

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

ĐOÀN NGỌC SƠN

**NGHIÊN CỨU, ỨNG DỤNG CÔNG NGHỆ
BLOCKCHAIN TRONG THANH TOÁN DI ĐỘNG**

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội - 2017

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

ĐOÀN NGỌC SƠN

**NGHIÊN CỨU, ỨNG DỤNG CÔNG NGHỆ
BLOCKCHAIN TRONG THANH TOÁN DI ĐỘNG**

Ngành: Công nghệ Thông Tin

Chuyên ngành: Hệ Thống Thông Tin

Mã số: 60480104

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS Nguyễn Ngọc Hóa

Hà Nội - 2017

LỜI CẢM ƠN

Lời đầu tiên tôi xin gửi lời cảm ơn và lòng biết ơn sâu sắc đến thầy giáo PGS.TS Nguyễn Ngọc Hóa (bộ môn Các hệ thống thông tin – trường Đại học Công Nghệ - Đại học Quốc Gia Hà Nội), người đã giúp tôi chọn đề tài, định hình hướng nghiên cứu, tận tình hướng dẫn và chỉ bảo tôi trong quá trình thực hiện luận văn tốt nghiệp.

Tôi xin được gửi lời tri ân sâu sắc đến thầy giáo PGS.TS Trịnh Nhật Tiến, người đã tận tình chỉ bảo, giúp đỡ tôi trong quá trình học tập cũng như giai đoạn đầu của quá trình thực hiện luận văn.

Tôi cũng xin gửi lời cảm ơn các thầy, cô giáo trong trường Đại học Công nghệ -Đại học Quốc gia Hà Nội. Các thầy, cô giáo đã dạy bảo và truyền đạt cho tôi rất nhiều kiến thức, giúp tôi có được một nền tảng kiến thức vững chắc sau những năm học tập tại trường Đại học Công Nghệ. Tôi xin gửi lời cảm ơn chân thành tới các bạn khóa K21 đã ủng hộ khuyến khích tôi trong suốt quá trình học tập tại trường.

Cuối cùng, tôi muốn gửi lời cảm ơn sâu sắc nhất đến gia đình và bạn bè, đặc biệt là bố, mẹ, vợ và em trai – những người thân yêu luôn kịp thời động viên và giúp đỡ tôi vượt qua những khó khăn trong học tập cũng như trong cuộc sống.

Hà Nội, ngày tháng năm 2017

Học viên

Đoàn Ngọc Sơn

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu và thực hiện luận văn thực sự của riêng tôi, dưới sự hướng dẫn của PGS.TS Nguyễn Ngọc Hóa. Mọi tham khảo từ các tài liệu, công trình nghiên cứu liên quan trong nước và quốc tế đều được trích dẫn rõ ràng trong luận văn. Mọi sao chép không hợp lệ, vi phạm quy chế hay gian trá tôi xin hoàn toàn chịu trách nhiệm và chịu mọi kỷ luật của Nhà Trường và ĐHQG Hà Nội.

Hà Nội, ngày tháng năm 2017

Học viên

Đoàn Ngọc Sơn

MỤC LỤC

LỜI CẢM ƠN.....	ii
LỜI CAM ĐOAN	iii
MỤC LỤC.....	iv
DANH MỤC CÁC TỪ VIẾT TẮT.....	vi
DANH MỤC CÁC BẢNG BIỂU - HÌNH VẼ.....	vii
LỜI MỞ ĐẦU.....	1
Chương 1. GIỚI THIỆU CÔNG NGHỆ BLOCKCHAIN.....	3
1.1. Giới thiệu	3
1.2. Nền tảng lý thuyết.....	4
1.2.1. Hàm băm.....	4
1.2.1.1. Khái niệm hàm băm.....	4
1.2.1.2. Đặc tính của hàm băm [1].....	4
1.2.1.3. Ứng dụng của hàm băm.....	5
1.2.2. Chữ ký số	5
1.2.2.1. Khái niệm chữ ký số	5
1.2.2.2. Ứng dụng của chữ ký số	6
1.3. Các kỹ thuật chính	7
1.3.1. Cấu trúc phi tập chung	7
1.3.2. Tính toán tin cậy	9
1.3.3. Bằng chứng công việc [6].....	10
1.3.4. Tính chất của Blockchain	10
1.4. Phân loại các hệ thống Blockchain	11
1.5. Các ứng dụng điển hình của công nghệ Blockchain.....	11
1.5.1. Ứng dụng Blockchain trong tiền số	11
1.5.2. Ứng dụng Blockchain trong hợp đồng thông minh (Smart Contracts)	11
1.5.3. Một số ứng dụng nổi bật khác	12
Kết luận chương.....	14
Chương 2. THANH TOÁN DI ĐỘNG VÀ TIỀN SỐ	15
2.1 Thanh toán di động	15

2.1.1	Giới thiệu.....	15
2.1.2	Thanh toán trên Apple Store	16
2.1.3	Thanh toán trên Google Play.....	19
2.2	Tiền số	19
2.2.1	Giới thiệu	19
2.2.2	Mô hình tiền số Bitcoin	21
2.2.3	Độ an toàn của tiền số.....	29
2.2.4	Tiềm năng phát triển của tiền số.....	29
	Kết luận chương.....	31
Chương 3. ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN TRONG THANH TOÁN DI ĐỘNG.....		32
3.1	Đặt vấn đề	32
3.1.1	Bài toán đặt ra.....	32
3.1.2	Cách tiếp cận và giải pháp	32
3.2	Xây dựng hệ thống tiền số và ứng dụng mua bán sách điện tử	35
3.2.1	Kiến trúc hệ thống	35
3.2.2	Đặc tả chức năng.....	36
3.2.3	Cài đặt hệ thống tiền số TYM.....	37
3.2.4	Xây dựng các API thao tác với hệ thống tiền số.....	41
3.3	Thực nghiệm và đánh giá.....	42
3.3.1	Môi trường phát triển và công cụ	42
3.3.2	Kết quả thử nghiệm.....	42
3.3.3	Đánh giá kết quả	46
	Kết luận chương.....	47
KẾT LUẬN CHUNG.....		48
	Các kết quả thu được trong luận văn	48
	Định hướng nghiên cứu tiếp theo.....	48
TÀI LIỆU THAM KHẢO		49

DANH MỤC CÁC TỪ VIẾT TẮT

STT	Tên viết tắt	Tên đầy đủ	Giải thích
1	API	Application Programming Interface	Giao diện lập trình ứng dụng
2	BTC	Bitcoin	Một loại tiền số
3	ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán ký số đường cong Elliptic
4	HTTP	HyperText Transfer Protocol	Giao thức truyền tải siêu văn bản
5	JSON	JavaScript Object Noation	Một kiểu định dạng dữ liệu
6	MD	Message Digest	Đại diện thông điệp
7	PoW	Proof of Work	Bằng chứng công việc
8	UTXO	Unspent Transaction Output	Các Output chưa được tiêu trong tiền số

DANH MỤC CÁC BẢNG BIỂU - HÌNH VẼ

Hình 1.1: Mô hình thực hiện chữ ký số	6
Hình 1.2: Cấu trúc dữ liệu của Blockchain[6]	7
Hình 1.3: Cấu trúc của block gốc trong blockchain.....	8
Hình 2.1: Số lượng ứng dụng trên các kho ứng dụng (tháng 3/2017)	15
Hình 2.2: Luồng thanh toán của Apple	16
Hình 2.3: Mô hình thanh toán có máy chủ web	18
Hình 2.4: Luồng thanh toán của Google	19
Hình 2.5: Biểu đồ chấp nhận BTC trên thế giới	22
Hình 2.6: Thông tin một block trong mạng bitcoin	24
Hình 2.7: Mô hình giao dịch của Bitcoin.....	24
Hình 2.8: Dữ liệu trong một Transaction	25
Hình 2.9: Tạo khóa để thực hiện giao dịch trong bitcoin.....	26
Hình 2.10: Danh sách các giao dịch trong một block [2]	28
Hình 2.11: So sánh tốc độ ký của ECDSA và RSA.....	29
Hình 2.12: Giá trị vốn hóa trên thị trường của một số đồng tiền điện tử (11/2017).....	30
Hình 2.13: Tăng trưởng của đồng tiền số Bitcoin (BTC)	30
Hình 2.14: Tăng trưởng của đồng tiền số Ethereum (ETH).....	31
Hình 3.1: Mô hình giải pháp ứng dụng tiền số trong thanh toán di động	33
Hình 3.2: Mô hình sàn giao dịch mua bán tiền số.....	34
Hình 3.3: Kiến trúc tổng quan của hệ thống	35
Hình 3.4: Biểu đồ luồng của hệ thống	37
Hình 3.5: Tạo một giao dịch trong mạng blockchain	38
Hình 3.6: Hàm giải bài toán PoW [6]	39
Hình 3.7: Tạo một block mới.....	39
Hình 3.8: Thêm block vào blockchain.....	40
Hình 3.9: Xác nhận một giao dịch là hợp lệ	40
Bảng 3.1: Các API của hệ thống tiền số	41
Bảng 3.2: Cấu hình phần cứng.....	42
Bảng 3.3: Các phần mềm sử dụng tiến hành thực nghiệm.....	42
Hình 3.10: Danh sách các sách đang bán.....	43
Hình 3.11: Thông tin cá nhân của người dùng.....	44
Hình 3.12: Giao diện xác nhận thanh toán.....	44
Hình 3.13: Các sách đã tải về.....	45
Hình 3.14: Số TYM còn lại sau khi thanh toán	45
Hình 3.15: Dữ liệu trả về của hệ thống tiền số khi giao dịch thành công.....	46
Hình 3.16: Hình ảnh blockchain sau khi block mới được thêm vào.....	46

LỜI MỞ ĐẦU

Internet xuất hiện không chỉ phục vụ cho việc gửi email hay tải phần mềm mà nó còn là động lực để phát triển nền kinh tế toàn cầu. Trong thực tế, Internet đã trở thành trình điều khiển của nền kinh tế. Sự xuất hiện của Internet và các mạng cục bộ đã giúp cho việc trao đổi thông tin trở nên nhanh chóng, dễ dàng hơn. Email cho phép chúng ta nhận hay gửi thư ngay trên máy tính của mình, E-business cho phép thực hiện giao dịch, buôn bán trên mạng... Cũng giống như Internet, blockchain xuất phát như một trào lưu với đồng tiền ảo Bitcoin.

Sự phát triển của Internet cũng đồng hành với những tổn thất sau các cuộc tấn công mạng, gây ảnh hưởng lớn đến nền kinh tế cũng như xã hội. Theo cuộc khảo sát của hãng phân tích Grant Thornton, khoản tiền mà doanh nghiệp mất vào tay tin tặc ở Châu Á-Thái Bình Dương lên tới 81,3 tỉ đô la trong vòng 12 tháng (tính đến cuối tháng 9/2015). Mức tổn thất từ các đợt tấn công mạng ở châu Á nhiều hơn Bắc Mỹ tới 20 tỉ USD và EU với con số tương tự, và chiếm đến hơn 25% tổng mức tổn thất của thế giới (315 tỉ USD)... Tại Việt Nam cũng xảy ra tình trạng mất an toàn với các tài khoản gửi ngân hàng, điển hình như vụ tấn công vào Vietcombank. [15]

Tháng 2/2016, thông tin về việc Ngân hàng Trung ương Bangladesh bị tin tặc đánh cắp 101 triệu USD gây chấn động thế giới là một bài học cho bất cứ tổ chức nào. Sự cố xảy ra được cho là do Ngân hàng nước này sử dụng bộ định tuyến cũ giá 10 USD mà không có bất cứ một hệ thống tường lửa nào. Số tiền tổn thất trong vụ này có thể lên đến hơn 1 tỷ USD nếu như tin tặc không viết sai lỗi chính tả. [15]

Từ những rủi ro từ an ninh mạng nên các tổ chức tài chính cần những công nghệ mới, ví dụ như nền tảng của đồng tiền số Bitcoin, chính là Blockchain, được kì vọng không chỉ nhằm cắt giảm chi phí ngân hàng mà còn đảm bảo tính an toàn và xa hơn nữa là cách mạng hóa các giải pháp bảo mật.

Với thực trạng đó, luận văn này có mục tiêu nghiên cứu, ứng dụng công nghệ Blockchain và công nghệ tiền số trong việc hỗ trợ thanh toán trên nền thiết bị di động. Mục tiêu này sẽ được tiến hành với những nội dung chính gồm:

Tìm hiểu tổng quan về công nghệ Blockchain, đồng tiền số nói chung và đồng tiền Bitcoin nói riêng. Một số lý thuyết toán học cơ bản, các kỹ thuật chính liên quan tới công nghệ Blockchain và cũng như tiềm năng ứng dụng thực tiễn cũng sẽ được nghiên cứu trong luận văn này.

Đề xuất giải pháp ứng dụng của công nghệ Blockchain trong việc thanh toán của các ứng dụng điện thoại di động (In-app purchase).

Xây dựng hệ thống thử nghiệm với khả năng thanh toán di động dựa trên công nghệ Blockchain và tiền số.

Các kết quả của luận văn thu được sau khi thực hiện các nội dung nghiên cứu trên được tổng hợp trên bản thảo gồm 3 chương chính như sau:

Chương 1: Giới thiệu công nghệ Blockchain

Đưa ra cái nhìn tổng quan về công nghệ Blockchain [6]. Nêu ra các nền tảng lý thuyết và các kỹ thuật chính sử dụng trong công nghệ Blockchain. Đồng thời trong chương này, luận văn cũng chỉ ra một số ứng dụng điển hình của Blockchain đang được áp dụng ở thời điểm hiện tại như tiền số, hợp đồng thông minh (smart contract [6])...

Chương 2: Thanh toán di động và tiền số

Trong chương này, luận văn sẽ trình bày về mô hình thanh toán di động truyền thống đang được sử dụng rộng rãi ở thời điểm hiện tại. Đồng tiền số cũng sẽ được trình bày cụ thể trong Chương 2, cách thức hoạt động của đồng tiền số nổi bật nhất hiện nay là Bitcoin sẽ được trình bày cụ thể và chi tiết.

Chương 3: Ứng dụng tiền số trong thanh toán di động

Trình bày về việc ứng dụng tiền số trong thanh toán các ứng dụng di động, ưu điểm so với phương pháp truyền thống vẫn đang được sử dụng phổ biến. Chương trình mô phỏng mô hình thanh toán sử dụng tiền số sẽ được mô tả cụ thể trong chương này.

Phần kết luận:

Nêu lên xu hướng phát triển của công nghệ blockchain, tóm tắt kết quả đạt được của luận văn, đồng thời đưa ra những định hướng nghiên cứu tiếp theo.

Chương 1. GIỚI THIỆU CÔNG NGHỆ BLOCKCHAIN

1.1. Giới thiệu

Blockchain (chuỗi khối), tên ban đầu block chain là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối thông tin được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối thông tin đều chứa thông tin về thời gian khởi tạo và được liên kết tới khối trước đó, kèm theo thông tin về dữ liệu giao dịch. [3]

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. Nếu một phần của hệ thống blockchain sụp đổ, những máy tính và nút khác sẽ tiếp tục hoạt động để bảo vệ thông tin.

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 [5].

Một số trích dẫn đáng chú ý về công nghệ này được liệt kê dưới đây:

- “Thế hệ đầu tiên của cuộc cách mạng kỹ thuật số mang lại cho chúng ta thông tin của Internet. Thế hệ thứ hai - được hỗ trợ bởi công nghệ blockchain - mang lại cho chúng ta giá trị của Internet: một nền tảng mới để định hình lại thế giới kinh doanh và biến đổi thứ tự công việc của con người trở nên tốt hơn.” [3]
- “Blockchain là một kho lưu trữ, cơ sở dữ liệu phân tán toàn cầu, chạy trên hàng triệu thiết bị và mở cho mọi người, không chỉ đơn thuần là thông tin mà còn cả những thứ có giá trị, cả danh hiệu, hành vi, danh tính, thậm chí cả phiếu bầu - có thể được di chuyển, lưu trữ và quản lý một cách an toàn và tư nhân. Sự tin tưởng được thiết lập thông qua hợp tác giữa số đông và mã thông minh chứ không phải bởi các nhà trung gian mạnh mẽ như các chính phủ và ngân hàng.” [3]

Không lâu sau khi Bitcoin được phát hành trên thế giới, nhiều người nhanh chóng nhận ra công nghệ đằng sau Bitcoin – Blockchain – có thể làm được nhiều hơn là xử lý các giao dịch tiền tệ. Nhà phân phối lớn nhất thế giới cho những hợp đồng tài chính cho rằng có thể làm cho các hợp đồng trở nên an toàn hơn bằng cách xây dựng một hệ thống dựa trên công nghệ Blockchain vào năm 2018. Nếu kế hoạch này đi vào hoạt động, mỗi năm sẽ có 11 nghìn tỷ USD được giao dịch qua hệ thống này [7].

1.2. Nền tảng lý thuyết

Công nghệ Blockchain [6] được phát triển dựa trên hai nền tảng kỹ thuật chính là hàm băm và chữ ký số. Mỗi người dùng sẽ sở hữu một cặp khóa gồm khóa bí mật và khóa công khai. Khóa bí mật được lưu trữ bí mật và sử dụng để ký kết các giao dịch. Các giao dịch đã ký dùng chữ ký số được phát đi trên toàn bộ mạng. Chữ ký số liên quan đến hai giai đoạn: giai đoạn ký kết và giai đoạn xác minh. Ví dụ: người dùng A muốn gửi một thông báo cho người dùng B, trong giai đoạn ký, A mã hóa dữ liệu của mình bằng khóa bí mật và gửi cho B kết quả đã được mã hóa và dữ liệu gốc. Trong giai đoạn xác minh, B xác nhận giao dịch bằng khóa công khai của A. Bằng cách đó, B có thể dễ dàng kiểm tra xem dữ liệu có bị giả mạo hay không [6].

1.2.1. Hàm băm

Hàm băm [1] dùng để chuyển đổi từ một thông tin sang một đoạn mã. Bất kỳ nỗ lực gian lận nào để thay đổi bất kỳ phần nào của blockchain sẽ bị phát hiện ngay lập tức vì giá trị băm mới sẽ không phù hợp với thông tin cũ trên blockchain. Bằng cách này, ngành khoa học bảo mật thông tin (cần thiết cho việc mã hóa thông tin và mua sắm trực tuyến, ngân hàng) đã trở thành một công cụ hiệu quả để giao dịch mở.

