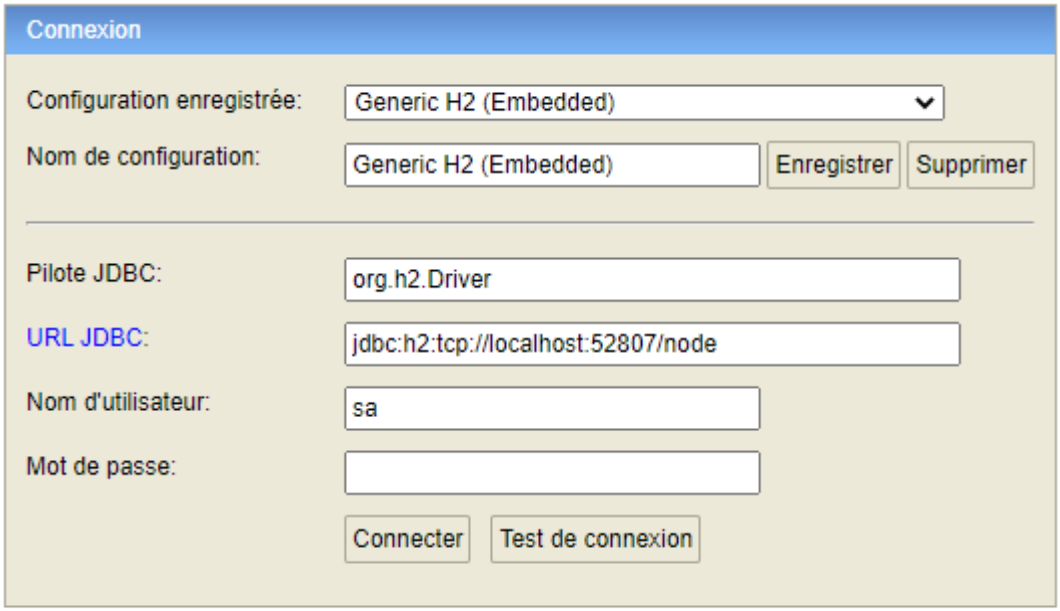
Bước 4: Thực hiện chạy Spring Boot server tại mỗi node bằng câu lệnh:

gradlew.bat runPartyXServer

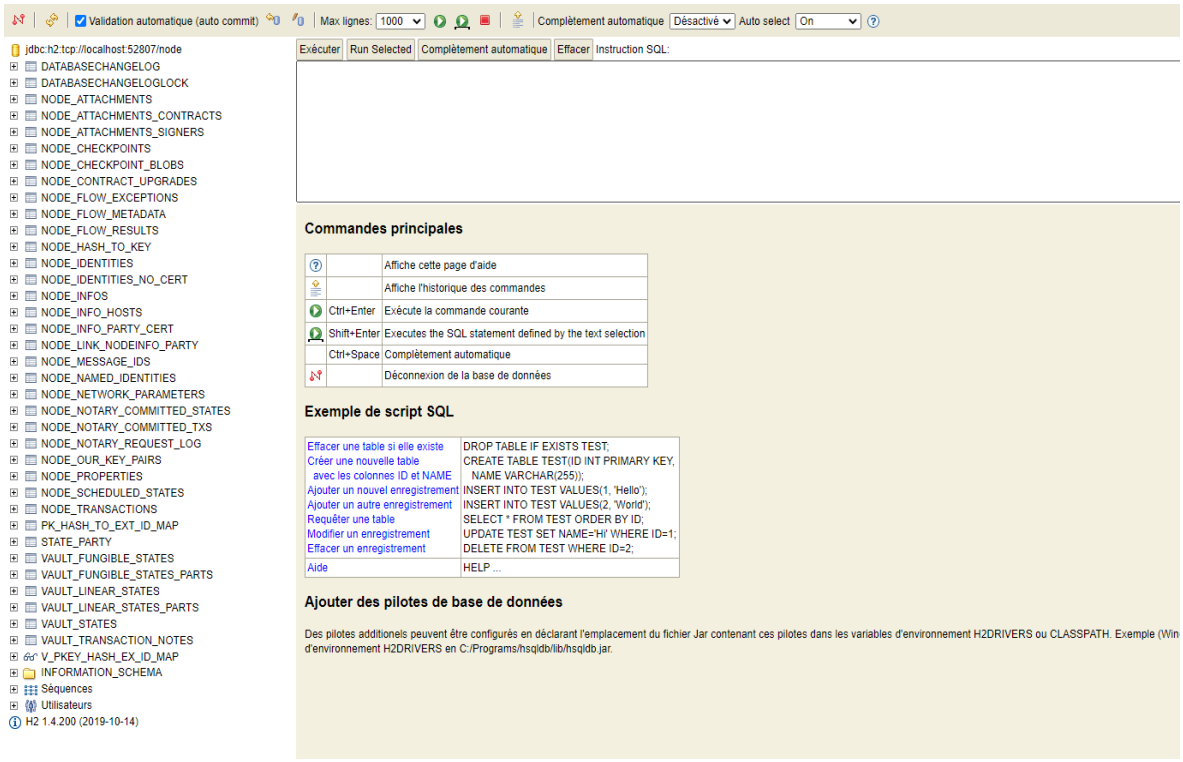
Với X là tên node.



