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

TÓM TẮT LUẬN VĂN THẠC SỸ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: **TS. ĐẶNG MINH TUẤN**

Phản biện 1:

……..

Phản biện 2:

……

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng .... năm .....

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

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

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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. Public

Cách rõ ràng nhất để vận hành các giao thức blockchain là ở dạng Public. 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.

1.3.2. Private

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).

1.3.3. Permissioned

Permissioned blockchain 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.

1.4. Các cơ chế đồng thuận

"Thống nhất ra quyết định 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."

1.4.1. Proof-of-work.

1.4.2. Proof-of-Stake.

1.4.3. Ủy nhiệm Proof-of-Stake.

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

1.4.4. Proof-of-Authority.

1.5. Cách hoạt động của Blockchain

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

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 đợn 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.
- Tăng tốc độ giao dịch: Do có khả năng loại bỏ đơn vị trung gian và thiết lập trên sổ cái phân tán cho phép tăng tốc độ giao dịch cao hơn so với nhiều hệ thống hiện nay.
- 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**

Các blockchain, đặc biệt là những loại đang sử dụng Proof of Work, là rất kém 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 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.

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.

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

Characteristics	Bitcoin	Ethereum	Hyperledger Fabric	R3 Corda
Programming Language	C++	Solidity (JavaScript, C++, Python)	Golang, Java	Kotlin ,JVM platform
Administration	No administration	No administration	Linux foundation	R3 consortium
Smart Contracts	Smart Contracts can be made	No legal bounding	No Legal Bounding	Legally Bounded
Consensus Algorithm	Decentralized, Transparent	Proof-of-Work, Proof-of-Stake	Practical Byzantine Fault Tolerance	Based on Notary nodes
Scalability	Scalability issue exist	Scalability issue exist	Increased with transactions	Highly scalable
Privacy	Privacy protected	Issue with privacy protection	Identity management services	Identity management services
Currency	BTC	Ether	No Native Currency	No Native Currency

2.2. Đặc trưng và triết lý của Corda

2.2.1. Permissioned

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.

2.2.2. Smart Contract 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.

2.2.4. Peer-to-Peer

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.

2.2.4. Message Queues

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.

2.3. Các khái niệm quan trọng trong Corda

2.3.1. States

2.3.2. Transactions

Transaction chỉ việc tiêu thụ các state và tạo ra các state mới. Các transaction chỉ có hoàn thành toàn bộ hoặc không có hiệu lực.

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.

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.

2.3.5. Consensus

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.

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.

2.3.12. Corda Network

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.

Kết chương

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

3.1. Đặt vấn đề

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

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.

Corda R3 là một giải pháp Blockchain 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 3.2: Các phần mềm hệ thống

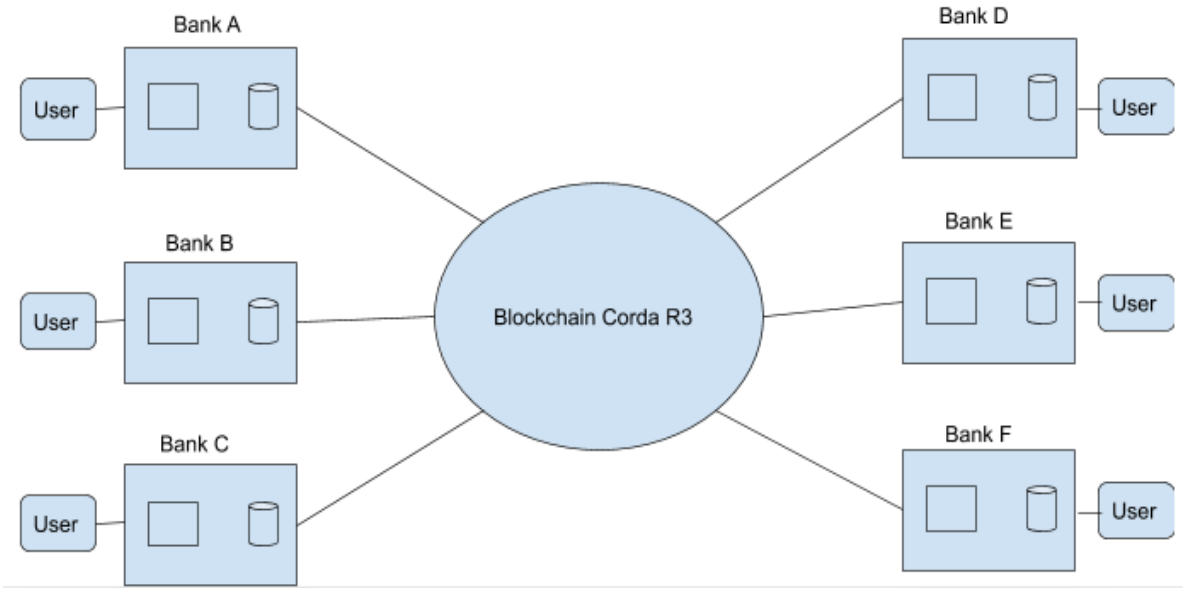
Phần mềm	Ghi chú
Oracle JDK	version 8u171 hoặc cao hơn
IDE	IntelliJ IDEA, visual code,
Git	source control