1.2.1.1. Khái niệm hàm băm

Hàm băm (hash function) là thuật toán dùng để ánh xạ dữ liệu có kích thước bất kỳ sang một giá trị “băm” có kích thước cố định, giá trị băm còn được gọi là “đại diện thông điệp” hay “đại diện bản tin”. [1]

Hàm băm là hàm một chiều, theo nghĩa giá trị của hàm băm là duy nhất, và từ giá trị băm này, “**khó**” có thể suy ngược lại được nội dung hay độ dài ban đầu của thông điệp gốc.

Các hàm băm dòng MD: MD2, MD4, MD5 được Rivest đưa ra có kết quả đầu ra với độ dài là 128 bit. Hàm băm MD4 đưa ra vào năm 1990. Một năm sau phiên bản mạnh MD5 cũng được đưa ra. Chuẩn hàm băm an toàn: SHA, phức tạp hơn nhiều cũng dựa trên các phương pháp tương tự, được công bố trong Hồ sơ Liên bang năm 1992 và được chấp nhận làm tiêu chuẩn vào năm 1993 do Viện Tiêu Chuẩn và Công Nghệ Quốc Gia (NIST), kết quả đầu ra có độ dài 160 bit.

1.2.1.2. Đặc tính của hàm băm [1]

Hàm băm **h** là hàm một chiều (One-way Hash) với các đặc tính sau:

1. Với thông điệp đầu vào (bản tin gốc) \mathbf{x} , chỉ thu được giá trị duy nhất $\mathbf{z} = \mathbf{h}(\mathbf{x})$.
2. Nếu dữ liệu trong bản tin \mathbf{x} bị thay đổi hay bị xóa để thành bản tin \mathbf{x}' , thì giá trị băm $\mathbf{h}(\mathbf{x}') \neq \mathbf{h}(\mathbf{x})$. Cho dù chỉ là một sự thay đổi nhỏ, ví dụ chỉ thay đổi 1 bit dữ liệu của bản tin gốc \mathbf{x} , thì giá trị băm $\mathbf{h}(\mathbf{x})$ của nó cũng vẫn thay đổi. Điều này có nghĩa là: hai thông điệp khác nhau, thì giá trị băm của chúng cũng khác nhau.
3. Nội dung của bản tin gốc “khó” thể suy ra từ giá trị hàm băm của nó. Nghĩa là: với thông điệp \mathbf{x} thì “dễ” tính được $\mathbf{z} = \mathbf{h}(\mathbf{x})$, nhưng lại “khó” tính ngược lại được \mathbf{x} nếu chỉ biết giá trị băm $\mathbf{h}(\mathbf{x})$ (Kể cả khi biết hàm băm \mathbf{h}).

1.2.1.3. Ứng dụng của hàm băm

Hàm băm được sử dụng trong nhiều ứng dụng thực tế, dưới đây là một số ứng dụng nổi bật của hàm băm được sử dụng phổ biến:

- Đảm bảo dữ liệu không bị sửa đổi: Khi An muốn gửi tài liệu X cho Bình, An gửi cả giá trị băm của X và thuật toán băm. Khi nhận được tài liệu X, Bình dùng thuật toán băm đó băm lại X và so sánh với giá trị băm An đã gửi, nếu kết quả không trùng khớp chứng tỏ tài liệu X đã bị chỉnh sửa.
- Hỗ trợ các thuật toán chữ ký số: Hàm băm giúp tạo ra đại diện tài liệu, các thuật toán ký số thay ví ký trên tài liệu ban đầu có dung lượng lớn, sẽ ký lên đại diện của tài liệu đó. Thời gian thực hiện của thuật toán ký sẽ nhanh hơn nhiều lần.
- Xây dựng cấu trúc dữ liệu bảng băm: Bảng băm là một cấu trúc dữ liệu cho phép tổ chức lưu trữ và tìm kiếm dữ liệu một cách nhanh chóng và thuận tiện.

1.2.2. Chữ ký số

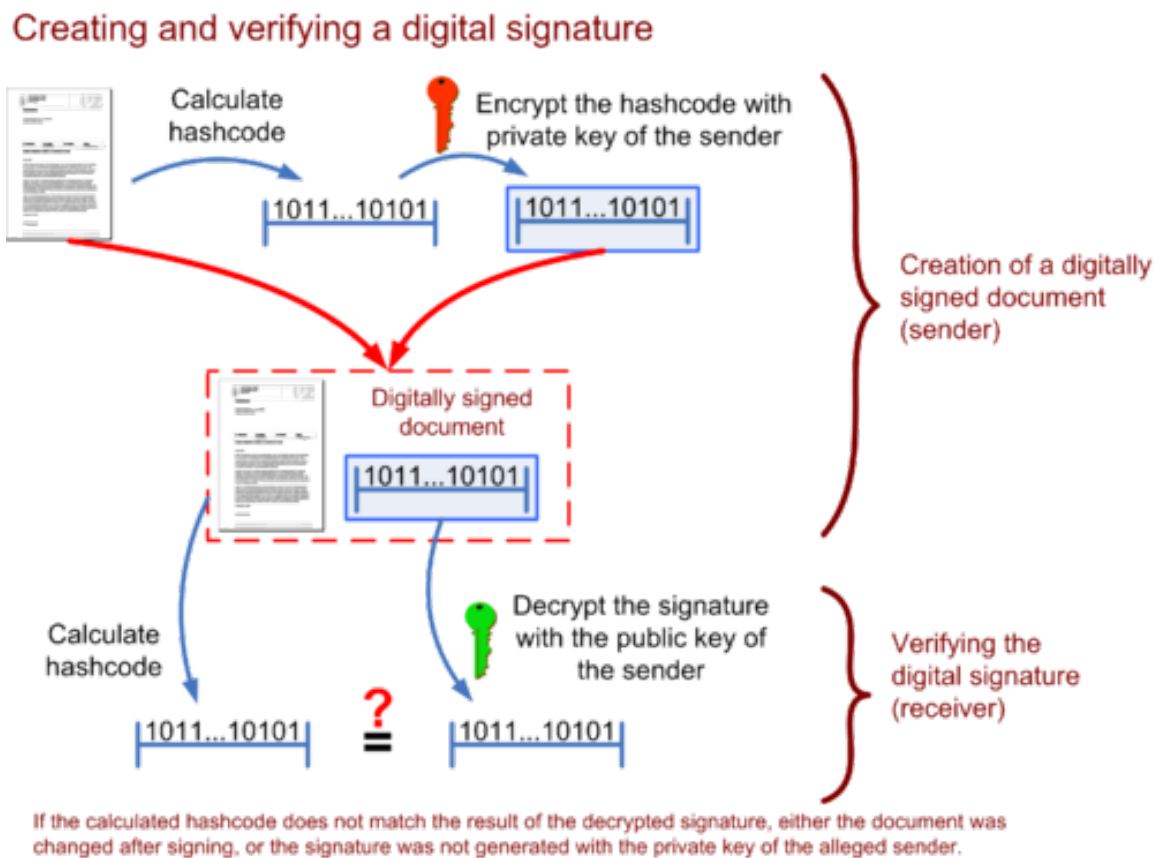
1.2.2.1. Khái niệm chữ ký số

Về mặt công nghệ, chữ ký số [1] là một thông điệp dữ liệu đã được mã hóa gắn kèm theo một thông điệp dữ liệu khác nhằm xác thực người gửi thông điệp đó. Quá trình ký và xác nhận chữ ký như sau: Người gửi muốn gửi thông điệp cho bên khác thì sẽ dùng một hàm băm, băm thông điệp gốc thành một “thông điệp tóm tắt” (Message Digest), thuật toán này được gọi là thuật toán băm (hash function) đã được trình bày trong mục 1.2.1. Người gửi mã hoá bản tóm tắt thông điệp bằng khóa bí mật của mình (sử dụng phần mềm bí mật được cơ quan

chứng thực cấp) để tạo thành một chữ ký số. Sau đó, người gửi tiếp tục gắn kèm chữ ký số này với thông điệp dữ liệu ban đầu và gửi thông điệp đã gắn kèm với chữ ký một cách an toàn qua mạng cho người nhận.

Sau khi nhận được, người nhận sẽ dùng khoá công khai của người gửi để giải mã chữ ký số thành bản tóm tắt thông điệp. Người nhận cũng dùng hàm băm giống hệt như người gửi đã làm đối với thông điệp nhận được để biến đổi thông điệp nhận được thành một bản tóm tắt thông điệp. Người nhận so sánh hai bản tóm tắt thông điệp này, nếu chúng giống nhau tức là chữ ký số đó là xác thực và thông điệp đã không bị thay đổi trên đường truyền đi.

Ngoài ra, chữ ký số có thể được gắn thêm một “nhãn” thời gian: sau một thời gian nhất định quy định bởi nhãn đó, chữ ký gốc sẽ không còn hiệu lực, đồng thời nhãn thời gian cũng là công cụ để xác định thời điểm ký.



Hình 1.1: Mô hình thực hiện chữ ký số

1.2.2.2. Ứng dụng của chữ ký số

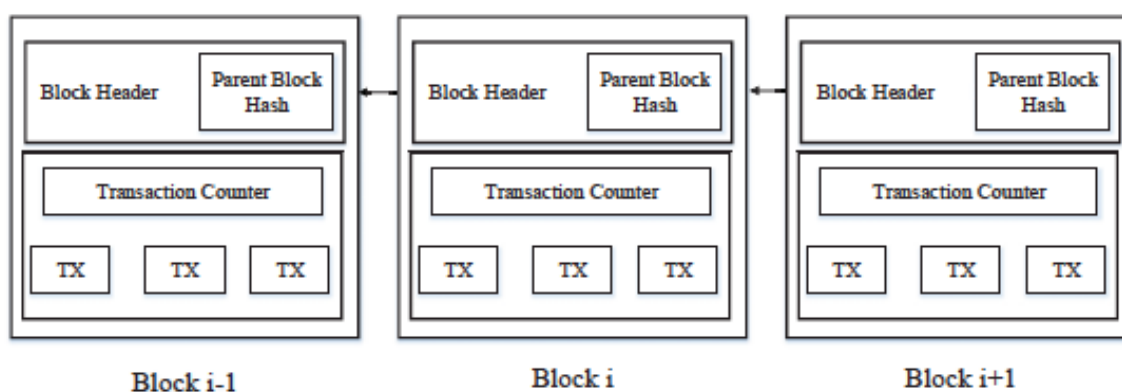
Chữ ký số có ý nghĩa to lớn và trở thành một phần không thể thiếu đối với ngành mật mã học. Ứng dụng của chữ ký số đã được triển khai trên nhiều quốc gia trên thế giới, trong đó có Việt Nam. So với chữ ký tay, chữ ký số giúp các cá nhân, doanh nghiệp thực hiện việc ký các tài liệu được nhanh chóng, hiệu quả hơn. Một số ứng dụng cụ thể của chữ ký số trong thực tế có thể kể đến như sau:

- Ứng dụng trong chính quyền điện tử: Các cá nhân và doanh nghiệp sẽ không cần đến các cơ quan nhà nước để xuất trình giấy tờ cũng như ký kết các giấy tờ. Thay vào đó, việc ký và gửi các tài liệu hoàn toàn thông qua hệ thống máy tính. Hiện nay ngành thuế ở Việt Nam đã cho phép gửi tài liệu kê khai thuế qua mạng sử dụng chữ ký số.
- Ứng dụng trong ký kết hợp đồng: Việc ký kết các hợp đồng thường được thực hiện với sự có mặt của tất cả các bên liên quan và cần người chứng kiến, điều này gây tốn thời gian đặc biệt là khi các bên ở xa nhau về khoảng cách địa lý. Chữ ký số có thể cải thiện được việc này, các bên có thể xác thực được chữ ký của các bên liên quan khác thông qua các thuật toán kiểm tra chữ ký.

Trong tương lai, tiềm năng của chữ ký số chắc chắn sẽ còn tiến xa hơn nữa và có thể được ứng dụng trong nhiều ứng dụng cụ thể khác như bỏ phiếu điện tử, y tế điện tử, ...

1.3. Các kỹ thuật chính

Công nghệ blockchain [6] tương đồng với cơ sở dữ liệu, chỉ khác ở việc tương tác với cơ sở dữ liệu. Để hiểu blockchain, cần nắm được năm định nghĩa sau: chuỗi khối (block chain), cơ chế đồng thuận phi tập trung (decentralized consensus), tính toán tin cậy (trusted computing), hợp đồng thông minh (smart contracts [6]) và bằng chứng công việc (proof of work [6]). Mô hình tính toán này là nền tảng của việc tạo ra các ứng dụng phân tán.









Hình 1.2: Cấu trúc dữ liệu của Blockchain[6]

1.3.1. Cấu trúc phi tập trung

Cơ chế này ngược lại với mô hình truyền thống – cơ sở dữ liệu được tập trung và được dùng để quản lý và xác thực giao dịch. Công nghệ Blockchain không dựa vào các tổ chức thứ ba để quản lý và xác thực, không có kiểm soát trung tâm, tất cả các nút nhận được thông tin tự kiểm tra, truyền tải, và quản lý,

đặt sự tin tưởng vào các nút, cho phép các nút lưu trữ các giao dịch trong một khối (block) [5]. Các block được ghép nối với nhau tạo nên một chuỗi khối (blockchain). Cấu trúc của một block được mô tả như hình 1.3. Cấu trúc phi tập chung là đặc điểm nổi bật và quan trọng nhất của Blockchain.

 Genesis Block	
 Previous Hash	0
 Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
 Data	Welcome to Blockchain CLI!
 Hash	0000018035a828da0...
 Nonce	56551

Hình 1.3: Cấu trúc của block gốc trong blockchain

Mỗi block trong Blockchain bao gồm các thành phần sau:

- Index (Block #): Thứ tự của block (block gốc có thứ tự 0)
- Hash: Giá trị băm của block
- Previous Hash: Giá trị băm của block trước
- Timestamp: Thời gian tạo của block
- Data: Thông tin lưu trữ trong block
- Nonce: Giá trị biến thiên để tìm ra giá trị băm thỏa mãn yêu cầu của mỗi Blockchain.

Giá trị băm (Hash) sẽ băm toàn bộ các thông tin cần thiết như timestamp, previous hash, index, data, nonce.

Khi có một block mới được thêm vào, block mới sẽ có giá trị “Previous Hash” là giá trị băm của block được thêm trước nó. Blockchain tìm kiếm block được thêm vào gần nhất để lấy giá trị index và previous hash. Block tiếp theo của hình 1.3 sẽ được tính như sau:

- Index: $0+1 = 1$
- Previous Hash: 0000018035a828da0...

- Timestamp: thời gian block được tạo ra
- Data: dữ liệu lưu trữ trong block
- Hash: ??
- Nonce: ??

Ta cần tìm giá trị “nonce” phù hợp để có giá trị băm Hash thỏa mãn điều kiện của Blockchain (có 4 số 0 ở đầu giá trị băm). Số lượng số 0 ở đầu được gọi là “difficulty” [12]. Mã giả của hàm kiểm tra giá trị Hash có thỏa mãn điều kiện hay không được viết như sau:

```
function isValidHashDifficulty(hash, difficulty) {
  for (var i = 0, b = hash.length; i < b; i++) {
    if (hash[i] !== '0') {
      break;
    }
  }
  return i >= difficulty;
}
```

Công việc trên cũng được gọi là bằng chứng công việc (Proof of Work) [6]. Quá trình tìm kiếm giá trị Nonce được thực hiện bằng mã giả sau:

```
let nonce = 0;
let hash;
let input;
while(!isValidHashDifficulty(hash)) {
  nonce = nonce + 1;
  input = index + previousHash + timestamp + data + nonce;
  hash = CryptoJS.SHA256(input)
}
```

Bằng cách lưu trữ dữ liệu trên tất cả các nút của mình, mạng blockchain loại bỏ các rủi ro đi kèm với dữ liệu được tổ chức lưu trữ tập trung. Trong mạng không có các điểm tập trung dễ bị tổn thương cho hệ thống, không có các điểm trung tâm làm cho hệ thống dừng hoạt động (central point of failure). Bất kỳ nút nào trong mạng khi dừng hoạt động sẽ không ảnh hưởng đến sự vận hành của hệ thống.

1.3.2. Tính toán tin cậy

Mỗi nút trong mạng có một bản sao lưu trữ toàn bộ blockchain [6], chất lượng của dữ liệu phụ thuộc vào sự đồng bộ liên tục theo thời gian giữa các nút. Các nút trong mạng đều có độ tin cậy như nhau, không có nút nào đáng tin cậy

hơn nút nào. Trao đổi dữ liệu trong hệ thống không yêu cầu các nút tin tưởng lẫn nhau. Quy chế hoạt động của toàn bộ hệ thống và tất cả các nội dung dữ liệu đều công khai và minh bạch. Vì vậy, các nút không thể giả mạo các quy tắc và thời gian do hệ thống chỉ định.

1.3.3. Bằng chứng công việc [6]

Bằng chứng công việc (proof of work) trong một mạng blockchain được hiểu là một thử thách cho các nút trong mạng. Cụ thể là các nút cần tìm ra các block mới của blockchain bằng cách tìm ra giá trị băm thỏa mãn điều kiện cho trước. Trong mục 1.3.1, điều kiện này là giá trị “difficulty” – số lượng số 0 đứng phía trước giá trị băm.