Hình 3.9. Giao diện sau khi thực hiện khởi tạo thành công node



Hình 3.10: Màn hình đăng nhập vào hệ quản trị CSDL blockchain



Hình 3.11. CSDL trong lưu trữ trong Corda

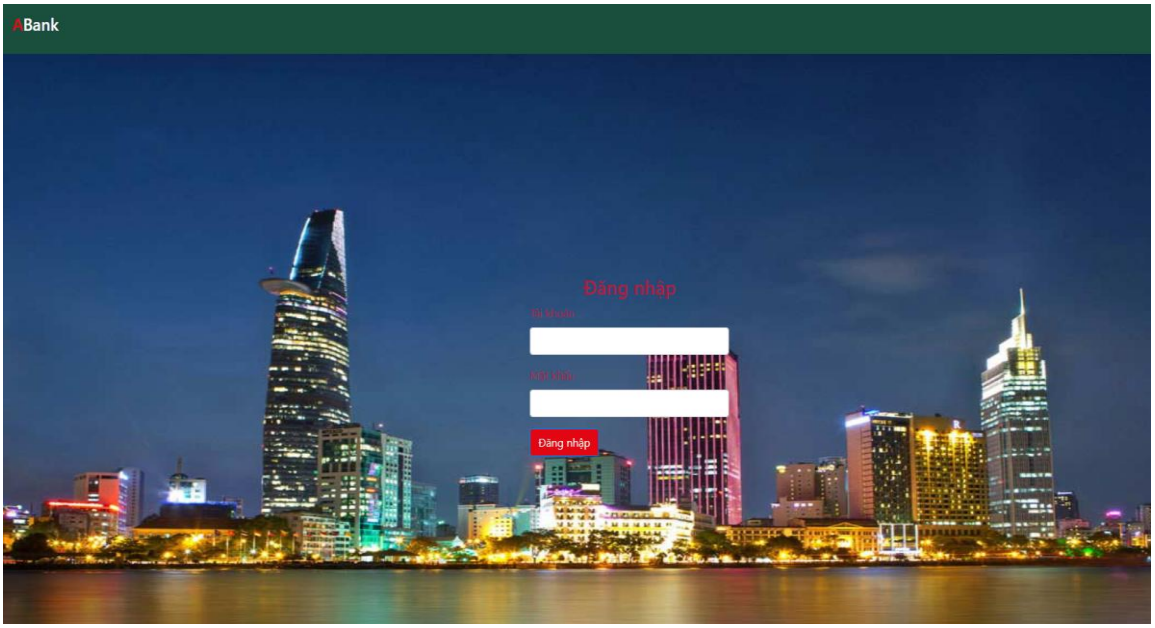
Phần hạ tầng các ngân hàng:

- Cài đặt docker Desktop trên windows tại địa chỉ: https://docs.docker.com/docker-for-windows/install/
- Sửa file host của window:

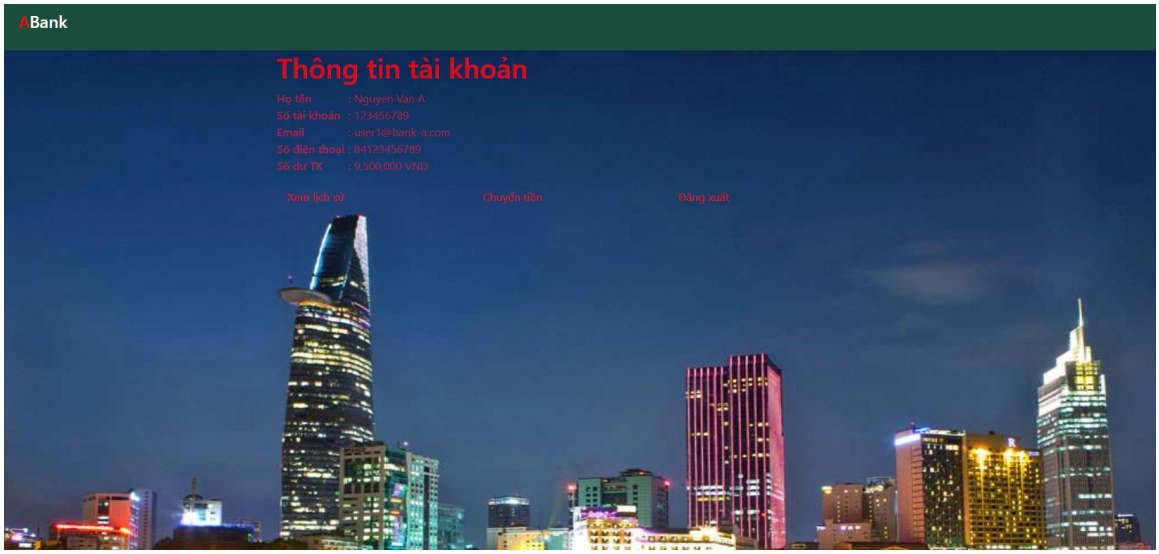
```
# Edit file host
`127.10.0.10   bank-a.local`
`127.10.0.11   bank-b.local`
```

- Khởi động server docker:

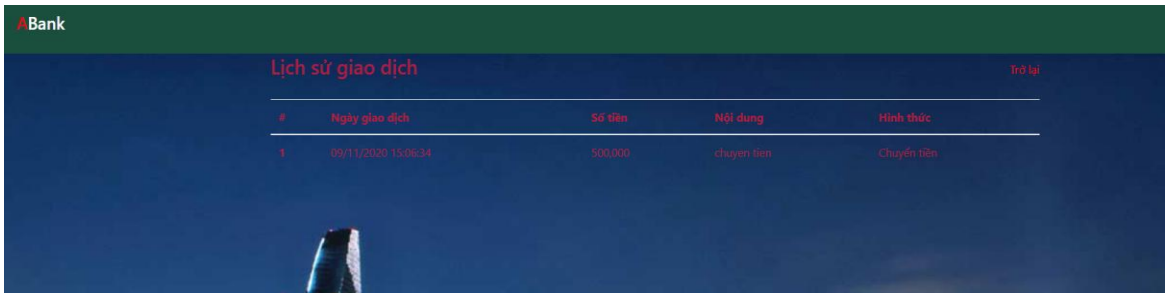
```
# Start Webservice
`docker-compose up`
```



