ĐẠI HỌC QUỐC GIA TP.HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA VẬT LÝ - VẬT LÝ KỸ THUẬT
CHUYÊN NGÀNH VẬT LÝ TIN HỌC

——————oOo——————

KHOÁ LUẬN TỐT NGHIỆP

Đề tài:

Blockchain

SVTH: Nguyễn Lễ
CBHD: Nguyễn Anh Thư

TP. HỒ CHÍ MINH - 2018

ĐẠI HỌC QUỐC GIA TP.HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA VẬT LÝ - VẬT LÝ KỸ THUẬT
CHUYÊN NGÀNH VẬT LÝ TIN HỌC

——————oOo——————

KHOÁ LUẬN TỐT NGHIỆP

Đề tài:

Blockchain

SVTH: Nguyễn Lễ
CBHD: Nguyễn Anh Thư

TP. HỒ CHÍ MINH - 2018

Lời cảm ơn

Đầu tiên, con xin gửi lời biết ơn đến mẹ, người đã thay thế vai trò người cha đã mất, cáng đáng cả gia đình và nuôi dưỡng con nên người, con cũng xin cảm ơn dì Chính, người mà còn vẫn luôn coi như người mẹ thứ hai, chăm sóc con từng miếng ăn, giấc ngủ và luôn coi con như con ruột của mình, công ơn của hai mẹ dành cho con không từ ngữ nào mà diễn tả được.

Em xin cảm ơn các thầy cô khoa Vật Lý - Vật Lý Kĩ Thuật, đã tận tâm truyền đạt kiến thức cho em trong những năm đầu đại học. Em xin chân thành cảm ơn thầy cô của Bộ môn Vật Lý Tin Học, đã xây dựng bộ môn với các trang thiết bị hiện đại và sự nhiệt tình, thân thiện của các thầy cô, giúp em có thể thoái mái học tập, nghiên cứu mà không cảm thấy căng thẳng, áp lực. Những lời chỉ bảo của thầy cô đã cho em những kiến thức cần thiết và quý báu cho định hướng của mình.

Và em cũng xin gửi lời cảm ơn tới thầy TS. Nguyễn Chí Linh, đã giới thiệu và hướng em vào đề tài này khi em không xác định được hướng đi cho mình, thầy cũng dành thời gian đọc, chỉnh sửa và góp ý cho bài báo cáo này được hoàn thiện hơn. Đồng thời tôi cũng muốn cảm ơn những người bạn ở Vật Lý Lý Thuyết, đã dành thời gian với tôi trong những ngày mới bước vào chuyên ngành, thông qua những buổi nói chuyện đó, tôi mới lần đầu biết đến nền tảng LaTeX.

Và cuối cùng, tôi xin cảm ơn những người bạn, những người đàn em đã cùng đồng hành với tôi trong suốt bốn năm trên giảng đường Đại học, cảm ơn vì những khoảng khắc trò chuyện vui vẻ giúp giải toả áp lực đã trở thành một phần kỉ niệm của đời sinh viên.

TP. Hồ Chí Minh, tháng 1 năm 2018.

Trịnh Tích Thiện

Mục lục

Danh sách hình vẽ

Lời giới thiệu

Ngày nay, ngoài các trình soạn thảo văn bản phổ biến, LaTeX cũng là một sự lựa chọn dành cho người soạn thảo được tạo ra với triết lý hoàn toàn khác biệt so với các trình hiện hành. Nhận thấy hạn chế của chất lượng in ấn ở những năm 1970, và việc người dùng tốn quá nhiều thời gian để định dạng thay vì tập trung soạn thảo, Donald E.Knuth đã phát triển hệ thống TeX, và từ đó, Leslie Lamport xây dựng thành LaTeX, với mục đích giúp người dùng sử dụng câu lệnh để việc thiết kế văn bản được thực hiện một cách tự động bởi hệ thống.

Tuy xuất hiện đã lâu nhưng do không có tính trực quan vốn có của các trình soạn thảo văn bản thông thường cũng như đòi hỏi người sử dụng có khái niệm cơ bản, về ngôn ngữ đánh dấu (markup language), cộng thêm việc nền tảng này chỉ lưu hành trong giới học thuật, nên LaTeX vẫn chưa thực sự phổ biến đến những người dùng phổ thông (mặc dù đối tượng sử dụng ngày càng đa dạng).

Nhận thấy LaTeX thích hợp để tạo các văn bản có quy chuẩn rõ ràng, đồng thời nền tảng cho phép người dùng thiết kế bố cục và kiểu văn bản cho riêng mình, đề tài này đã ra đời nhằm mục đích thiết kế, xây dựng một mẫu báo cáo khoá luận chuẩn trên nền LaTeX, định nghĩa các câu lệnh mới để hỗ trợ những người dùng sau này có thể dễ dàng định dạng các báo cáo khoá luận mà không tốn nhiều thời gian vào việc thiết kế, canh chỉnh, thay vào đó tập trung hơn vào nội dung và thành phần văn bản của mình, kế thừa đúng với tinh thần của những người sáng tạo ra LaTeX.