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:

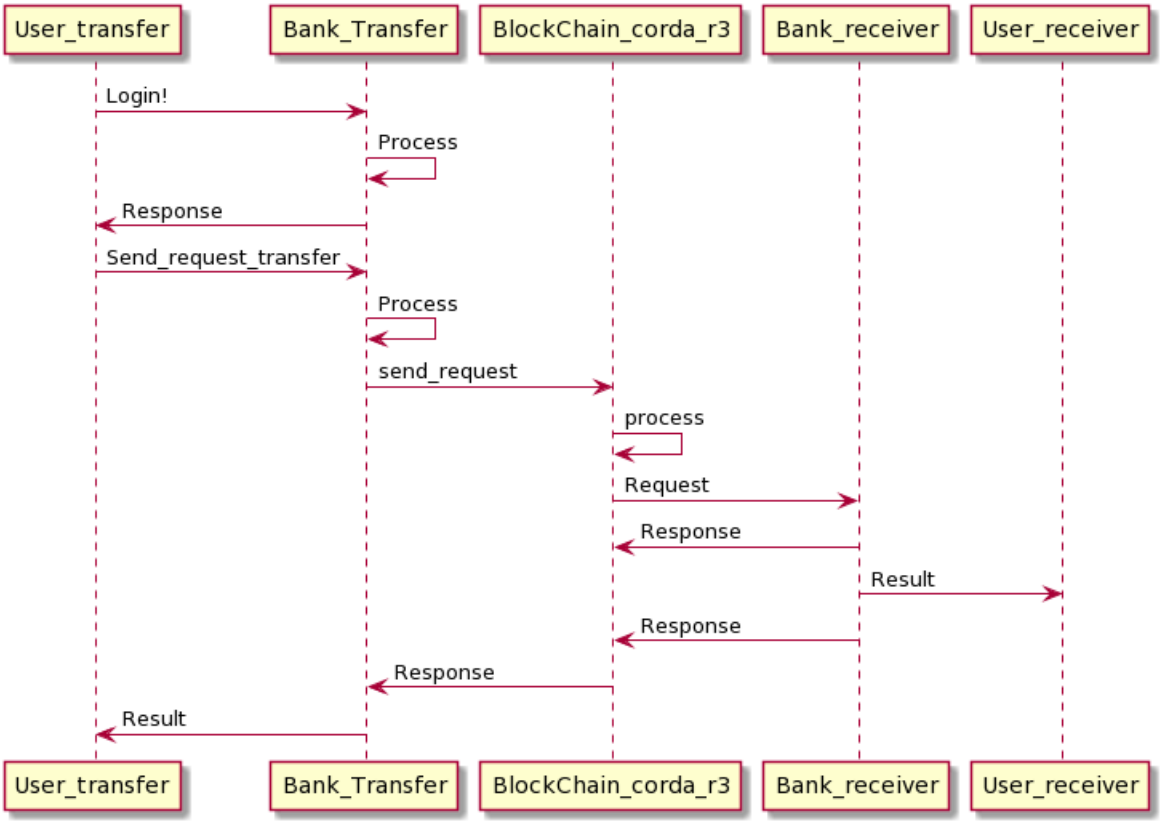
- Mạng lưới Blockchain Corda R3
- Hệ thống các ngân hàng có các node trong Blockchain
- Người dùng thuộc các ngân hàng đó.