1.3.4. Tính chất của Blockchain

Cơ chế đồng thuận phân quyền (decentralized consensus)

Cơ chế này ngược lại với mô hình cổ điển về cơ chế đồng thuận tập trung – nghĩa là khi một cơ sở dữ liệu tập trung được dùng để quản lý việc xác thực giao dịch. Một sơ đồ phi tập trung chuyển giao quyền lực và sự tin tưởng cho một mạng lưới ảo phi tập trung và cho phép các nút của mạng lưới đó liên tục lưu trữ các giao dịch trên một khối (block) công khai, tạo nên một chuỗi (chain) độc nhất: chuỗi khối (blockchain). Mỗi khối kế tiếp chứa một giá trị băm của khối trước nó; vì thế, mã hóa (thông qua hàm băm) được sử dụng để bảo đảm tính xác thực của nguồn giao dịch và loại bỏ sự cần thiết phải có một bên trung gian. Sự kết hợp của mã hóa và công nghệ blockchain lại đảm bảo rằng sẽ không bao giờ một giao dịch được thực hiện hai lần. [11]

Bảo trì tập thể (collective maintainance)

Khối dữ liệu (block) trong hệ thống được duy trì bởi tất cả các nút với chức năng bảo trì trong toàn bộ hệ thống. Bất kỳ nút nào cũng có khả năng ghi block vào blockchain. Hơn nữa, các nút trong hệ thống có thể được tham gia bởi bất cứ ai. [5]

Tính bảo mật và độ tin cậy

Khi không nắm được 51% số nút trong mạng, dữ liệu mạng không thể bị kiểm soát và sửa đổi. Do đó, bản thân Blockchain đã trở nên tương đối an toàn và có thể tránh việc sửa đổi dữ liệu. Vì thế, nếu một số lượng lớn các nút có khả năng tính toán mạnh được tham gia vào hệ thống thì dữ liệu trong hệ thống này sẽ có độ bảo mật cao hơn. [5]

Mã nguồn mở

Công nghệ blockchain được phát hành theo mã nguồn mở. Ngoài thông tin cá nhân được mã hóa bởi các bên kinh doanh, dữ liệu Blockchain có thể truy cập được bởi tất cả mọi người. Bất cứ ai cũng có thể tìm kiếm dữ liệu Blockchain thông qua giao diện công khai, cũng như phát triển các ứng dụng có liên quan. Toàn bộ hệ thống rất minh bạch. [5]

1.4. Phân loại các hệ thống Blockchain

Phân chia theo tính công khai, các hệ thống Blockchain hiện tại được chia làm 3 loại: blockchain công khai, blockchain bí mật và blockchain liên kết [6]. Trong blockchain công khai, tất cả các dữ liệu được hiển thị công khai và tất cả mọi người có thể tham gia và trở thành một nút vào trong mạng blockchain. Trong blockchain liên kết, chỉ có các nút được chỉ định để tham gia vào mạng blockchain. Blockchain bí mật chỉ bao gồm các nút của một tổ chức cụ thể.

1.5. Các ứng dụng điển hình của công nghệ Blockchain

Blockchain được đảm bảo nhờ cách thiết kế sử dụng hệ thống lưu trữ phân cấp với khả năng chịu lỗi cao. Vì vậy Blockchain phù hợp để ghi lại những sự kiện, hồ sơ y tế, xử lý giao dịch, công chứng, danh tính và chứng minh nguồn gốc,... Công nghệ này có tiềm năng giúp chống lại việc dữ liệu bị thay đổi, xử lý các vấn đề thiếu tính minh bạch trong bối cảnh thương mại toàn cầu.

1.5.1. Ứng dụng Blockchain trong tiền số

Blockchain không chỉ dành riêng cho Bitcoin. Blockchain là công nghệ đằng sau, bảo đảm cho Bitcoin và những đồng tiền số (digital currency) khác hoạt động. Điều này có nghĩa là: Bất cứ đồng tiền nào chưa chứng minh được chúng sở hữu công nghệ Blockchain thì chúng ta đều có quyền nghi ngờ tính chính xác của của đồng tiền đó. Cách thức hoạt động của tiền số sẽ được trình bày cụ thể trong chương 2.

1.5.2. Ứng dụng Blockchain trong hợp đồng thông minh (Smart Contracts)

Smart Contract [9] (Hợp đồng thông minh) là một thuật ngữ mô tả khả năng tự đưa ra các điều khoản và thực thi thỏa thuận của hệ thống máy tính bằng cách sử dụng công nghệ Blockchain. Toàn bộ quá trình hoạt động của Smart Contract là hoàn toàn tự động và không có sự can thiệp từ các yếu tố bên ngoài. Xe tự lái, hợp đồng thuê nhà dạng chìa khóa trao tay hay thu phí bảo hiểm...vv chỉ là một số ví dụ về cách Smart Contract có thể chi phối hoạt động kinh doanh và đời sống của con người trong tương lai.

Smart Contract giúp đảm bảo việc thực thi hợp đồng hiệu quả hơn hợp đồng truyền thống và giảm thiểu những chi phí giao dịch gây lãng phí cho các

bên. Các điều khoản của Smart Contract tương đương với một hợp đồng pháp lý và được ghi lại dưới dạng ngôn ngữ lập trình và không thể thay đổi.

Mục tiêu chính của Smart Contract là cho phép hai bên không cần xác định danh tính có thể làm việc hay giao dịch với nhau trên Internet mà không cần thông qua trung gian.

Sự khác biệt giữa Truyền thống và hiện đại

Hợp đồng truyền thống được tạo ra bởi các chuyên gia pháp lý với một lượng lớn tài liệu và cần bên thứ ba chứng thực. Điều này rất mất thời gian và trên thực tế vẫn thường xảy ra các trường hợp lừa đảo, làm giả. Nếu hợp đồng xảy ra sự cố thì cần dựa vào sự giải quyết của tư pháp, điều này dẫn đến tốn kém nhiều chi phí liên quan. Thậm chí trường hợp xấu xảy ra là mâu thuẫn.

Với Smart Contract được tạo ra bởi hệ thống máy tính bằng các ngôn ngữ lập trình. Trong đó đã nêu rõ các điều khoản và hình phạt tương đương giống như hợp đồng truyền thống đưa ra. Điều khác biệt là, Smart Contract không cần bất cứ sự can thiệp nào của con người, do vậy đảm bảo việc thực thi là chính xác và công bằng nhất. Toàn bộ đoạn mã của Smart Contract được thực hiện bởi hệ thống sổ cái phân tán của Blockchain.

Như vậy, dựa trên công nghệ Blockchain, ứng dụng Smart Contract tiếp tục cho chúng ta thấy mức độ tin cậy cao về mặt thỏa thuận và triển khai thực thi. Điều này giúp chúng ta liên tưởng tới việc ứng dụng Smart Contract sẽ làm thay đổi hoàn toàn suy nghĩ của con người trong các mối quan hệ có sự ràng buộc. Đặc biệt trong kinh doanh, điều này là vô cùng cần thiết.

1.5.3. Một số ứng dụng nổi bật khác

Ngành vận tải biển

Maersk là công ty vận tải biển lớn nhất thế giới vừa qua đã hoàn tất việc thử nghiệm ứng dụng blockchain vào theo dõi hàng hóa. Bài kiểm tra không chỉ có Maersk mà còn bao gồm sự tham gia của đại diện Hải quan Hà Lan và Bộ An Ninh Nội Địa Hoa Kỳ. Công nghệ blockchain đảm bảo độ tin cậy thông qua chữ ký điện tử giúp cho việc bỏ sót hoặc gian lận hàng hóa trong quá trình vận chuyển trở nên khó khăn hơn và giảm thời gian trung chuyển hàng hóa.

Ngành ngân hàng

Bất chấp sự phức tạp đặc thù của mình, ngành ngân hàng vẫn bị ám ảnh bởi các hệ thống chậm chạp có thể mất hàng giờ hoặc vài ngày để xác nhận các giao dịch cơ bản như bán cổ phiếu hoặc chuyển tiền. Tuy nhiên, việc Barclays (một công ty của nước Anh chuyên điều hành dịch vụ tài chính trên toàn thế giới) tiến hành một giao dịch đột phá (liên quan đến xuất khẩu bơ) bằng việc sử dụng công nghệ blockchain vào năm 2016 cho thấy điều này đang dần thay đổi. Các ngân hàng lớn thậm chí đang dự kiến sử dụng blockchain để làm lại hệ thống SWIFT - được sử dụng trong các giao dịch liên ngân hàng toàn cầu.

Ngành tạp hóa

Walmart là một trong những doanh nghiệp tiên phong sử dụng blockchain, gã khổng lồ bán lẻ này đã sử dụng blockchain từ năm 2016 để theo dõi nguồn lợn nhập từ Trung Quốc đến Mỹ. Trong tháng 8, một nhóm nông dân ở tiểu bang Arkansas đã in mã QR trên thùng đựng thịt gà để theo dõi giao dịch. Tất cả những ứng dụng này đều giúp nhà cung cấp giảm thiểu số lượng thực phẩm bị hư hỏng và ngăn chặn bệnh dịch tràn lan.

Ngành luật pháp

Tất cả các bản thỏa thuận từ bán nhà cho đến hợp đồng lao động đều yêu cầu có sự tham gia của luật sư và tòa án. Hiện nay, nhiều công ty đang thử nghiệm sáng kiến hợp đồng thông minh - một ứng dụng của công nghệ blockchain - để giảm thiểu thủ tục. Cụ thể, hệ thống sẽ là nơi tiếp tiếp nhận chìa khóa an toàn của người cho thuê nhà và tiền của người đi thuê nhà. Nếu thời hạn giao nhận chìa khóa và tiền không trùng khớp thì hợp đồng sẽ không được thực thi. Hiện nay, các luật sư có thể chưa lo lắng vì hợp đồng thông minh vẫn còn là một khái niệm mới lạ, nhưng điều này có thể thay đổi sớm, đặc biệt là khi các tiểu bang như Arizona của Hoa Kỳ thông qua luật xác nhận hợp đồng thông minh là hợp lệ.

Ngành quản trị nhân lực

Trong lĩnh vực này, quản lý thông tin chính là chìa khóa để thành công. Tính xác thực của thông tin nguồn nhân lực đã trở thành yếu tố quan trọng ảnh hưởng đến chi phí và hiệu quả của việc quản lý nguồn nhân lực. Với sự phát triển nhanh chóng của các thiết bị di động và công nghệ Internet, các rủi ro nhân lực khác nhau gây ra bởi sự sai sót thông tin mang lại thiệt hại kinh tế đối với các doanh nghiệp. Dựa vào nghiên cứu của Blockchain, một số mô hình đã được đưa ra nhằm mục đích kết hợp công nghệ mã hoá truyền thống với công nghệ Internet để thiết lập một mô hình quản lý thông tin nhân sự, góp phần làm giảm chi phí quản lý thông tin cho các doanh nghiệp [5].

Kết luận chương

Chương 1 đã cho thấy công nghệ blockchain được xây dựng dựa trên hai kỹ thuật chính là hàm băm và chữ ký số, giúp cho dữ liệu được đảm bảo tính an toàn cao. Với các tính chất đặc trưng của mình, những tác động có thể gây ảnh hưởng của công nghệ blockchain đối với các ngành công nghiệp khác nhau là rất đáng chú ý. Blockchain là công nghệ hứa hẹn một vai trò to lớn đối với các ứng dụng thực tế và rất nhiều thứ khác, và điều này chỉ mới bắt đầu!

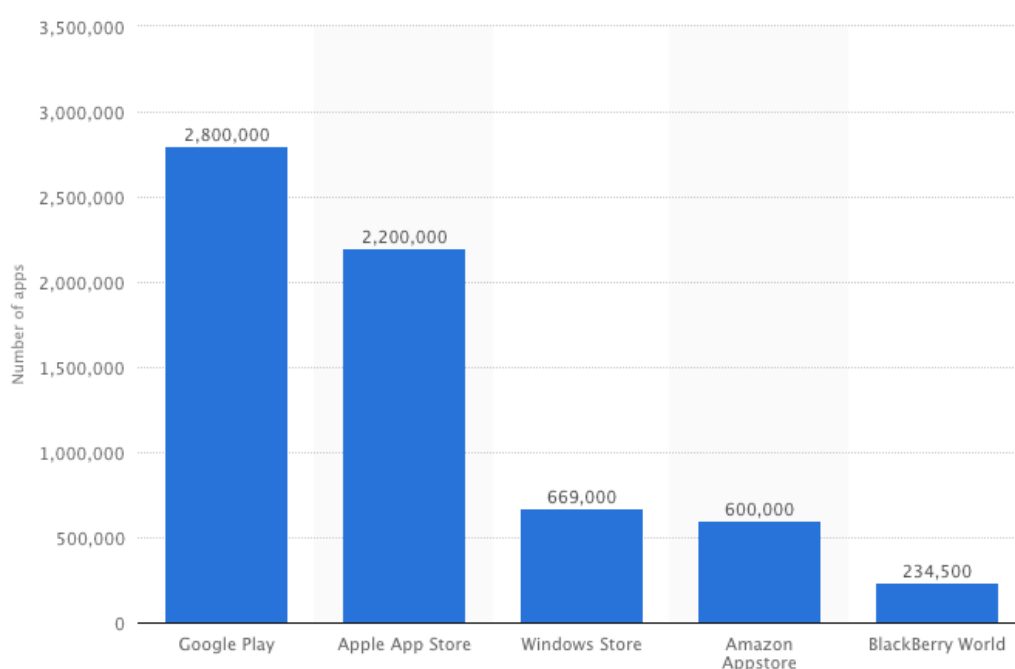
Chương 2. THANH TOÁN DI ĐỘNG VÀ TIỀN SỐ

2.1 Thanh toán di động

2.1.1 Giới thiệu

Thanh toán di động là dịch vụ thanh toán thông qua các thiết bị di động như điện thoại, máy tính bảng hay các thiết bị di động các nhân khác tại bất cứ đâu, bất cứ khi nào một cách nhanh chóng mà không cần giao dịch trực tiếp tiền mặt hay séc. Đây là một trong những dịch vụ hiện đại với khả năng tương tác nhanh, đã và đang được đầu tư phát triển trong bối cảnh hiện nay.

Cùng với sự phát triển của các thiết bị di động, các kho ứng dụng (platform phân phối content) dành cho các thiết bị này cũng phát triển một cách nhanh chóng trong đó không thể không kể đến AppStore và Google Play Store. Kho ứng dụng là nơi người viết ứng dụng tải ứng dụng lên và người dùng thiết bị di động có thể tải về các ứng dụng cho thiết bị của mình. Có nhiều điều khoản mà các bên sử dụng kho ứng dụng cần tuân theo, trong đó có điều khoản về độc quyền thanh toán. Trong khi thanh toán di động là một dịch vụ với khả năng tương tác nhanh và được đầu tư phát triển, các kho ứng dụng đã thay đổi chính sách độc quyền thanh toán dịch vụ content qua hệ thống thanh toán của họ. Cách thức gắn thanh toán của Apple và Google sẽ được trình bày trong mục 2.1.2 và 2.1.3.



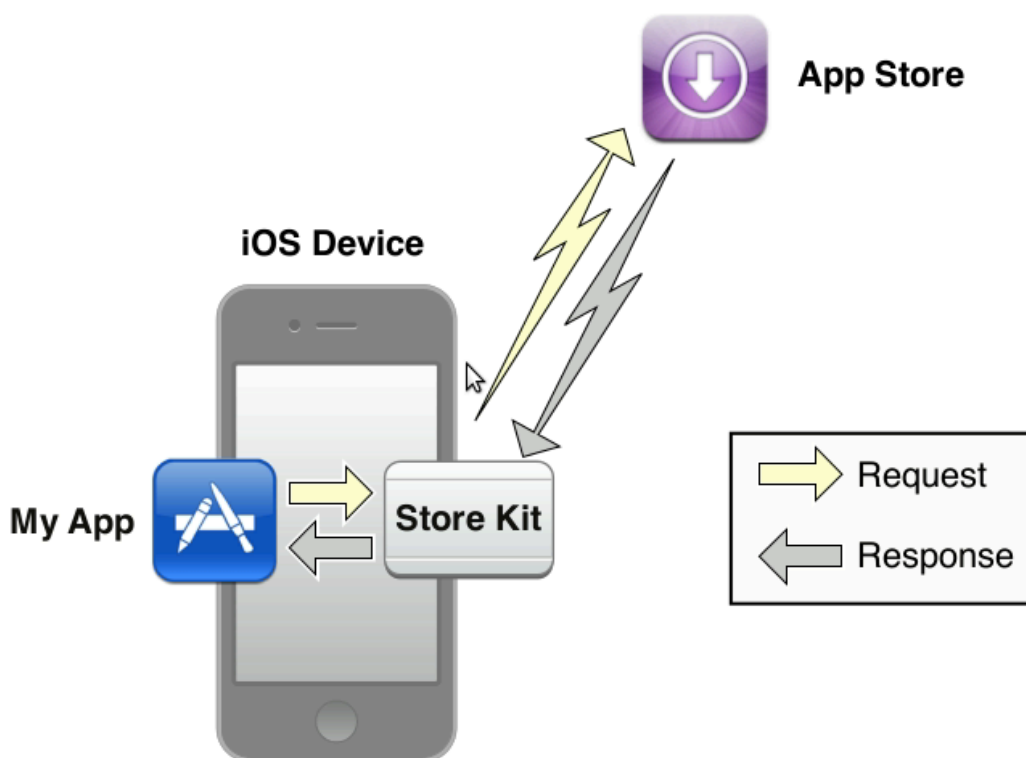
Hình 2.1: Số lượng ứng dụng trên các kho ứng dụng (tháng 3/2017)

Việc áp đặt thanh toán bằng Visa và Master Card cũng có nhiều kẽ hở bị kẻ gian lợi dụng để trục lợi, gây ảnh hưởng đến doanh thu của các doanh nghiệp kinh doanh nội dung số. Cụ thể, khách hàng sau khi thanh toán trên kho ứng dụng để chơi game, khi vừa thanh toán xong họ có thể yêu cầu hoàn trả lại tiền (refund) thì ngay lập tức sẽ được Google trả lại tiền. Như vậy, cả nhà phát hành và Google đều không thu được tiền. Thời hạn một giao dịch mua content trong ứng dụng có thể yêu cầu hoàn trả lại tiền của Apple là 90 ngày, của Google là 180 ngày.