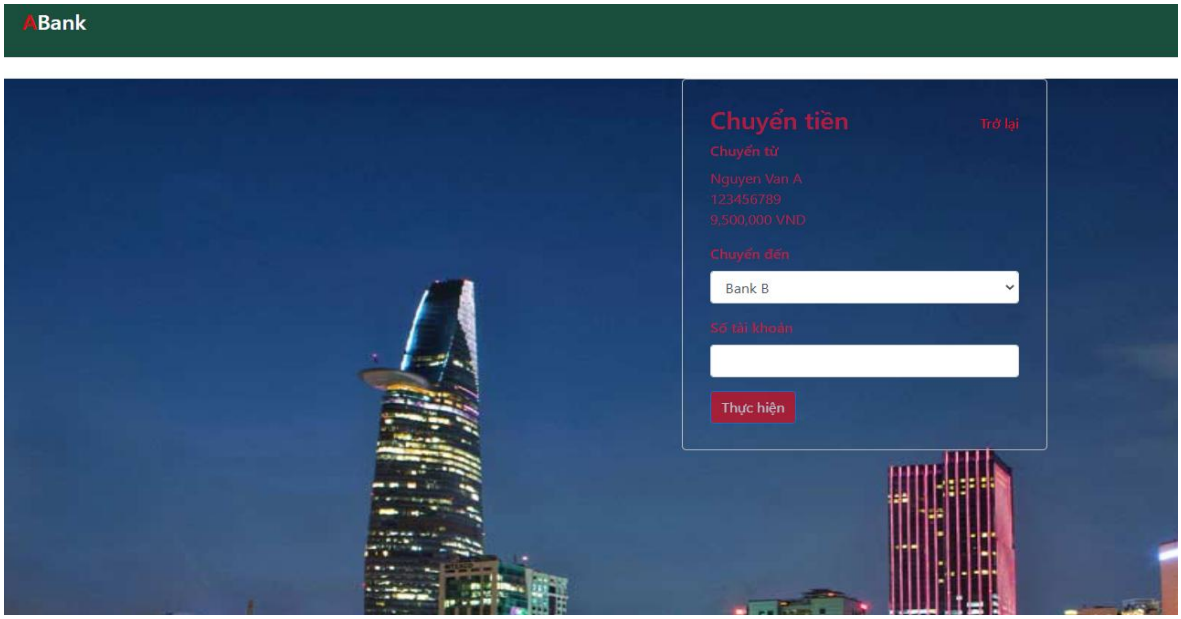
Hình 3.12. Màn hình đăng nhập bank A



Hình 3.13. Màn hình hiển thị thông tin sau khi đăng nhập thành công



Hình 3.14. Màn hình lịch sử giao dịch



Hình 3.15. Màn hình chuyển tiền

3.3. Thực nghiệm đánh giá

3.3.1. Kết quả thử nghiệm

Hệ thống ngân hàng giả lập đã được triển khai và cài đặt trên domain:

http://bank-a.local/login.php

http://bank-b.local/login.php

http://bank-c.local/login.php

Hệ thống blockchain Corda đã được triển khai và cài đặt trên webservice, bao gồm 1 notary, 3 node là thể hiện của 3 ngân hàng trong mạng.

http://localhost:50005/

http://localhost:50006/

http://localhost:50007/

Mỗi Spring Boot servers của Corda R3 blockchain sẽ bao gồm các API:

/api/example/me: Trả ra thông tin của node đang gọi vào

VD:

```
{
   me: "O=BankB, L=HaNoi, C=VN"
}
```

/api/example/peers: Trả ra thông tin các node ngang hàng khác trong mạng

VD:


```
{
   peers:
   [
      "O=BankC, L=HaNoi, C=VN",
      "O=BankA, L=HaNoi, C=VN"
   ]
}
```