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

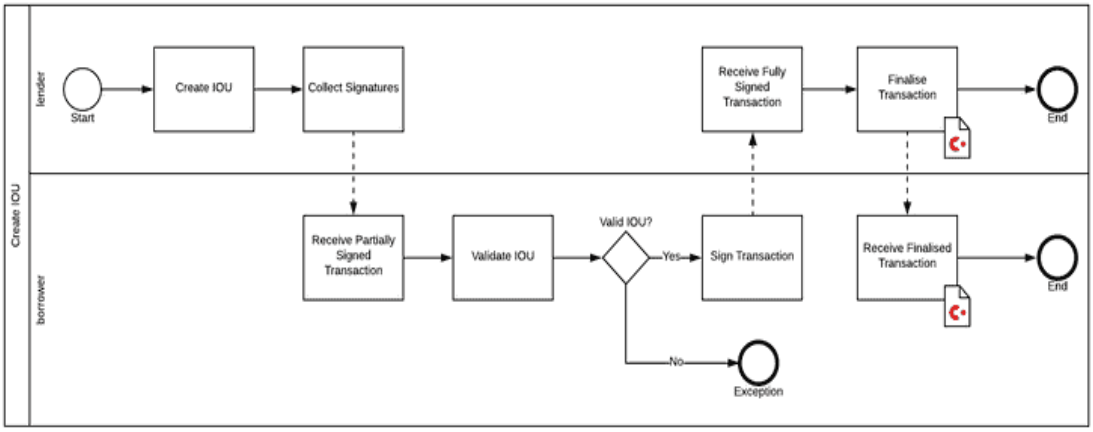
3.2.3. Đặc tả chức năng

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.

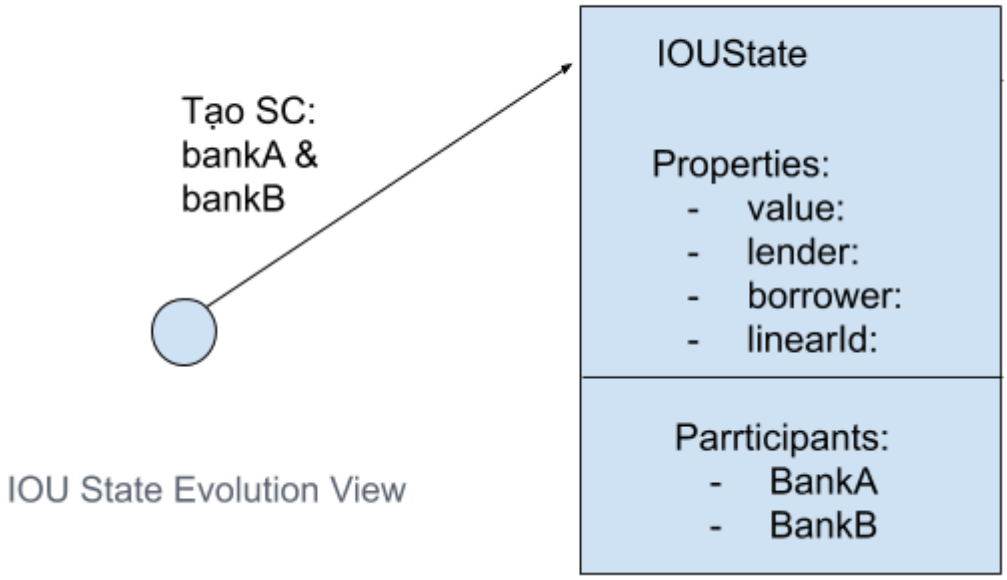


Hình 3.5: Luồng giao dịch chuyển tiền giữa 2 user khác Bank thông qua Blockchain Corda R3

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.

3.3. Thực nghiệm đánh giá

3.3.1. *Kết quả thử nghiệm*

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

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.

• Mô hình ứng dụng blockchain trong chuyển tiền liên ngân hàng.

2. Thực nghiệm:

• Xây dựng thành công hệ thống chuyển tiền liên ngân hàng 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