Theo ông Bảo, giám đốc công ty VTC Mobile, số lượng giao dịch bằng thẻ thanh toán quốc tế bị hoàn về chiếm bình quân tới 70%, có ứng dụng lên tới 90%. Hầu như nhà phát hành không có doanh thu, trong khi phải chi phí rất nhiều tiền để phát triển game cũng như chi phí quảng cáo. [13]

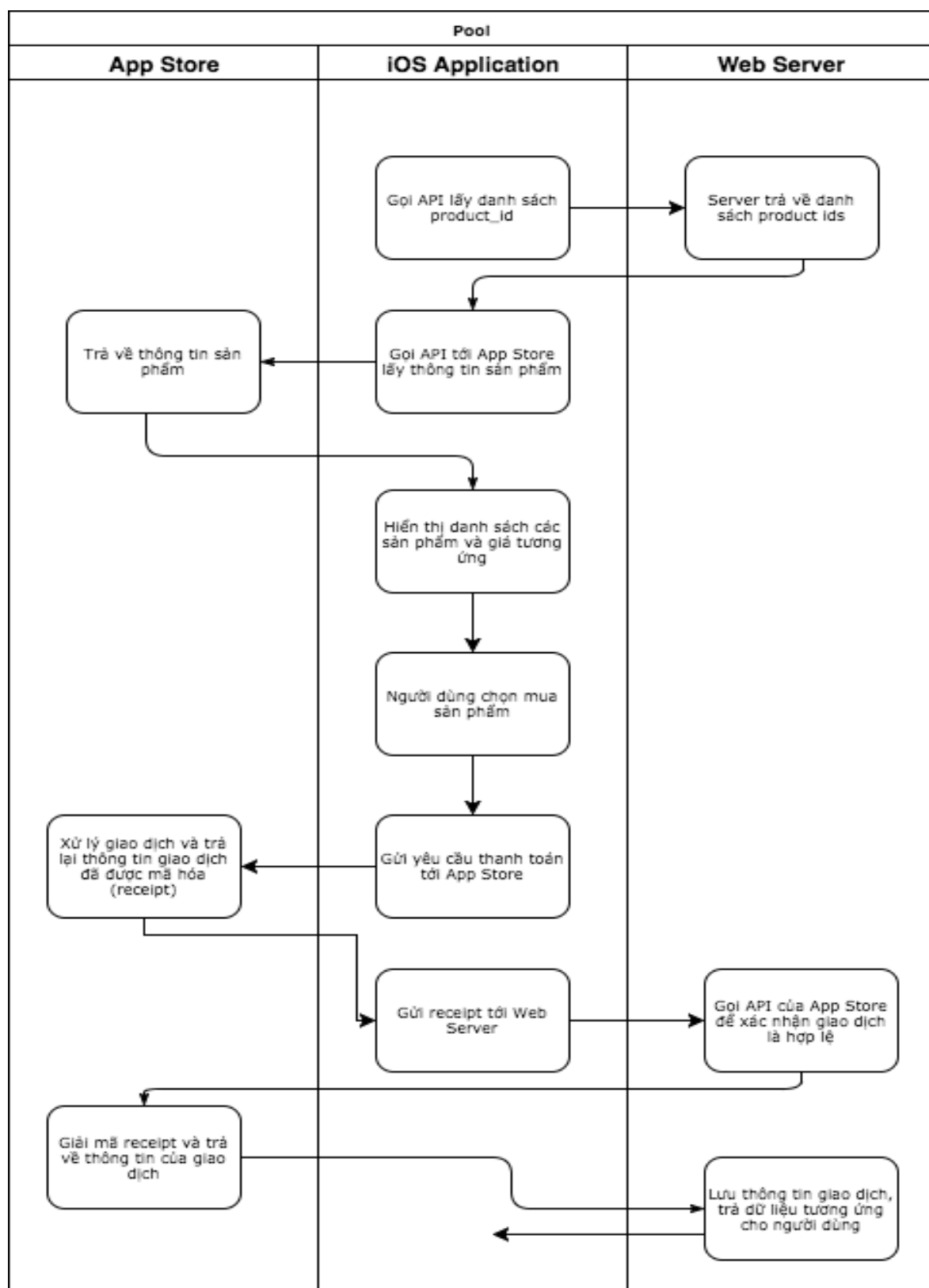
Để ngăn chặn kẻ gian trục lợi, một số nhà phát hành Game đã buộc phải ra chính sách để game thủ không thể thanh toán được bằng thẻ quốc tế, hoặc khi thấy khách hàng thanh toán bằng thẻ nhiều tiền quá thì sẽ từ chối giao dịch. Tuy nhiên làm vậy sẽ bị Store hạ xuống với lý do từ chối phục vụ khách hàng.

2.1.2 Thanh toán trên Apple Store



Hình 2.2: Luồng thanh toán của Apple

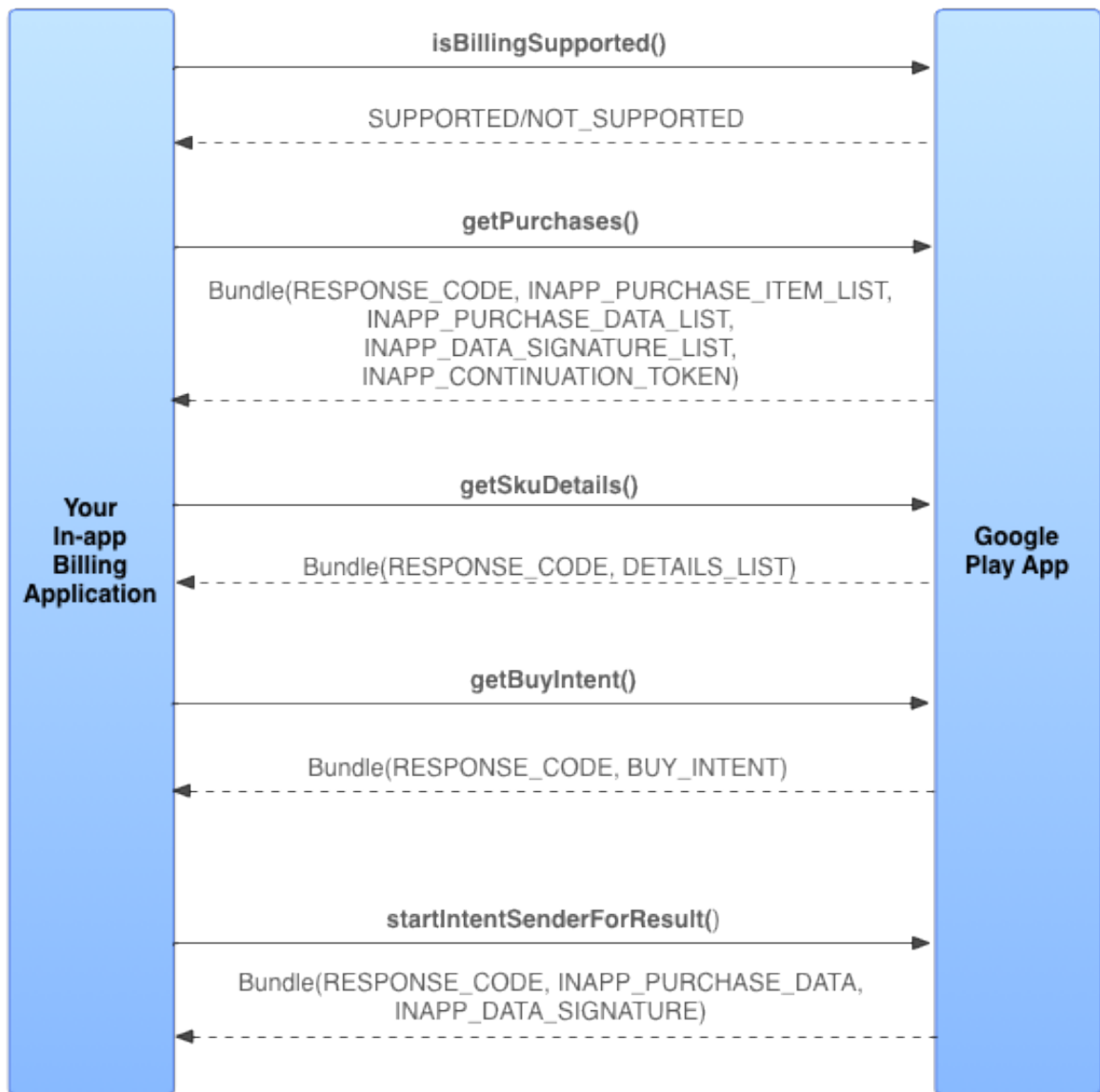
Apple cung cấp bộ thư viện StoreKit để hỗ trợ việc thanh toán giữa Server Apple và ứng dụng của lập trình viên. Luồng thanh toán của Apple được chia thành hai mô hình để triển khai: Mô hình thanh toán không có máy chủ web và mô hình thanh toán có máy chủ web. Với các ứng dụng game, thông thường áp dụng theo mô hình có máy chủ web (web server). Apple yêu cầu tất cả các Game nếu có thực hiện mua bán nội dung bên trong phải gắn thanh toán qua cổng thanh toán của Apple, doanh thu sẽ chia theo tỉ lệ nhà phát hành 70% - Apple 30%. 30% là một con số khá lớn, lớn hơn rất nhiều so với các kênh thanh toán bằng thẻ nạp như thẻ Viettel, Vinaphone,...



Hình 2.3: Mô hình thanh toán có máy chủ web

Theo hình 2.3, sau khi giao dịch kết thúc, web server thực hiện nghiệp vụ và trả nội dung mà người dùng đã mua vào ứng dụng. Nếu sau bước này người dùng yêu cầu hoàn trả tiền, khi đó web server không có cách nào để lấy lại nội dung đã cấp cho người dùng.

2.1.3 Thanh toán trên Google Play



Hình 2.4: Luồng thanh toán của Google

Hình 2.4 mô tả luồng thanh toán của các ứng dụng trên Google Play Store không có máy chủ web. Với các giao dịch có máy chủ web, một bước nữa được thêm vào luồng trên: sau khi nhận được “INAPP_PURCHASE_DATA” từ Google Play App, ứng dụng gửi thông tin này kèm theo một số thông tin khác liên quan đến tài khoản vừa thực hiện thanh toán lên máy chủ web, máy chủ web tiến hành xác thực thông tin dựa vào “INAPP_PURCHASE_DATA” và tiến hành xử lý nghiệp vụ đối với người dùng vừa thanh toán thành công.

2.2 Tiền số

2.2.1 Giới thiệu

Cũng giống như tiền giấy truyền thống, tiền số là một loại tiền tệ thể hiện tài sản của người chủ sở hữu, cho phép giao dịch và chuyển giao quyền sở hữu không giới hạn. Loại tiền tệ này cũng có thể được sử dụng để mua hàng hóa, dịch vụ trong một cộng đồng nhất định. Điểm đặc biệt của tiền số là nó không tồn tại dưới dạng vật chất mà được lưu trữ trên mạng máy tính.

Bitcoin và blockchains có một số đặc điểm hứa hẹn làm chúng trở thành công nghệ tốt để xử lý các khoản thanh toán. Thứ nhất, chúng được dựa trên một mạng ngang hàng (P2P) để thực hiện lưu trữ và thực hiện các giao dịch. Tính chất phi tập trung của bitcoins dựa vào blockchain cho phép nó hỗ trợ các giao dịch tự trị. Lợi thế khác là rất dễ dàng tạo tài khoản mới - mỗi thiết bị có thể dễ dàng có tài khoản riêng, một tài khoản mới có thể được tạo ra trong vài giây. Vì vậy, không có bên thứ ba nào kiểm soát các tài khoản và các tài khoản không trực tiếp liên kết với bất kỳ cá nhân nào [8].

Chúng ta cần phân biệt giữa tiền ảo và tiền số. Tiền ảo là tiền không có giá trị thực, không được bảo lãnh bởi các tài sản có giá trị như tiền mặt, vàng,.... Tiền ảo thường được sử dụng trong các ứng dụng như trò chơi điện tử, chúng có thể sử dụng ở trong trò chơi nhưng không thể đem ra ngoài để mua các sản phẩm và dịch vụ khác [14]. Một số doanh nghiệp phát hành trò chơi điện tử tại Việt Nam như Garena sử dụng tiền ảo là “sò”, Gamota sử dụng tiền ảo là “Gxu”, “vàng”, “KNB”, Tiền số là loại tiền được sinh ra bởi các thuật toán mã hóa phức tạp. Khác với tiền ảo, tiền số có giá trị thực và được trao đổi thông qua các thiết bị có kết nối internet mà không thông qua tổ chức trung gian hay quốc gia nào. [14]

Hiện tại trên thế giới có rất nhiều loại tiền số khác nhau, hầu hết đều sử dụng công nghệ blockchain đã trình bày trong chương 1. Đi đầu trong các loại tiền số đó là Bitcoin (BTC), ngoài ra còn nhiều đồng tiền số khác có giá trị cao được thị trường chấp nhận như một loại tiền tệ thanh toán như Ethereum (ETH), Litecoin (LTC),...

Tiền số đảm bảo được 3 yếu tố sau:

- Được nhiều người chấp nhận và được sử dụng để thanh toán, trao đổi hàng hóa, dịch vụ.
- Có thể chuyển đổi sang các loại tiền tệ khác một cách nhanh chóng.
- Việc phát hành cũng tuân theo một số quy tắc nhằm đảm bảo không gây ra lạm phát làm giảm giá trị của đồng tiền.

Ta có thể thấy tiền số cũng là một loại tiền tệ. Việc sở hữu những đồng tiền số cũng coi như sở hữu một khối tài sản. Tiền số là xu thế tất yếu trong quá trình tiến hóa của tiền tệ cũng như khoa học công nghệ.

2.2.2 Mô hình tiền số Bitcoin

Bitcoin là một loại tiền số sử dụng như một cuốn sổ cái phân quyền, sử dụng công nghệ blockchain để theo dõi tất cả các giao dịch đã thực hiện và tất cả các khoản tiền hiện có của mỗi tài khoản. Bitcoin được giới thiệu vào năm 2008 với biệt danh Satoshi Nakamoto. Tổng quan về dự án Bitcoin được giới thiệu tại trang web của dự án [4]. Bitcoin là một cuộc cách mạng lớn khi bài toán giao dịch được giải quyết mà không có sự kiểm soát từ bất cứ ai, không ai có thể thay đổi thuật toán cũng như phương thức vận hành.

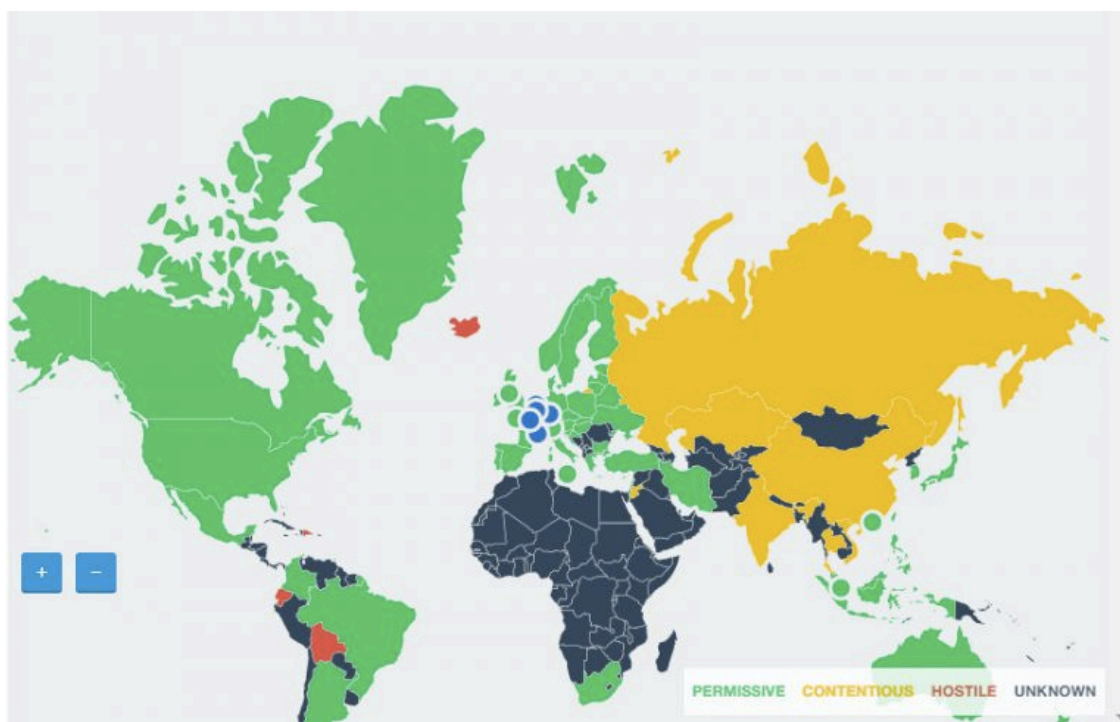
Bitcoin có những ưu điểm đáng kể sau:

- Thuận tiện trong giao dịch: giao dịch của BTC được thực hiện theo giao thức P2P, tiền được gửi trực tiếp từ người gửi đến người nhận mà không thông qua bên thứ ba nên giao dịch được thực hiện nhanh chóng và thuận tiện.
- An toàn và bảo mật: Mỗi giao dịch đều được thực hiện và ẩn danh người gửi và người nhận.
- Không thể bị làm giả: BTC không hiện hữu dưới dạng vật chất nên không thể bị làm giả.
- Chi phí giao dịch thấp: Mỗi giao dịch chỉ mất phí xử lý giao dịch, không mất một khoản phí trung gian nào.
- Bảo vệ môi trường: Hệ thống máy tính xử lý bitcoin tốn ít tài nguyên hơn nhiều so với hệ thống tài chính in tiền truyền thống.
- Tiềm năng thương mại điện tử: Mọi giao dịch của BTC không thể bị hoàn trả, có thể giải quyết được vấn đề người sử dụng dịch vụ yêu cầu hoàn tiền đã trình bày trong mục 2.1.1.

Bên cạnh các lợi ích của mình, BTC cũng có những hạn chế riêng:

- Khó sử dụng: Để sử dụng BTC, người dùng phải thành thạo sử dụng các thiết bị như máy tính, điện thoại. Đối với một người ít tiếp xúc với công nghệ sẽ không thể sử dụng đồng tiền này.
- Tội phạm rửa tiền lộng hành: Với đặc trưng ẩn danh của mình, cả người gửi và người nhận BTC đều không bị phát hiện, tội phạm rửa tiền có thể sử dụng đồng tiền này như một phương pháp giao dịch.

Trên thế giới có nhiều quốc gia đã chấp nhận và ủng hộ đồng tiền BTC, tuy nhiên một số nơi vẫn không chấp nhận đồng tiền này.



Hình 2.5: Biểu đồ chấp nhận BTC trên thế giới

Để hiểu rõ cách thức hoạt động của đồng tiền số, chúng ta hãy cùng tìm hiểu chi tiết về BTC. Ta cần làm rõ ba vấn đề:

- Bitcoin được sinh ra như thế nào?
- BTC được lưu trữ như thế nào?
- Cách một giao dịch BTC được thực hiện.