/api/example/ious: Trả ra thông tin các giao dịch mà các node đã thực hiện

VD:


```
[
• {
   ○ state:
      {
       ▪ data:
          {
           ▪ @class: "com.example.state.IOUState",
           ▪ value: 100,
           ▪ lender: "O=BankA, L=HaNoi, C=VN",
           ▪ borrower: "O=BankB, L=HaNoi, C=VN",
           ▪ linearId:
              {
               ▪ externalId: null,
               ▪ id: "84eda410-892a-4d72-8af2-
                 fc69ef81e3be"
              }
```

```
        },
        ▪ contract: "com.example.contract.IOUContract",
        ▪ notary: "O=Notary, L=HaNoi, C=VN",
        ▪ encumbrance: null,
        ▪ constraint:
          {
            ▪ @class: "net.corda.core.contracts.SignatureAttachmentConstraint",
            ▪ key: "aSq9DsNNvGhYxYyqA9wd2eduEAZ5AXWgJTbTEw3G5d2maAq8vtLE4kZHgCs5jcB1N31cx1hpsLeqG2ngSysVHqcXhbNts6SkRWDaV7xNcr6MtcbufGUchxredBb6"
          }
      },
    ○ ref:
      {
        ▪ txhash: "A6D14D700BD6B97FF0992376B66365D4A2CC586E070D3F75FFD64B84CAF0B89E",
        ▪ index: 0
      }
• }
]
```


/api/example/create-iou: API tạo giao dịch chuyển tiền

Sau khi thực hiện cài đặt và triển khai thành công toàn bộ hệ thống từ Client, Webservice Bank và hệ thống Blockchain, việc thực hiện chuyển tiền từ hệ thống ngân hàng A sang hệ thống ngân hàng B theo số tài khoản được thực hiện thành công, lịch sử giao dịch được xử lý và lưu trữ đầy đủ trên hệ thống ngân hàng chuyển, ngân hàng nhận và Blockchain Corda

3.3.2. Đánh giá kết quả

Với mục tiêu bài toán đã đưa ra, hệ thống đã hoạt động theo giao thức P2P đã giải quyết được vấn đề chuyển tiền liên ngân hàng, thay vì với quy trình cũ, tính xác thực và xử lý khi có sự cố không cao, quy trình đối soát chậm chạp.

Giúp cho người dùng thực hiện chuyển tiền liên ngân hàng nhanh chóng hơn.

3.4. Kết chương

Chương này đã mô tả một cách trực quan toàn bộ hệ thống ngân hàng sử dụng công nghệ Blockchain trong lĩnh vực chuyển tiền liên ngân hàng, cụ thể là sử dụng nền tảng Corda R3 trong việc xử lý và xác thực thông tin chuyển khoản. Với những tính chất công khai, minh bạch và không dễ mạo danh, sửa đổi, Blockchain là 1 khối vững chắc. Nghiệp vụ chuyển tiền liên ngân hàng sẽ đi theo con đường tích hợp công nghệ này trong một tương lai không xa.

KẾT LUẬN CHUNG

Các kết quả thu được trong luận văn

Qua quá trình nghiên cứu về blockchain và một số ứng dụng của công nghệ này, cùng với sự giúp đỡ tận tình của thầy cô và bạn bè, luận văn đã đạt được một số kết quả nhất định, đưa ra cái nhìn rõ ràng hơn về khái niệm blockchain, cài đặt được hệ thống blockchain và phát triển được một ứng dụng của nó trong mảng chuyển tiền liên ngân hàng.

Về mặt nội dung, luận văn đã đạt được một số kết quả sau đây:

1. Tìm hiểu và nghiên cứu lý thuyết:

• Chi tiết về công nghệ blockchain và tiềm năng của công nghệ này.

• Hàm băm và chữ ký số, các kỹ thuật sử dụng trong blockchain.

• Tiền số, một trong những ứng dụng của blockchain.

• Các mô hình chuyển tiền liên ngân hàng ở thời điểm hiện tại.

2. Thực nghiệm:

• Xây dựng mô phỏng thành công một hệ thống chuyển tiền liên ngân hàng đơn giản áp dụng framework Corda R3.

Định hướng nghiên cứu tiếp theo

Do thời gian chưa có nhiều, bên cạnh các kết quả đạt được, luận văn cũng còn nhiều hạn chế trong việc triển khai chương trình thực nghiệm. Để mạng blockchain thực sự hoạt động tốt cần có sự tham gia của nhiều nút và chương trình mô phỏng có số nút còn hạn chế. Ngoài ra, hệ thống cần thử nghiệm các loại chữ ký số khác để so sánh về tốc độ thực hiện cũng như cải thiện hiệu năng của hệ thống.

Với các hạn chế kể trên, luận văn sẽ tiếp tục nghiên cứu các vấn đề sau:

• Tiếp tục hoàn thiện mạng blockchain với nhiều nút cùng hoạt động

• Thử nghiệm các phương pháp ký số khác và so sánh về tốc độ xử lý, độ an toàn của thuật toán để cải thiện hiệu năng và tính bảo mật của blockchain.

• Bổ sung thêm các nghiệp vụ cần thiết của nghệ thống ngân hàng vào hệ thống Blockchain

DANH MỤC TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] Trịnh Nhật Tiến (2008), *Giáo trình An toàn dữ liệu*, Hà Nội.

[2] Đặng Minh Tuấn (2016), *Hệ mật mã công khai dựa trên đường cong Elipptic*, Hà Nội.

Tiếng Anh

[3] Andreas M.Antolopoulos (2015), *Masetering Bitcoin*, O'Reilly.

[4] *Blockchain*. https://blockchain.info/.

[5] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., and Felten, E.W (2015), *Sok: Research perspectives and challenges for Bitcoin and cryptocurrencies*, In 2015 IEEE Symposium on Security and Privacy, pages 104–121.

[6] Crosby, M., Nachiappan, Pattanayak, P., Verma, S., and Kalyanaraman, V., *Blockchain technology beyond Bitcoin*, Technical report, Berkeley, CA, USA.

[7] Hakobyan, D. (2012), *Authentication and authorization systems in cloud environments. Master's thesis*, Stockholm, Sweden.

[8] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press.

[9] Rodrigues, E. (2016), *The blockchain architecture in a nutshell*, Technical report, Linkedin, September 2016, https://www.linkedin.com/pulse/blockchain-architecture-nutshell-eder-rodrigues.

[10] Tucker, C. and Catalini, C., *Blockchain research at mit*, http://blockchain.mit.edu/.

[11] Xu, J. J. (2016), *Are blockchains immune to all malicious attacks?*, Financial Innovation, 2(1):25, ISSN 2199-4730.

[12] Wood, G., "*Ethereum: A Secure Decentralised Generalised Transaction Ledger*.", https://bravenewcoin.com/assets/Whitepapers/Ethereum-A-Secure-DecentralisedGeneralised-Transaction-Ledger-Yellow-Paper.pdf.

PHỤ LỤC

1. Phần source code mô tả luồng xử lý trong Blockchain Corda R3

Luồng giao dịch sẽ được khởi tạo khi có request từ phía Bank gửi qua:

Initiator extends FlowLogic<>

```
1.  public static class Initiator extends FlowLogic<SignedTransaction> {
2.
3.      private final int iouValue;
4.      private final Party otherParty;
5.
6.      private final Step GENERATING_TRANSACTION = new Step("Gen
    erating transaction based on new IOU.");
7.      private final Step VERIFYING_TRANSACTION = new Step("Verifyi
    ng contract constraints.");
8.      private final Step SIGNING_TRANSACTION = new Step("Signing tr
    ansaction with our private key.");
9.      private final Step GATHERING_SIGS = new Step("Gathering the cou
    nterparty's signature.") {
```