1. Cách tạo ra Bitcoin

Trong hệ thống tiền tệ truyền thống, tiền được in ra bằng vật chất. BTC là một đồng tiền số, hoạt động của nó dựa trên một mạng lưới các máy tính, mỗi máy tính trong mạng được gọi là một nút (node) của mạng đó. Mỗi nút thực hiện việc “đào” BTC bằng cách thực hiện tính toán. Mỗi nút còn có tên gọi khác là “thợ mỏ”, vì sao lại gọi như vậy ta sẽ cùng tìm hiểu cách hoạt động của mạng bitcoin.

Các giao dịch bitcoins được thực hiện mọi lúc, mọi nơi thông qua mạng bitcoin, không ai có thể theo dõi được giao dịch đó được gửi từ ai và gửi cho ai. Mạng bitcoin đảm bảo vấn đề này bằng cách tập hợp tất cả các giao dịch trong một khoảng thời gian nhất định vào một danh sách, sau đó công việc của các nút trong mạng là giải bài toán PoW [6] để tìm ra block mới và cập nhật vào blockchain.

Sổ cái là một blockchain (đã giới thiệu trong Chương 1), có thể dùng để tra cứu bất kỳ giao dịch nào của bất kỳ địa chỉ bitcoin nào, tại bất cứ thời điểm nào trên mạng. Bất cứ khi nào một block được tạo ra sẽ được thêm vào blockchain, tạo ra một danh sách ngày càng tăng của các giao dịch đã từng thực hiện trên mạng bitcoin. Mỗi nút trong mạng luôn có một bản sao được cập nhật liên tục các block để đảm bảo các nút có thể thực hiện tính toán một cách chính xác, đảm bảo sổ cái được tin tưởng và blockchain không thể bị giả mạo.

Khi danh sách các giao dịch được tập hợp lại, các nút bắt đầu thực hiện xử lý, tìm ra block thỏa mãn điều kiện của blockchain. Cụ thể là tìm ra hàm băm thỏa mãn điều kiện của blockchain. Công việc này được gọi là “proof of work” [6] được trình bày trong mục 1.3.3. Giá trị băm được tính toán dựa trên thông tin về các giao dịch, thời gian, giá trị băm của block trước đó được lưu trong blockchain. Với việc giá trị băm sử dụng cả giá trị băm của block trước đó, blockchain đảm bảo dữ liệu của một block khó có thể bị thay đổi, vì nếu một block bị thay đổi thông tin thì tất cả các block sau nó sẽ bị thay đổi giá trị băm, dẫn tới các block đó được đánh giá là không hợp lệ.

Trên đây là cách một nút trong mạng bitcoin hoạt động, các nút sử dụng phần mềm được phát hành bởi tổ chức/cá nhân đã phát hành bitcoin, và cạnh tranh với nhau để thực hiện công việc này. Bất cứ khi nào một block được một nút tìm ra, nút đó sẽ nhận được một phần thưởng là một lượng bitcoin cụ thể (12.5 BTC ở thời điểm 09/2017) và phí giao dịch của các giao dịch nằm trong block đó. Hình 2.6 là thông tin chi tiết về một block trong mạng bitcoin. Việc tìm giá trị băm của một tập dữ liệu là rất đơn giản, tuy nhiên mạng bitcoin đã áp dụng bằng chứng công việc để làm việc này khó khăn hơn giúp cho lượng BTC không thể bị khai thác hết trong một thời gian ngắn.

Để tìm ra một block, các nút trong mạng không được phép thay đổi thông tin các giao dịch, nhưng phải thay đổi dữ liệu để tìm ra một giá trị băm phù hợp. Điều này được thực hiện bằng cách sử dụng một dữ liệu ngẫu nhiên được gọi là “nonce” (đã được trình bày trong mục 1.3.1). Khi một giá trị băm không phù hợp, “nonce” được thay đổi và thực hiện lại quá trình băm. Điều này có thể mất nhiều thời gian và các nút trong mạng luôn cố gắng thực hiện, chỉ có nút tìm ra đầu tiên mới được hưởng phần thưởng bitcoin. Đó là cách các nút kiếm được bitcoins, và vì sao chúng lại được gọi là “thợ mỏ”.

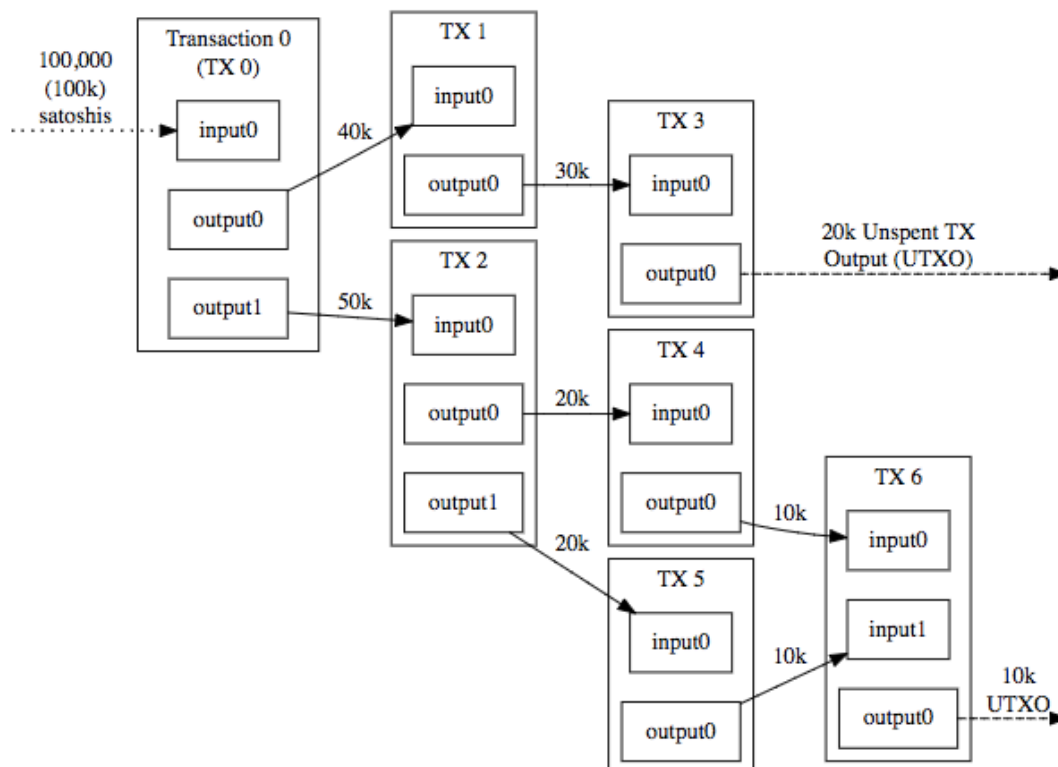
Block #488889

Summary		Hashes	
Number Of Transactions	789	Hash	0000000000000000021175e4362664b6f77210b96e642dd0f4e0f4af0105c87
Output Total	2,255.39824092 BTC	Previous Block	00000000000000000913a50c6a5c1b7f48ada4875b71fb937f48016e7517262
Estimated Transaction Volume	825.94814876 BTC	Next Block(s)	
Transaction Fees	0.09386862 BTC	Merkle Root	b88318e254b6b75b2f3d51428e88261e4326126def605ea51b0cef682acfe84
Height	488889 (Main Chain)		
Timestamp	2017-10-08 15:19:15		
Received Time	2017-10-08 15:19:15		
Relayed By	BW.COM		
Difficulty	1,123,863,285,132.97		
Bits	402717299		
Size	999.17 kB		
Weight	3996.32 kWU		
Version	0x20000000		
Nonce	3578296310		
Block Reward	12.5 BTC		



Hình 2.6: Thông tin một block trong mạng bitcoin
(nguồn: <https://blockchain.info>)

2. Cách lưu trữ Bitcoin



Hình 2.7: Mô hình giao dịch của Bitcoin

Trong mô hình tiền số Bitcoin, dữ liệu được lưu trong các giao dịch là các Input và Output, được liên kết với nhau như hình 2.7. Mỗi Input của một giao

dịch cần được tham chiếu bởi một Output của một giao dịch trước đó. Theo hình 2.8, mỗi Input gồm các thông tin:

- Previous tx: giá trị băm của giao dịch có chứa Output tham chiếu tới Input này
- Index: chỉ số của Output ở giao dịch trước đó
- ScriptSig: gồm hai thành phần, chữ ký của người thực hiện giao dịch và khóa công khai của người đó.

```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

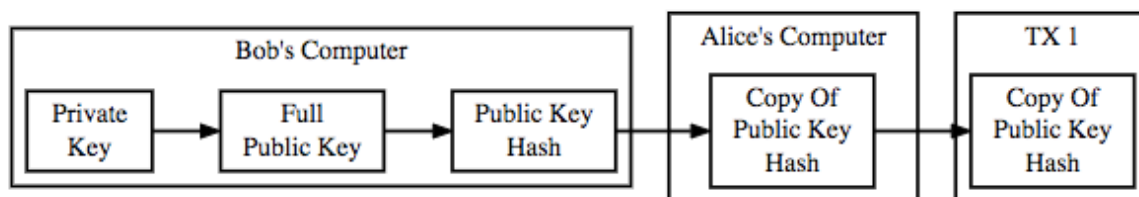
Hình 2.8: Dữ liệu trong một Transaction
(nguồn: <https://en.bitcoin.it/wiki/Transaction>)

Output được chia thành hai loại, đã được tiêu và chưa được tiêu (UTXO) [9]. Output gồm các thông tin:

- Value: Giá trị Satoshi gửi cho người nhận
- ScriptPubKey: Chứa thông tin về hàm băm, địa chỉ người nhận

Giá trị BTC của một địa chỉ ví không được lưu trữ bằng một giá trị cụ thể, mà được tính bằng tổng số BTC trong các Output chưa tiêu (UTXOs) [9] của địa chỉ ví đó. Tổng số BTC trong các UTXOs [9] luôn bằng tổng số BTC của mạng blockchain.

Khi A muốn gửi BTC cho B, A cần tạo ra các giao dịch với Input lấy từ tập các UTXOs [9] của A, và Output có địa chỉ nhận là địa chỉ ví của B. Khi các nút thực hiện xác thực giao dịch chính là kiểm tra chữ ký trong Input mà A đã tạo. Nếu giao dịch thành công, Output tham chiếu tới Input của giao dịch đó sẽ được cập nhật trạng thái đã tiêu, xóa khỏi tập UTXOs [9], và các Output mới được tạo ra sẽ được thêm vào tập UTXOs [9].



Hình 2.9: Tạo khóa để thực hiện giao dịch trong bitcoin

Mỗi người dùng bitcoin cần tạo một ví bitcoin để lưu trữ khóa bí mật để truy cập vào địa chỉ bitcoin để có thể thực hiện các giao dịch. Theo hình 2.9, khi Alice muốn gửi BTC cho Bob, Bob cần tạo ra cặp khóa gồm khóa bí mật và khóa công khai, bitcoin sử dụng thuật toán chữ ký số đường cong Elliptic (ECDSA) [10] để thực hiện ký các giao dịch. Địa chỉ ví của Bob chính là giá trị băm của khóa công khai được mã hóa base58, Alice gửi BTC vào địa chỉ ví của Bob bằng cách giải mã base58 để lấy giá trị băm khóa công khai của Bob, Alice tạo các Outputs của các giao dịch cho phép bất cứ ai cũng có thể tiêu các Output đó nếu chứng minh được họ có khóa bí mật của Bob. Quá trình giao dịch như trên được gọi là thanh toán qua giá trị băm khóa công khai (P2PKH – Pay to Public Key Hash).

Ví bitcoin có nhiều hình thức khác nhau, được thiết kế cho nhiều loại thiết bị khác nhau. Nếu không muốn lưu trữ trên máy tính, bạn có thể in ra giấy và lưu trữ như ví vật lý thông thường. Ví bitcoin có một số dạng chính như: máy tính, điện thoại di động, online, giấy và phần cứng.

- Máy tính: Bitcoin cung cấp phần mềm “Bitcoin Core” (<https://bitcoin.org/en/download>) cho phép người dùng cài đặt trên máy tính. Ngoài việc đóng vai trò như một nút trong mạng, phần mềm này cho phép chúng ta tạo ra một địa chỉ bitcoin để gửi và nhận bitcoin, lưu trữ khóa bí mật.
- Điện thoại di động: Với xu thế phát triển của các thiết bị di động và thanh toán online mọi lúc mọi nơi, ngay cả trên đường phố, ví được cài đặt trên điện thoại di động là rất cần thiết. Ví bitcoin cũng được cài đặt như các phần mềm khác trên thiết bị di động của bạn, cho phép lưu trữ các khóa và thực hiện thanh toán trực tiếp bằng điện thoại.

Ví trên điện thoại di động có một điểm chung là không thể lưu trữ đầy đủ bản sao của blockchain, nó chỉ lưu trữ một tập con rất nhỏ và dựa vào các nút đáng tin cậy trong mạng bitcoin để đảm bảo rằng các giao dịch được thực hiện chính xác.

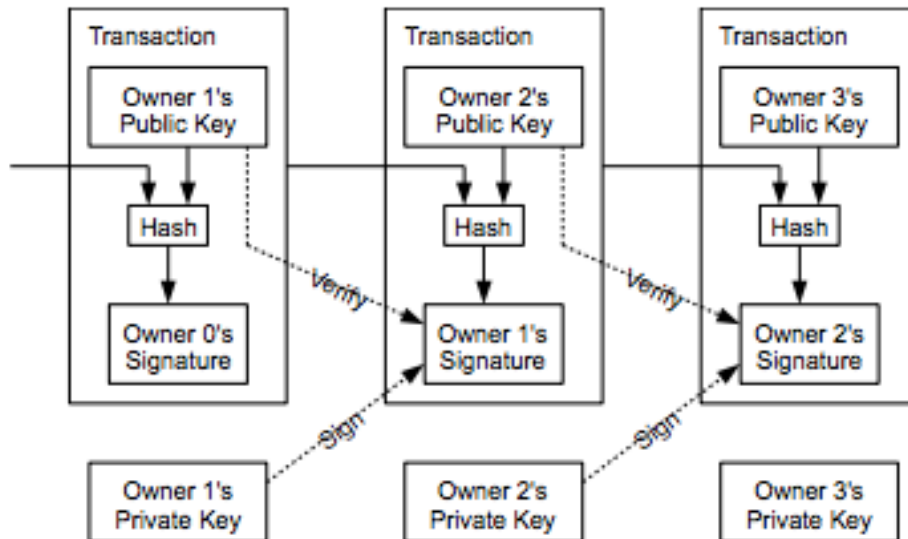
- Online: Ví online được thực hiện thông qua website, bạn có thể đăng ký tài khoản thông qua một trang web, khóa bí mật và địa chỉ ví của bạn sẽ được lưu trữ trên máy tính sở hữu bởi một người khác. Có một bất lợi lớn khi bạn sử dụng ví hình thức này, website mà bạn tin tưởng đang nắm giữ khóa bí mật của bạn và có thể thực hiện giao dịch, cũng như nắm giữ toàn bộ số bitcoin của bạn.
- Một số website uy tín đang được nhiều người sử dụng như:
 - ✓ Coinbase: <https://www.coinbase.com>
 - ✓ Circle: <https://www.circle.com>
 - ✓ Blockchain: <https://blockchain.info>
 - ✓ Xapo: <https://xapo.com>
- Ví giấy: Ví giấy là một lựa chọn phổ biến để lưu trữ bitcoin, một số trang web cung cấp dịch vụ in ví giấy. Trên ví sẽ chứa hai thông tin, một là địa chỉ bitcoin để nhận bitcoin, hai là khóa bí mật sử dụng để sử dụng bitcoins được lưu trữ tại địa chỉ đó.
- Phần cứng: Ví phần cứng hiện nay rất hạn chế về số lượng, chúng là các thiết bị chuyên dụng dùng để lưu trữ khóa bí mật và tạo thuận lợi cho việc thanh toán.

3. Cách thực hiện giao dịch Bitcoin

Các giao dịch bitcoin được gửi và nhận thông qua các địa chỉ ví bitcoin. Các nút trong mạng đều biết về các giao dịch, có thể tra cứu lịch sử của các giao dịch cũng như của các ví bitcoin.

Như ta đã biết, bitcoin không được lưu trữ ở bất kỳ đâu, chỉ có lịch sử các giao dịch được ghi lại. Không giống như một tài khoản ngân hàng có một giá trị tiền cụ thể, bitcoin không tồn tại trên bất kỳ thiết bị phần cứng hay phần mềm nào, thay vào đó, các giao dịch bitcoin được ghi lại, đó chính là thông tin tăng hay giảm số dư tại một địa chỉ ví bitcoin. Blockchain của bitcoin lưu trữ toàn bộ các giao dịch, nếu muốn tìm giá trị bitcoin của ví ta chỉ cần tra cứu lại các giao dịch của địa chỉ ví đó trong blockchain.

Hình 2.8 là một ví dụ về giao dịch BTC với 1 Input và 1 Output. Trong ví dụ trên, giao dịch chuyển 50 BTC từ Output #0 (index của Output) trong giao dịch có giá trị băm “f5d8e...” cho địa chỉ ví “4043...”. Output sinh ra được gọi là UTXO (unspent transaction output) [9]. Bất kỳ ai cũng có thể chi tiêu UTXO [9] này nếu chứng minh được họ có khóa bí mật có thể tạo ra Input mới chứa scriptSig đáp ứng điều kiện trong scriptPubKey của UTXO [9] đó.



Hình 2.10: Danh sách các giao dịch trong một block [2]

Quy trình thực hiện một giao dịch bitcoins:

- Giao dịch được thông báo cho các nút trong mạng.
- Các nút tập hợp các giao dịch mới và thực hiện PoW [6] tạo một block.
- Khi một block được tìm ra, nó được thông báo cho tất cả các nút trong mạng.
- Các nút khác tiến hành xác thực các giao dịch trong block đó, và chỉ chấp nhận block đó khi tất cả các giao dịch là hợp lệ.
- Các nút sau khi chấp nhận block sẽ thêm nó vào blockchain, và sử dụng giá trị băm của block đó là 1 tham số để tìm giá trị băm của block tiếp theo.

Các giao dịch bitcoins cũng có thể mất một khoản phí, phí giao dịch được tính dựa trên nhiều yếu tố. Các nút trong mạng thực hiện tính toán và nhận được phần thưởng bitcoin, vì thế phí giao dịch hiện tại có thể ở mức thấp. Khi phần thưởng bitcoin không còn nhiều, có thể mức phí giao dịch sẽ tăng lên để đảm bảo các nút trong mạng hoạt động mà không bị thua lỗ.

Để xác thực một giao dịch, một nút không cần duyệt toàn bộ blockchain. Mỗi nút trong mạng lưu một bản sao của blockchain, và mỗi block đều lưu trữ thời gian tạo, khi cần xác thực một giao dịch, nút đó sẽ tiến hành xác thực chữ ký trong các Input của giao dịch có hợp lệ với các Output tham chiếu tới Input đó. Nếu toàn bộ các Input có chữ ký hợp lệ thì giao dịch là hợp lệ.

Trên đây là mô hình hoạt động chính của bitcoin, giúp chúng ta hiểu được khái quát cách thức mạng bitcoin lưu trữ giao dịch và thực hiện các giao dịch

đảm bảo độ tin cậy và tránh được bài toán tiêu một đồng tiền nhiều lần (double spending).

2.2.3 Độ an toàn của tiền số

Với cách thức thực hiện giao dịch được trình bày trong mục 2.2.2, khi An muốn gửi tiền cho Bình, An tạo ra giao dịch có Output chứa thông tin khóa công khai của Bình. Output này sẽ có trạng thái là chưa tiêu (UTXO), và bất cứ có khóa bí mật của Bình đều có thể thực hiện chi tiêu Output này, nói cách khác, bất cứ ai có thể tạo ra giao dịch mới có Input được tham chiếu từ UTXO của Bình đều có thể tiêu tiền của Bình. Vậy độ an toàn của tiền số phụ thuộc vào chữ ký số mà đồng tiền đó sử dụng.

Để đánh giá độ an toàn của một đồng tiền số, ta cần đánh giá thuật toán ký số mà đồng tiền đó sử dụng, cụ thể là đánh giá về tốc độ ký, độ dài của khóa và khả năng phá khóa. Đồng tiền số Bitcoin và TYM (sẽ trình bày trong chương 3) sử dụng thuật toán ký số ECDSA, thuật toán này đã được kiểm chứng thực tế với cùng kích thước khóa, tốc độ ký của ECDSA nhanh hơn nhiều lần so với RSA (hình 2.11). Khả năng phá khóa của thuật toán ECDSA là việc giải bài toán logarit rời rạc, khó hơn nhiều so với bài toán tách số đơn thuần của RSA.

	sign/s
256 bit ecdsa (nistp256)	9516.8
rsa 2048 bits	1001.8

(openssl 1.0.2 beta on x86_64 with enable-ec_nistp_64_gcc_128)








Hình 2.11: So sánh tốc độ ký của ECDSA và RSA

(nguồn: <https://blog.cloudflare.com>)

2.2.4 Tiềm năng phát triển của tiền số

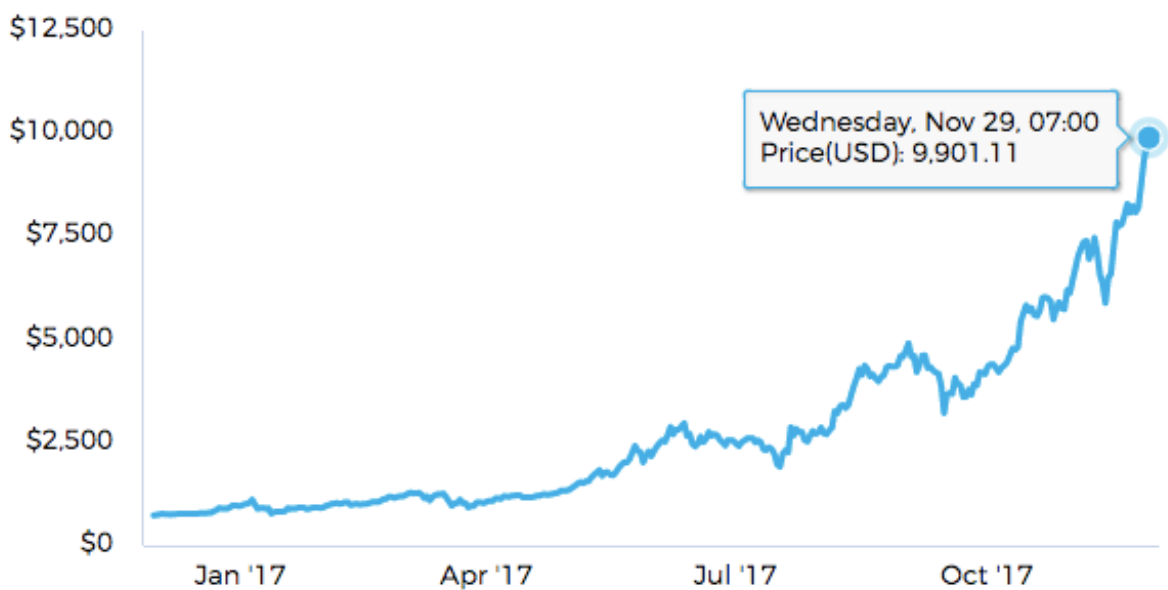
Cũng giống như tiền giấy, tiền số cũng là một đơn vị tiền tệ và người sở hữu tiền số cũng là sở hữu một khối tài sản có giá trị nhất định. Ngoài ra tiền số có nhiều ưu điểm vượt trội hơn tiền giấy, tiền số giúp người sử dụng thanh toán dễ dàng và thuận tiện, không phải mang theo tiền trong ví như tiền giấy. Tiền số cũng đảm bảo được tính an toàn và bảo mật cao nhờ việc ứng dụng công nghệ blockchain và chữ ký số trong việc thực hiện các giao dịch.

Hiện nay, trên thế giới có rất nhiều đồng tiền số đã ra đời và được nhiều tổ chức, doanh nghiệp chấp nhận thanh toán. Nhiều lĩnh vực về kinh tế cũng như khoa học công nghệ đã chấp nhận thanh toán bằng đồng Bitcoin, Ethereum,..., nổi bật trong số đó là các công ty lớn như Microsoft, Reddit, WordPress.com,....

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)
1	 Bitcoin	\$173,993,206,750	\$10,414.00	\$6,974,580,000	16,707,625 BTC	6.65%
2	 Ethereum	\$47,080,642,737	\$490.33	\$1,512,690,000	96,017,887 ETH	2.18%
3	 Bitcoin Cash	\$25,251,796,139	\$1,500.61	\$1,270,900,000	16,827,688 BCH	-6.53%
4	 Ripple	\$11,178,115,286	\$0.289417	\$630,669,000	38,622,870,411 XRP *	7.83%
5	 Litecoin	\$5,447,731,233	\$100.80	\$530,327,000	54,042,808 LTC	10.00%
6	 Bitcoin Gold	\$5,197,000,359	\$311.62	\$107,787,000	16,677,311 BTG	-12.02%
7	 Dash	\$5,105,259,723	\$661.59	\$166,445,000	7,716,699 DASH	5.20%

Hình 2.12: Giá trị vốn hóa trên thị trường của một số đồng tiền điện tử (11/2017)

Hình 2.12 cho thấy giá trị vốn hóa của các đồng tiền điện tử hiện nay là rất lớn, riêng đồng tiền Bitcoin khoảng 174 tỷ USD. Các đồng tiền điện tử hiện vẫn đang có xu hướng tăng trưởng mạnh mẽ. Trong tương lai, tiền điện tử hứa hẹn sẽ còn phát triển như một giải pháp mới cho vấn đề về tài chính và tiền tệ.



Hình 2.13: Tăng trưởng của đồng tiền số Bitcoin (BTC)



Hình 2.14: Tăng trưởng của đồng tiền số Ethereum (ETH)

Kết luận chương

Chương 2 đã trình bày chi tiết về mô hình thanh toán trên các ứng dụng di động sử dụng nền tảng của App Store và Google Play Store và các vấn đề mà các nhà phát hành nội dung số đang gặp phải. Đồng thời chương này cũng trình bày về mô hình hoạt động của đồng tiền số Bitcoin - ứng dụng đầu tiên của Blockchain. Phần tiếp theo luận văn sẽ trình bày về cách xây dựng một hệ thống Blockchain và giải pháp sử dụng tiền số để thanh toán cho các ứng dụng di động. Dựa vào các phân tích ở chương 2, chương tiếp theo sẽ trình bày cụ thể về phương pháp cài đặt một blockchain và kết quả thực nghiệm thu được.

Chương 3. ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN TRONG THANH TOÁN DI ĐỘNG

3.1 Đặt vấn đề

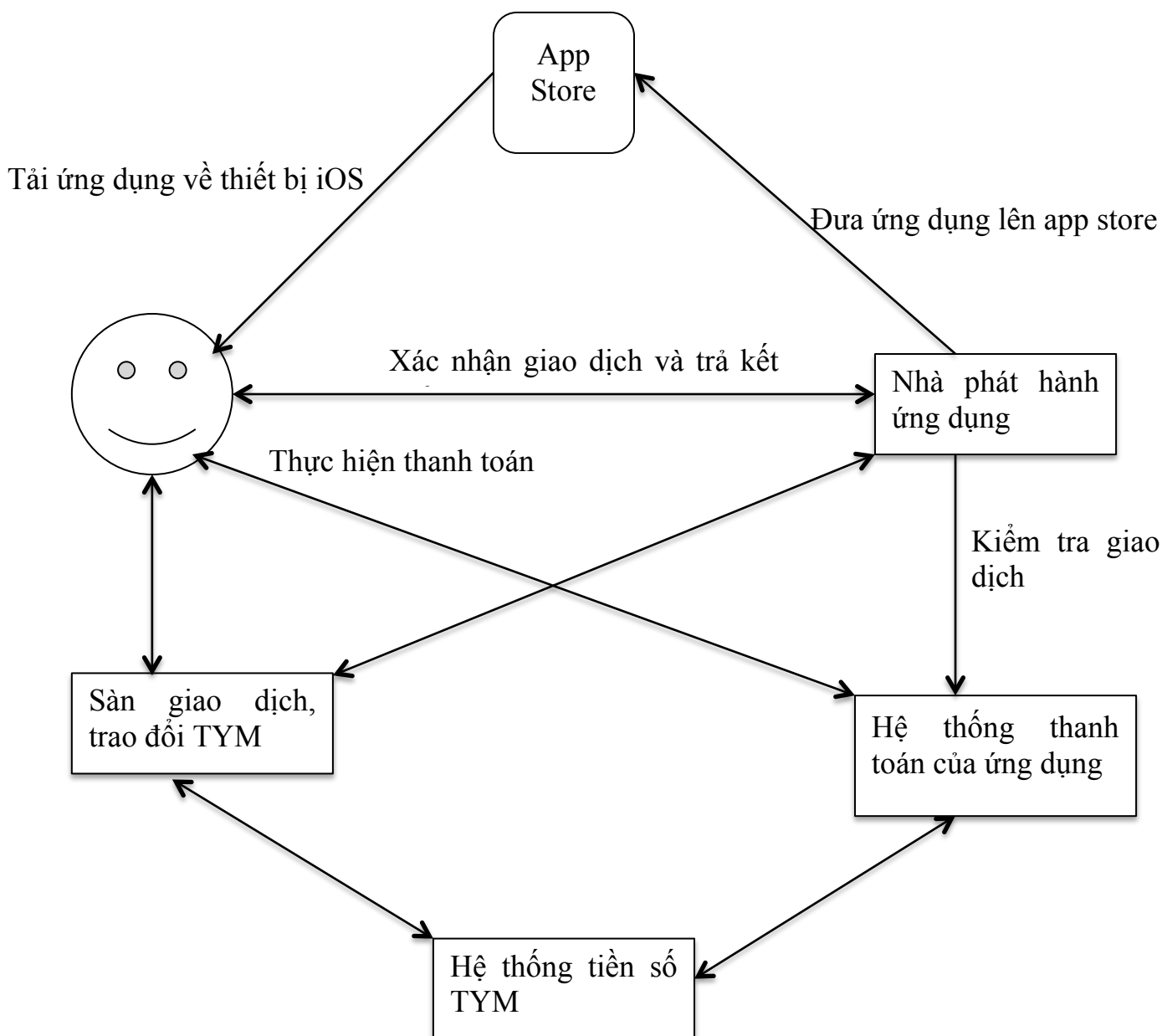
3.1.1 Bài toán đặt ra

Như đã trình bày trong chương 2, các phương thức thanh toán hiện tại theo chính sách của Apple và Google rất bất lợi cho các doanh nghiệp kinh doanh nội dung số. Một ứng dụng sau khi hoàn thành sẽ được đẩy lên các nền tảng phát hành ứng dụng, sau đó người dùng sẽ sử dụng phần mềm được cài đặt sẵn trên máy để lên các kho ứng dụng này tải về máy và tiến hành cài đặt. Thông thường, mỗi giao dịch sẽ bị Apple hay Google trừ một khoản phí 30% số tiền người dùng thanh toán. Không chỉ có vậy, người làm ứng dụng có thể bị thua lỗ do chính sách hoàn tiền của nền tảng phát hành, người dùng được phép yêu cầu hoàn tiền sau khi thanh toán, việc này khiến cho nhà phát hành ứng dụng không thu được tiền từ người dùng và cũng không thể lấy lại nội dung số đã cấp cho người dùng.

Với thực trạng trên, để đảm bảo tính công bằng cho cả nhà phát hành và người sử dụng ứng dụng, luận văn đề xuất xây dựng một hệ thống tiền số để thực hiện thanh toán cho các ứng dụng di động. Mục tiêu của luận văn là xây dựng một hệ thống tiền số TYM, hỗ trợ việc thanh toán trong các ứng dụng theo giao thức P2P, giúp quá trình thanh toán được thực hiện nhanh chóng và an toàn, tiền được chuyển trực tiếp từ người sử dụng đến ví của nhà phát hành mà không phải thông qua bên trung gian khác, giúp giảm thiểu rủi ro và chi phí cho nhà phát hành ứng dụng.

3.1.2 Cách tiếp cận và giải pháp

Luận văn đã xây dựng một đồng tiền số TYM, và ứng dụng đồng tiền số này vào quá trình thanh toán của ứng dụng mua bán sách điện tử được mô tả như hình 3.1. Tiền số TYM được thiết kế ứng dụng công nghệ blockchain, giúp đảm bảo tính an toàn của các giao dịch và của đồng tiền.



Hình 3.1: Mô hình giải pháp ứng dụng tiền số trong thanh toán di động

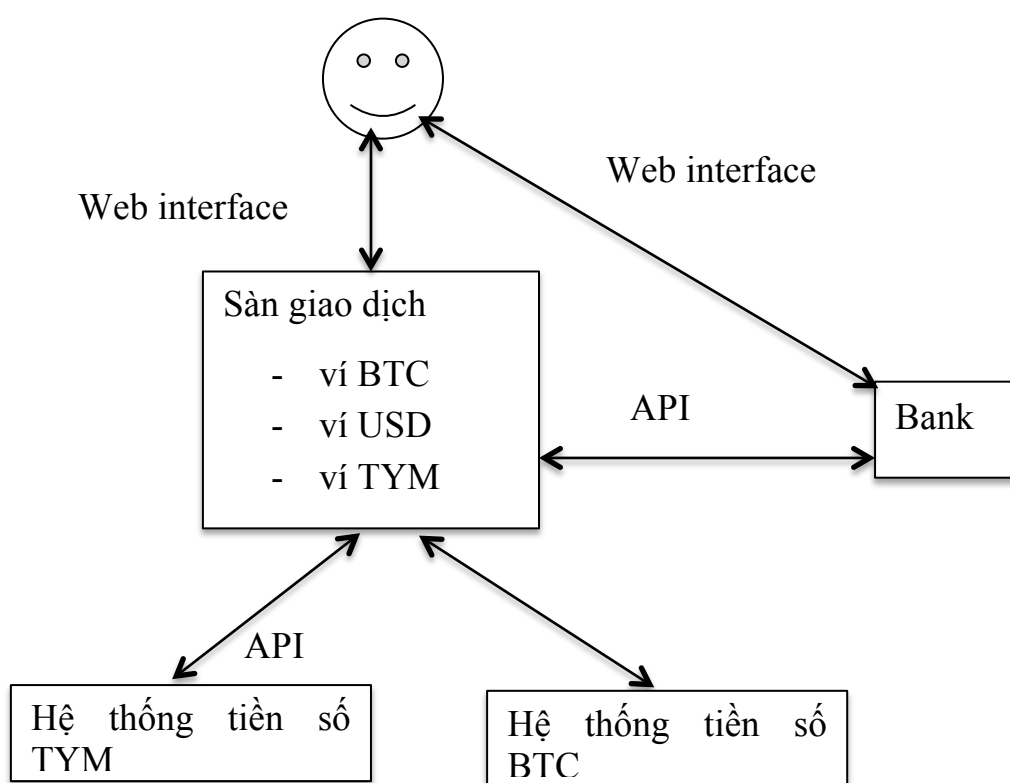
Ứng dụng mua bán sách điện tử gồm các bước sau:

- 1) Nhà phát hành đưa ứng dụng lên App Store.
- 2) Người dùng tải ứng dụng về từ App Store.
- 3) Khi muốn mua sách điện tử, người dùng thanh toán trực tiếp TYM vào ví của nhà phát hành ứng dụng thông qua hệ thống thanh toán. Giao thức thanh toán P2P giúp cho nhà phát hành có thể nhận tiền ngay sau đó.
- 4) Người dùng sau khi thanh toán, yêu cầu nhà phát hành kiểm tra thông tin giao dịch và trả về sách điện tử mà người dùng đã mua.

5) Nhà phát hành cần gọi sang hệ thống thanh toán để kiểm tra giao dịch là hợp lệ và trả về dữ liệu tương ứng cho người dùng.

Để có được tiền số TYM, người dùng cần thực hiện giao dịch mua bán, trao đổi (exchange) thông qua một sàn giao dịch TYM. Nhà phát hành sau khi bán được sách cho người dùng cũng có thể lên sàn giao dịch này để thực hiện mua bán, chuyển đổi sang các đơn vị tiền tệ khác như USD, BTC, ETH,...

Hiện nay các đồng tiền số được thực hiện mua bán, trao đổi thông qua các sàn giao dịch uy tín như Remitano (remitano.com), LiveCoin (livecoin.net), Bittrex (bittrex.com),... Mô hình thao tác để mua được TYM được mô tả như hình 3.2.



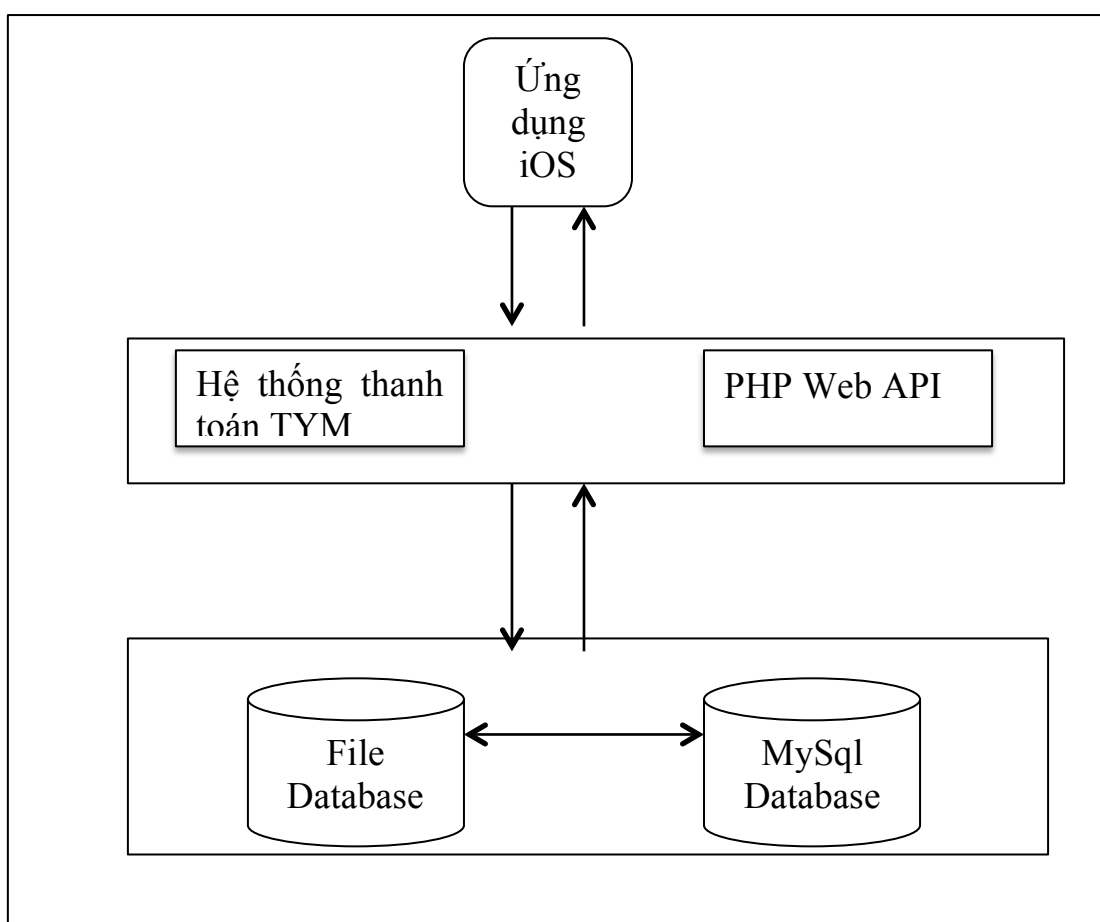
Hình 3.2: Mô hình sàn giao dịch mua bán tiền số

Người dùng khi đăng ký tài khoản trên các sàn giao dịch sẽ có các địa chỉ ví của đồng tiền mà sàn giao dịch đó hỗ trợ. Các lệnh mua và bán được thực hiện với người dùng khác trên sàn giao dịch đó. Người dùng có thể rút tiền từ ví USD về tài khoản ngân hàng, cũng như nạp tiền từ tài khoản ngân hàng vào ví USD. Người dùng có thể sử dụng ví USD hoặc bất kỳ một đồng tiền số nào đó để mua một đồng tiền số khác. Các sàn giao dịch cũng cho phép người dùng chuyển trực tiếp một đồng tiền số tới một địa chỉ ví khác của đồng tiền số đó, ví dụ TYM có thể được chuyển trực tiếp sang một ví TYM khác.

Sau đây luận văn sẽ trình bày cách xây dựng một hệ thống tiền số dựa trên công nghệ blockchain, và viết một ứng dụng mua bán sách điện tử sử dụng đồng tiền số TYM trên thiết bị iOS. Hệ thống được triển khai theo mô hình trong hình 3.1. Kèm theo việc phát triển của điện thoại di động, việc sử dụng các đồng tiền số để thực hiện giao dịch trong các ứng dụng là điều tất yếu.

3.2 Xây dựng hệ thống tiền số và ứng dụng mua bán sách điện tử

3.2.1 Kiến trúc hệ thống



Hình 3.3: Kiến trúc tổng quan của hệ thống

Hệ thống được xây dựng dựa trên ba thành phần chính

- Ứng dụng iOS: Hiển thị giao diện, cho phép người dùng mua bán sách điện tử.
- PHP Web API: Cung cấp các API thực hiện các chức năng đặc trưng của ứng dụng như đăng nhập, đăng xuất, lấy danh sách các sách đang bán, sách đã mua,...
- Hệ thống tiền số TYM: Lưu trữ các giao dịch, cung cấp các API để ứng dụng iOS có thể thực hiện giao dịch và kiểm tra giao dịch.

Tương tự như các đồng tiền số hiện tại, hệ thống sẽ lưu trữ dữ liệu của Blockchain vào file database nhằm mục đích dễ dàng triển khai trên nhiều nút. Các nút khi cài đặt cần lưu trữ dữ liệu vào file, giúp cho hệ thống dễ dàng cài đặt và triển khai trên nhiều thiết bị khác nhau.

Cơ sở dữ liệu MySQL được dùng để lưu trữ thông tin của người dùng, thông tin sách, và các dữ liệu khác đặc thù của ứng dụng.

Dữ liệu trong các API của hệ thống được trả về dưới định dạng JSON. Trong phạm vi của luận văn, việc cài đặt hệ thống tiền số TYM sử dụng công nghệ blockchain sẽ được trình bày chi tiết, cách cài đặt Web API cũng như ứng dụng iOS sẽ không được mô tả cụ thể.

3.2.2 Đặc tả chức năng

Hệ thống tiền số TYM cung cấp API với các chức năng sau:

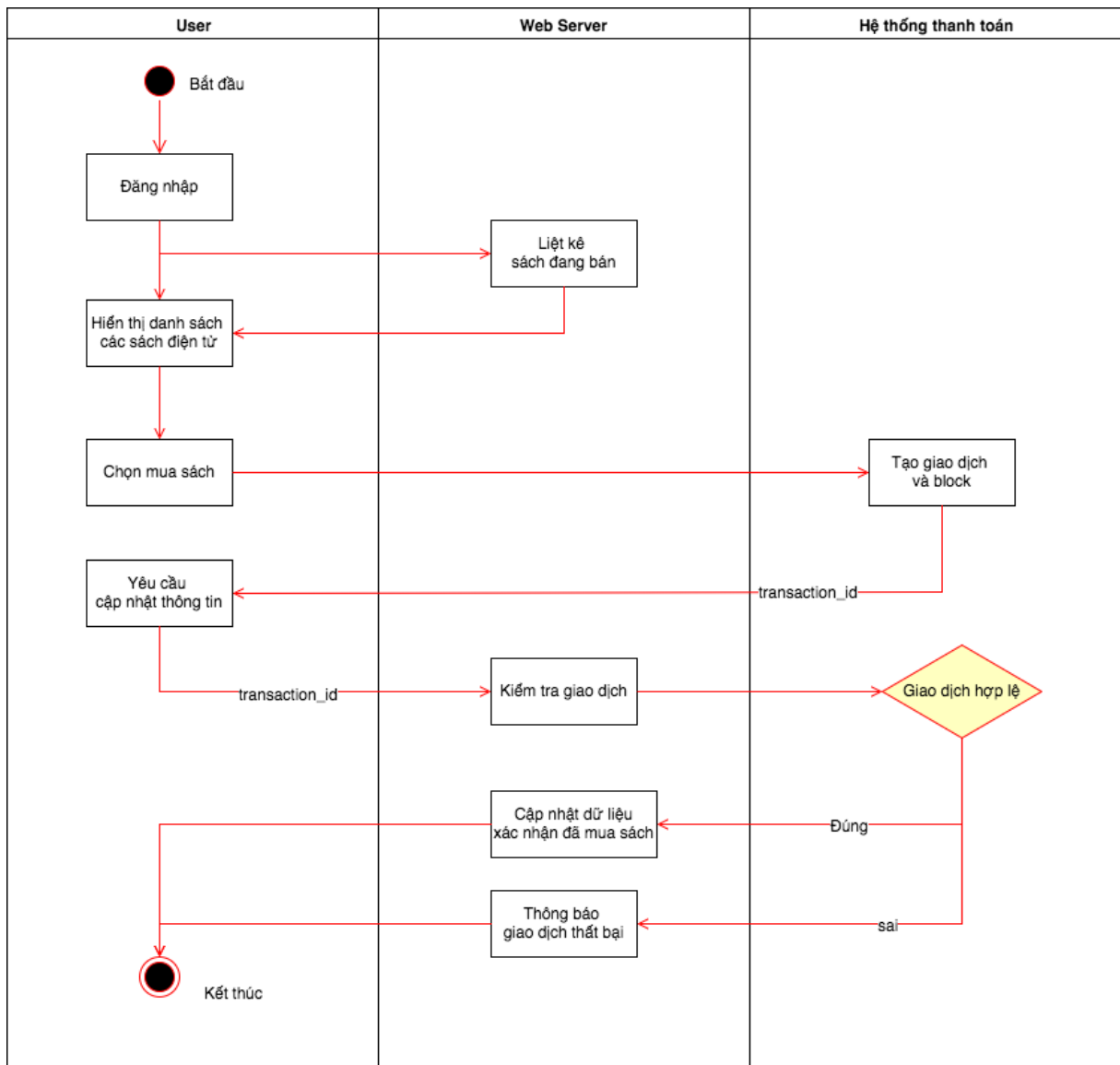
- API thực hiện giao dịch chuyển tiền từ ví A sang ví B.
- API thực hiện kiểm tra giao dịch có hợp lệ hay không.
- API kiểm tra giá trị TYM có thể chi tiêu của ví (balance).
- API hiển thị toàn bộ các block trong Blockchain.

Các API này được mô tả chi tiết trong bảng 3.1.

Các chức năng của ứng dụng mua sách điện tử:

- Người bán chính là nhà phát hành ứng dụng, người bán sử dụng một hệ thống giao diện web để thao tác với cơ sở dữ liệu, thêm hoặc xóa sách, chỉnh sửa nội dung sách.
- Người mua sau khi đăng nhập vào ứng dụng, ứng dụng sẽ thực hiện gọi một số API cần thiết của PHP Web API để thực hiện lấy danh sách các sách điện tử đang bán, các sách bán chạy, sách nổi bật,...
- Người dùng chọn mua sách, sau khi xác nhận hệ thống sẽ kiểm tra xem số dư trong ví có đủ hay không, nếu đủ số dư sẽ gọi tới API của hệ thống thanh toán để thực hiện giao dịch, API sẽ trả về mã giao dịch.
- Ứng dụng iOS dùng mã giao dịch nhận được gọi PHP Web API để thực hiện cập nhật thông tin giao dịch đã thanh toán.
- PHP Web API gọi API của hệ thống thanh toán để xác nhận lại giao dịch, và tiến hành cập nhật cơ sở dữ liệu, lưu trạng thái của người dùng đã mua cuốn sách mà người dùng chọn.

Các bước thực hiện được mô tả chi tiết như hình 3.4.



Hình 3.4: Biểu đồ luồng của hệ thống

3.2.3 Cài đặt hệ thống tiền số TYM

Như đã phân tích về công nghệ blockchain trong chương 1 và đồng tiền số Bitcoin trong chương 2, để xây dựng được một hệ thống tiền số ta cần cài đặt 3 chức năng chính là: tạo giao dịch, tạo block và thêm block vào blockchain hiện tại. Ba chức năng này sẽ được thực thi bởi các hàm CreateTransaction, NewBlock và AddBlock. Hàm tạo giao dịch được mô tả trong hình 3.5.

Mô tả hàm CreateTransaction:

INPUT:

- pubKey: Khóa công khai của người gửi
- privKey: Khóa bí mật của người gửi
- dest: Địa chỉ ví người nhận
- amount: Giá trị TYM cần gửi

- data: Dữ liệu người gửi đính kèm

OUTPUT: Giao dịch chứa các Inputs, Outputs cần được ghi vào block.