Acceptor extends FlowLogic <>

```
1.  public static class Acceptor extends FlowLogic<SignedTransaction> {
2.
3.      private final FlowSession otherPartySession;
4.
5.      public Acceptor(FlowSession otherPartySession) {
6.          this.otherPartySession = otherPartySession;
7.      }
8.
9.      @Suspendable
10.     @Override
```

```
11.       public SignedTransaction call() throws FlowException {
12.           class SignTxFlow extends SignTransactionFlow {
13.               private SignTxFlow(FlowSession otherPartyFlow, ProgressTracke
    r progressTracker) {
14.                   super(otherPartyFlow, progressTracker);
15.               }
16.
17.               @Override
18.               protected void checkTransaction(SignedTransaction stx) {
19.                   requireThat(require -> {
20.                       ContractState output = stx.getTx().getOutputs().get(0).getData
    ();
21.                       require.using("This must be an IOU transaction.", output inst
    anceof IOUState);
22.                       IOUState iou = (IOUState) output;
23.                       require.using("I won't accept IOUs with a value over 100.", io
    u.getValue() <= 100);
24.                       return null;
25.                   });
26.               }
27.           }
28.           final SignTxFlow signTxFlow = new SignTxFlow(otherPartySession
    , SignTransactionFlow.Companion.tracker());
29.           final SecureHash txId = subFlow(signTxFlow).getId();
30.
31.           return subFlow(new ReceiveFinalityFlow(otherPartySession, txId));


32.       }
33.   }
```

```
34. }
```

Lưu ý rằng *me = getOurIdentity ()* được đặt ở vị trí ngân hàng chuyển. Vì vậy, flow này phải được bắt đầu bởi người chuyển.

```
1. val iouState = IOUState(
2.     value = iouValue,
3.     lender = serviceHub.myInfo.legalIdentities.first(),
4.     borrower = otherParty)
```

Tạo Command với những người ký được yêu cầu sign:

```
1. final Command<IOUContract.Commands.Create> txCommand = new Com
   mand<>(
2.                 new IOUContract.Commands.Create(),
3.                 ImmutableList.of(iouState.getLender().getOwningKey(), iouStat
   e.getBorrower().getOwningKey()));
```

Liên kết *IOUState* với *IOUContract.* Đây là nơi mà state thực sự chỉ vào hợp đồng sẽ xác minh giao dịch thay mặt cho nó.

```
1. final TransactionBuilder txBuilder = new TransactionBuilder(notary)
2.                 .addOutputState(iouState, IOUContract.ID)
3.                 .addCommand(txCommand);
```

Xác minh cục bô rằng giao dịch là hợp lệ.

```
1. final TransactionBuilder txBuilder = new TransactionBuilder(notary)
2.                 .addOutputState(iouState, IOUContract.ID)
3.                 .addCommand(txCommand);
4. txBuilder.verify(getServiceHub());
```

Ký tên vào nó với chữ ký của bank chuyển

```
1. .
   final SignedTransaction partSignedTx = getServiceHub().signInitialTransact
   ion(txBuilder);
```

Mở phiên ngang hàng với bank nhận

```
1. FlowSession otherPartySession = initiateFlow(otherParty);
```

Yêu cầu chữ ký từ bank nhận.

```
1. final SignedTransaction fullySignedTx = subFlow(
2.                     new CollectSignaturesFlow(partSignedTx, ImmutableSet.of(oth
   erPartySession), CollectSignaturesFlow.Companion.tracker()));
```

Khi nhận được giao dịch đã ký đầy đủ và tiếp tục.

Kết thúc bằng cách gửi giao dịch cho bank nhận và chờ phản hồi.

```
return subFlow(new FinalityFlow(fullySignedTx, ImmutableSet.of(otherPartySess
ion)));
```