```

1 func (bc *Blockchain) CreateTransaction(pubKey, privKey, dest string, amount int, data string) Transaction {
2     source := ComputeHashForString(pubKey)
3     var tx Transaction
4     utxos := bc.Utxos[source] //list all utxo of source wallet
5     var outputs []Output
6     var inputs []Input
7     total := 0
8     for _, output := range(utxos){
9         if total < amount{
10            total += output.Value
11            input := CreateInput(output, pubKey, privKey)
12            inputs = append(inputs, input)
13        } else{
14            break
15        }
16    }
17    //not enough balance
18    if total < amount{
19        return tx
20    }
21    output := CreateOutput(index, amount, dest)
22    outputs = append(outputs, output)
23
24    //Create input to redeem
25    if total > amount{
26        output := CreateOutput(len(outputs) + 1, total - amount, source)
27        outputs = append(outputs, output)
28    }
29    tx.Version = bc.Version
30    tx.Type = "payment"
31    tx.OutputCount = len(outputs)
32    tx.Inputs = inputs
33    tx.InputCount = len(inputs)
34    tx.Hash = computeHashTransaction(tx)
35    tx.Outputs = outputs
36    tx.Data = data
37    for i, _ := range tx.Outputs{
38        tx.Outputs[i].TransactionHash = tx.Hash
39    }
40    return tx
41 }

```

Hình 3.5: Tạo một giao dịch trong mạng blockchain

Mỗi giao dịch gồm các Inputs và Outputs, Inputs được tham chiếu từ tập UTXO [9] của địa chỉ ví hiện tại (các Output của các giao dịch trước đó). Sau khi các giao dịch được tạo, chương trình cần thực hiện tạo ra các block. Hàm tạo block được mô tả như hình 3.7. Mỗi block hợp lệ cần giải được bài toán PoW [6], hàm giải bài toán này được mô tả như hình 3.6.

```

1 func (bc *Blockchain) ProofOfWork(block Block) (int64, string) {
2     var nonce int64 = 0
3     hash := computeHashForBlock(block)
4     for !bc.ValidHash(hash) {
5         nonce += 1
6         block.Nonce = nonce
7         hash = computeHashForBlock(block)
8     }
9     return nonce, hash
10 }
11

```

Hình 3.6: Hàm giải bài toán PoW [6]

Hàm NewBlock có nhiệm vụ tập hợp các giao dịch đang ở trạng thái chờ vào một Block, giải bài toán PoW để tìm ra giá trị băm thỏa mãn điều kiện của đồng tiền số TYM. Đồng thời giao dịch tạo Output chứa phần thưởng cho nút hiện tại cũng được thêm vào trong Block này. Mô tả hàm NewBlock như sau:

INPUT:

- previousHash: Giá trị băm của block mới nhất của Blockchain

OUTPUT: Block tập hợp các giao dịch đang cần thực hiện, và có giá trị băm thỏa mãn điều kiện của Blockchain.

```
1 func (bc *Blockchain) NewBlock(previousHash string) Block {
2     var outputs []Output
3     var inputs []Input
4     // Reward transaction
5     output := CreateOutput(0, bc.Limit_reward, bc.PubKeyHash)
6     outputs = append(outputs, output)
7     tx := Transaction{
8         Type: "coinbase",
9         Version: bc.Version,
10        InputCount: len(inputs),
11        Inputs: inputs,
12        OutputCount: len(outputs),
13        Outputs: outputs,
14    }
15    tx.Hash = computeHashTransaction(tx)
16    for i, _ := range tx.Outputs{
17        tx.Outputs[i].TransactionHash = tx.Hash
18    }
19    bc.Transactions = append(bc.Transactions, tx)
20    newBlock := Block{
21        Index: int64(len(bc.Chain) + 1),
22        Timestamp: time.Now().UnixNano(),
23        Transactions: bc.Transactions,
24        PreviousHash: previousHash,
25    }
26    nonce, hash := bc.ProofOfWork(newBlock) // PoW to find block hash match conditions
27    newBlock.Nonce = nonce
28    newBlock.Hash = hash
29
30    bc.Transactions = nil
31    return newBlock
32 }
```

Hình 3.7: Tạo một block mới

Sau khi một block được tạo ra, block sẽ được gửi tới các nút khác trong mạng và các nút khác thực hiện một hàm cực kỳ quan trọng là xác nhận tất các các giao dịch trong block là hợp lệ trước khi thêm block đó vào blockchain hiện tại. Hàm này cũng thực hiện cập nhật tập dữ liệu UTXOs của các giao dịch trong block. Hàm thêm mới một block được mô tả như hình 3.8. Mô tả hàm AddBlock như sau:

INPUT:

- block: Block cần được thêm vào Blockchain.

OUTPUT: bool

- true nếu Block được thêm thành công.
- false nếu có lỗi xảy ra.

```

1 func (bc *Blockchain) AddBlock(block Block) bool {
2     for _, tx := range block.Transactions{
3         if !bc.VerifyTransaction(tx){ //verify all inputs is valid
4             return false
5         }
6     }
7     bc.Chain = append(bc.Chain, block)
8     // After add new block to chain, update outputs data
9     for _, tx := range block.Transactions{
10        // Add new outputs to utxos
11        for _, output := range tx.Outputs{
12            if bc.Utxos[output.ScriptPubKey] == nil{
13                var outputs []Output
14                bc.Utxos[output.ScriptPubKey] = outputs
15            }
16            bc.Utxos[output.ScriptPubKey] = append(bc.Utxos[output.ScriptPubKey], output)
17        }
18        // Make old outputs is spent
19        for _, input := range tx.Inputs{
20            if !bc.SpentOutput(input.PrevTransaction, input.Index){
21                bc.RollbackTx(tx)
22                return false
23            }
24        }
25    }
26    return true
27 }

```

Hình 3.8: Thêm block vào blockchain

```

1 func (bc *Blockchain) VerifyTransaction(tx Transaction) bool {
2     // Verify all inputs is valid
3     success := 0
4     for _, input := range tx.Inputs{
5         tx := bc.GetTxByHash(input.PrevTransaction)
6         for _, output := range tx.Outputs{
7             if output.Index == input.Index{
8                 // Check key sign
9                 s := strings.Split(input.ScriptSign, " ")
10                sign, pub := s[0], s[1]
11                if ComputeHashForString(pub) == output.ScriptPubKey{
12                    if ValidateSign(sign, pub, input.PrevTransaction){ // verify signature
13                        success += 1
14                    }else{
15                        return false
16                    }
17                }else{
18                    return false
19                }
20            }
21        }
22    }
23    if success == len(tx.Inputs){
24        return true
25    }
26    return false
27 }

```

Hình 3.9: Xác nhận một giao dịch là hợp lệ

Trong hàm xác thực giao dịch sẽ diễn ra quá trình kiểm tra chữ ký trong các Inputs của giao dịch đó. Chương trình đã sử dụng chữ ký số ECDSA [10] để thực hiện quá trình ký và kiểm tra chữ ký.

Với các hàm được cài đặt như trên, chương trình đã xây dựng được một blockchain đơn giản, đáp ứng được như cầu thanh toán của người dùng với các API phục vụ mua bán và kiểm tra giao dịch.

3.2.4 Xây dựng các API thao tác với hệ thống tiền số

Các thành phần trong hệ thống giao tiếp với nhau thông qua Restful HTTP API. Bảng dưới đây mô tả các chức năng của các API đã được xây dựng.

URI	Phương thức	Giá trị truyền vào	Ghi chú
/transactions/new	POST	“data”, “amount”, “public_key”, “private_key”, “dest”	Tạo giao dịch chuyển tiền số đến ví có địa chỉ là “dest”
/transactions/check	GET	“txid”	Kiểm tra giao dịch có mã giao dịch là “txid”
/wallet/balance	GET	“wallet”	Lấy số dư ví của địa chỉ “wallet”
/wallet/register	GET		Tạo một ví mới. Khi người dùng mới đăng ký tài khoản cần gọi API này.
/chain	GET		Lấy toàn bộ các block trong blockchain
/transactions/history	GET	“wallet”	Lấy lịch sử giao dịch của ví có địa chỉ là “wallet”

Bảng 3.1: Các API của hệ thống tiền số

3.3 Thực nghiệm và đánh giá

3.3.1 Môi trường phát triển và công cụ

1. Phần cứng

Hệ thống blockchain đã được triển khai trên máy tính có cấu hình như sau:

TT	Nội dung	Thông số kỹ thuật
1	CPU	1.4 GHz Intel Core i5
2	RAM	4 GB 1600 MHz DDR3
3	Hard Disk	256GB SSD
4	OS	MacOS 10.11

Bảng 3.2: Cấu hình phần cứng

2. Phần mềm

Phần mềm	Ghi chú
Hệ điều hành	
▪ MacOS 10.11	
Third party software	
▪ Golang	Cài đặt Blockchain
▪ Apache 2.4	Webserver cho module web
▪ Mysql	Lưu thông tin của module web
▪ PHP 5.6.19	Module web được viết bằng ngôn ngữ PHP

Bảng 3.3: Các phần mềm sử dụng tiến hành thực nghiệm

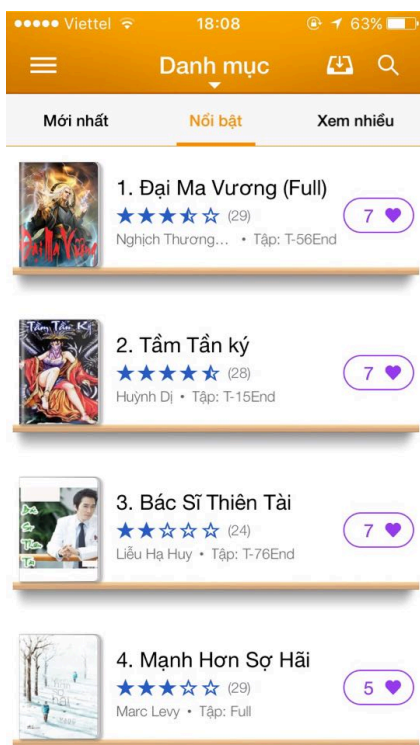
3.3.2 Kết quả thử nghiệm

Hệ thống tiền số TYM đã được triển khai và cài đặt trên server tại địa IP sau: <http://103.53.171.111:8002/chain>. Ứng dụng iOS đã được hoàn thành và chạy thử nghiệm trên điện thoại iPhone, sau khi thực hiện thanh toán đã thấy rõ được sự thay đổi của các block trong blockchain đã xây dựng. Quá trình thanh toán hoạt động tốt và giúp ta thấy được các thay đổi trong blockchain cũng như

cách hoạt động của toàn bộ quá trình tạo giao dịch, tạo block, ký và kiểm tra chữ ký.

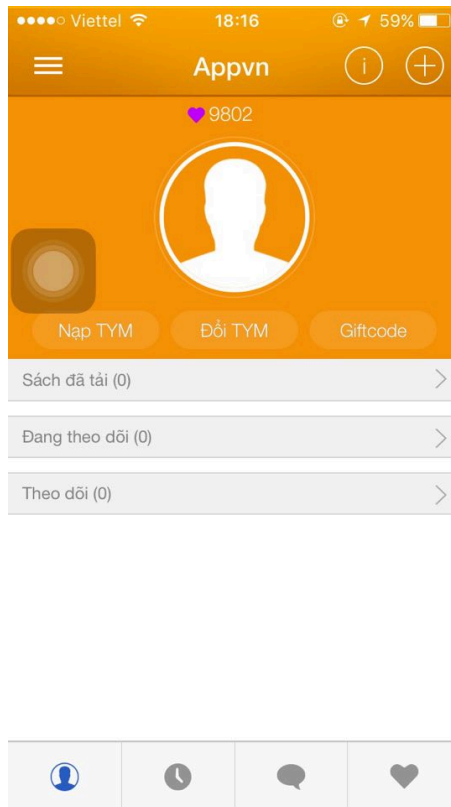
Dưới đây là một số màn hình của ứng dụng iOS đã xây dựng.

Khi mới truy cập ứng dụng, màn hình sẽ hiển thị danh sách các sản phẩm như hình 3.10.



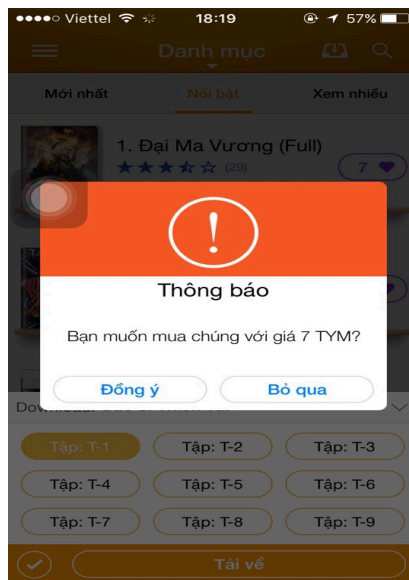
Hình 3.10: Danh sách các sách đang bán

Người dùng có thể kiểm tra số TYM trong ví khi truy cập vào phần thông tin cá nhân. Như hình 3.11, người dùng hiện đang có 9802 TYM.



Hình 3.11: Thông tin cá nhân của người dùng

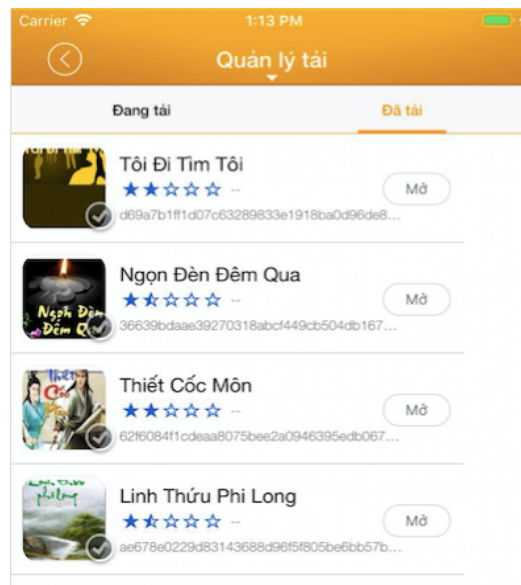
Khi chọn mua một cuốn sách tại danh sách các sách đang bán, người dùng sẽ được hỏi có xác nhận mua sách như hình 3.12.



Hình 3.12: Giao diện xác nhận thanh toán

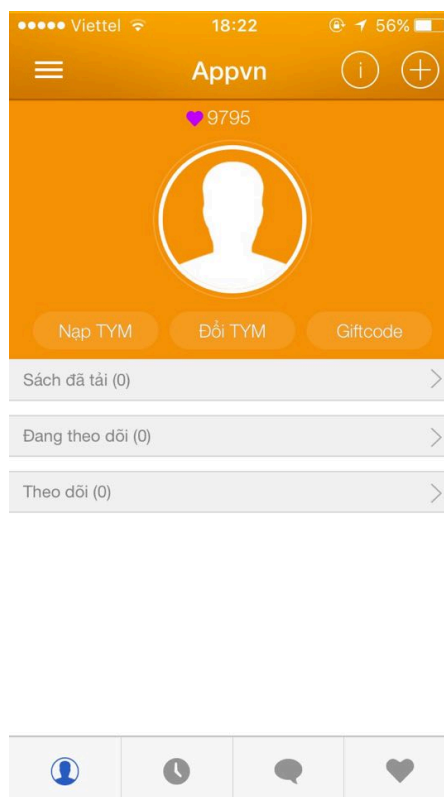
Sau khi xác nhận thanh toán, luồng xử lý được thực hiện như hình 3.3. Quá trình này hệ thống sẽ thực hiện chuyển TYM từ ví của người dùng sang ví của người bán sách, ở đây là nhà phát hành ứng dụng. Người dùng có thể quản lý

các sách đã tải trong mục “Quản lý tải” như hình 3.13. Sách đã tải về có thể mở bằng các ứng dụng hỗ trợ đọc tài liệu trên thiết bị di động.



Hình 3.13: Các sách đã tải về

Khi mua sách thành công, ví của người dùng sẽ bị trừ một khoản TYM tương ứng với giá trị sách mà người bán đưa ra. Hình 3.14 cho thấy giá trị TYM còn lại của người dùng là 9795 (9802 - 7).



Hình 3.14: Số TYM còn lại sau khi thanh toán

Kết quả JSON trả về khi gọi API thanh toán:

```

{
  "block": {
    "index": 2,
    "timestamp": 1511685026996539647,
    "transactions": [
      {
        "version": "0.0.1",
        "type": "payment",
        "input_count": 1,
        "inputs": [
          {
            "prev_transaction": "9bd27eb81367c78cbef88965ae0e8fda56af28ba2dda319e9267e7bb4911465a",
            "index": 1,
            "script_sign":
              "106865631779885298146535573792265026030778087550642636138589883242847008513711|2623006297710773391414136774557049122
              5246595770453229436188346382008294266375 MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEVTunb1bd
              +N18MiU0F8N6QeIb6JmWGUjpHqkG9Y0SGWhJ1P2pUJY9PRniURHJu+uxZhJSCCIuL/93Ijx8S7zzJA=="
          }
        ],
        "output_count": 2,
        "outputs": [
          {
            "index": 0,
            "value": 10,
            "status": "unspent",
            "script_pubkey": "d46149a39f70e0db835108c75e5270505a6454340f312167613ab67fe6ac0ba5",
            "transaction_hash": "9bd27eb81367c78cbef88965ae0e8fda56af28ba2dda319e9267e7bb4911465a"
          },
          {
            "index": 1,
            "value": 100,
            "status": "spent",
            "script_pubkey": "6b860b4ce97abfb1023c7ece8f1a5a1f0b268aee7ebf969fe5169ec36fe00a8",
            "transaction_hash": "9bd27eb81367c78cbef88965ae0e8fda56af28ba2dda319e9267e7bb4911465a"
          }
        ],
        "hash": "9bd27eb81367c78cbef88965ae0e8fda56af28ba2dda319e9267e7bb4911465a",
        "data": "custom data"
      }
    ],
    "nonce": 110627,
    "hash": "0000d309a0326e664ae895795f372e3a8e7337ee5b2bf1b7487f1d77ed0938ff",
    "previous_hash": "00005ca73360bad2b8d0b722891b3dd556b8918df590ad1dd98918e0400f94ee"
  },
  "error_code": 0,
  "message": "New Block added"
}

```

Hình 3.15: Dữ liệu trả về của hệ thống tiền số khi giao dịch thành công

```

{
  "chain": [
    {
      "index": 1,
      "timestamp": 1511685019137719579,
      "transactions": [
        {
          "version": "0.0.1",
          "type": "coinbase",
          "input_count": 0,
          "inputs": null,
          "output_count": 2,
          "outputs": [
            {
              "index": 0,
              "value": 10,
              "status": "unspent",
              "script_pubkey": "d46149a39f70e0db835108c75e5270505a6454340f312167613ab67fe6ac0ba5",
              "transaction_hash": "9bd27eb81367c78cbef88965ae0e8fda56af28ba2dda319e9267e7bb4911465a"
            },
            {
              "index": 1,
              "value": 100,
              "status": "spent",
              "script_pubkey": "6b860b4ce97abfb1023c7ece8f1a5a1f0b268aee7ebf969fe5169ec36fe00a8",
              "transaction_hash": "9bd27eb81367c78cbef88965ae0e8fda56af28ba2dda319e9267e7bb4911465a"
            }
          ],
          "hash": "9bd27eb81367c78cbef88965ae0e8fda56af28ba2dda319e9267e7bb4911465a",
          "data": ""
        }
      ],
      "nonce": 46409,
      "hash": "00005ca73360bad2b8d0b722891b3dd556b8918df590ad1dd98918e0400f94ee",
      "previous_hash": "0000"
    }
  ],
  "length": 2
}

```

Hình 3.16: Hình ảnh blockchain sau khi block mới được thêm vào

3.3.3 Đánh giá kết quả

Với mục tiêu bài toán đã đưa ra, hệ thống tiền số hoạt động theo giao thức P2P đã giải quyết được vấn đề thanh toán di động hiện tại. Thay vì người làm ứng dụng phải chờ 2 tháng mới nhận được khoản tiền thanh toán của người dùng

từ nền tảng phát hành ứng dụng là App Store hay Google Play thì hiện nay, tiền sẽ được chuyển trực tiếp từ ví của người dùng sang ví của người làm ứng dụng.

Tiền số áp dụng công nghệ blockchain giúp người làm ứng dụng không gặp phải các rủi ro như yêu cầu hoàn tiền của khách hàng, dùng thẻ thanh toán không hợp pháp. Độ an toàn và bảo mật của việc thanh toán bằng tiền số cũng được đảm bảo bằng cách sử dụng chữ ký số.

Kết luận chương

Chương 3 luận văn đã trình bày bài toán thanh toán trên ứng dụng di động, giải pháp đưa ra là sử dụng đồng tiền số để thực hiện thanh toán. Đồng tiền số TYM đã được xây dựng và ứng dụng trong việc mua bán sách điện tử trên nền tảng iOS. Giải pháp ứng dụng tiền số hoàn toàn khả thi trong thực tế và có thể khắc phục được khó khăn cho các doanh nghiệp đang kinh doanh nội dung số vì tiền số là không thể yêu cầu hoàn trả. Chương 3 cũng đã trình bày chi tiết về cách cài đặt đồng tiền số TYM dựa trên phân tích về mô hình của Bitcoin trong chương 2.

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 thanh toán ứng dụng di động.

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 thanh toán trên các ứng dụng di động ở thời điểm hiện tại.
- Mô hình ứng dụng blockchain trong thanh toán di động, mua bán nội dung số.

2. Thực nghiệm:

- Xây dựng thành công đồng tiền số TYM.
- Xây dựng ứng dụng mua bán sách điện tử sử dụng đồng tiền số TYM.

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.

TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] Trịnh Nhật Tiến, *Giáo trình An Toàn Dữ Liệu*, Hà Nội, 2008, tr.21-46

Tiếng Anh

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," <https://bitcoin.org/bitcoin.pdf>

[3] Don Tapscott and Alex Tapscott, "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World," <http://blockchain-revolution.com/>

[4] Bitcoin project, "Bitcoin – open source P2P money," 2017.

[5] Wang, L. Feng, H. Zhang, C. Lyu, L. Wang and Y. You, "Human Resource Information Management Model based on Blockchain Technology," *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, San Francisco, CA, 2017, pp. 168-173.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, 2017, pp. 557-564.

[7] M. E. Peck and S. K. Moore, "The blossoming of the blockchain," in *IEEE Spectrum*, vol. 54, no. 10, pp. 24-25, October 2017.

[8] T. Lundqvist, A. de Blanche and H. R. H. Andersson, "Thing-to-thing electricity micro payments using blockchain technology," *2017 Global Internet of Things Summit (GIoTS)*, Geneva, 2017, pp. 1-6.

[9] J. Sidhu, "Syscoin: A Peer-to-Peer Electronic Cash System with Blockchain-Based Services for E-Business," *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, Vancouver, BC, 2017, pp. 1-6.

[10] Patrick D. Gallagher, "Digital Signature Standard (DSS)," in FIPS PUB 186-4, pp. 26-30, July 2013.

Các nguồn trên Internet

[11] <https://vi.wikipedia.org/wiki/Blockchain>

[12] <https://en.bitcoin.it/wiki/Difficulty>

[13] <http://ictnews.vn/internet/chinh-sach-doc-quyen-thanh-toan-cua-google-va-apple-dang-bi-cheater-truc-loi-157137.ict>

[14] <https://bfsystem.org/khac-biet-giua-tien-thuat-toan-tien-ao-tien-dien-tu/>

[15]<http://www.pcworld.com.vn/articles/congnghe/congnghe/2017/03/1250627/blockchain-xu-huong-moi-trong-tuong-lai/>