Tài liệu về LaTeX tuy đa dạng, nhưng lại có tính chuyên môn, đòi hỏi thời gian tìm hiểu và tổng hợp những tài liệu thật sự cần thiết, nhưng cũng nhờ đó, tôi đã có thêm kĩ năng đọc hiểu, tìm kiếm thông tin, đồng thời hiểu thêm được các khái niệm, thao tác lập trình với macro, cũng như tiếp cận và biết thêm được nhiều thủ thuật soạn thảo, trình bày văn bản theo ý mình sử dụng LaTeX, và đó là những lý do tôi chọn đề tài này. Thông qua đề tài, ngoài việc xây dựng thành công một mẫu khoá luận, tôi cũng muốn phổ biến sự tiện lợi trong việc soạn thảo các văn bản khoa học của LaTeX đến nhiều người hơn bằng việc giới thiệu, đưa ra những hướng dẫn cơ bản và tổng hợp những nguồn tham khảo tin cậy cho hệ thống LaTeX này.

Báo cáo đề tài gồm bốn chương chính như sau:

- **Chương 1: Tổng quan về LaTeX.** Giới thiệu khái niệm của LaTeX và lịch sử hình thành của hệ thống, đồng thời giới thiệu sơ lược về trình soạn thảo hỗ trợ LaTeX.
- **Chương ??: Soạn thảo văn bản trong LaTeX.** Hướng dẫn cách tải và cài đặt nền tảng LaTeX trên hai hệ điều hành Windows và Linux, đồng thời đưa ra những hướng dẫn cơ bản về cách soạn thảo văn bản bằng LaTeX, các khái niệm, thuật ngữ và câu lệnh cần nắm để dễ dàng hiểu được các tài liệu hướng dẫn LaTeX.
- **Chương ??: Thiết kế định dạng văn bản riêng trong LaTeX.** Sẽ tập trung vào cách thức thiết kế các định dạng văn bản riêng trong LaTeX, từ đó tiến tới thiết kế bài báo cáo, luận văn, sau đó phân tích quy trình tạo và cấu trúc của tập tin (file) sản phẩm đề tài.
- **Chương ??: Kết luận và hướng phát triển.** Đưa ra kết luận về kết quả thu được của đề tài này và đánh giá hướng phát triển của thành phẩm.

CHƯƠNG 1

Khái quát về blockchain

1.1 Lịch sử

Những ý tưởng đầu tiên về chuỗi các block bảo mật nhờ các phương pháp mã hóa được mô tả vào năm 1991 bởi hai nhà khoa học Stuart Haber và W. Scott Stornetta [**haber**]. Vào năm 1992, Bayer, Haber và Stornetta tích hợp cây Merkle vào thiết kế, giúp cải thiện tính hiệu quả bằng cách cho phép nhiều văn bản được gom chung vào một block [**cryptocurrencytech**].

Khái niệm về blockchain được trình bày lần đầu bởi một người (hoặc nhóm người) có bút danh Satoshi Nakamoto vào năm 2008. Nó được hiện thực hóa vào năm tiếp theo bởi Nakamoto như một thành phần cốt lõi của đồng tiền ảo bitcoin, nơi blockchain hoạt động như một sổ ghi chép công cộng mọi giao dịch trên hệ thống mạng. Thông qua việc ứng dụng blockchain, bitcoin trở thành đồng tiền ảo đầu tiên giải quyết được vấn đề trả-tiền-hai-lần mà không cần đến một một bên được ủy quyền và là nguồn cảm hứng cho nhiều ứng dụng khác.

Tháng Tám năm 2014, kích thước file của blockchain bitcoin, chứa ghi chép của tất cả giao dịch diễn ra trên hệ thống mạng, đạt 20 GB. Vào tháng Một năm 2015, kích thước file đã tăng lên đến gần 30 GB, và từ tháng Một 2016 đến tháng 2017, blockchian bitcoin đã tăng từ 50 GB lên 100 GB về kích thước.

Từ *block* và *chain* được sử dụng một cách riêng rẻ trong tài liệu gốc của Satoshi Nakamoto, nhưng dần dần trở nên phổ biến như một từ đơn, *blockchan*, vào năm 2016. Thuật ngữ blockchain 2.0 chỉ những ứng dụng mới của cơ sở dữ liệu blockchain phân tán, nổi lên lần đầu vào năm 2014. Tạp chí *The Economist* mô tả *Ethereum*, một ứng dụng của blockchain có khả năng lập trình thế hệ thứ hai này như sau: "một ngôn ngữ lập trình cho phép người dùng viết ra những hợp đồng thông minh phức tạp hơn, nhờ đó tạo ra những hóa đơn tự trả khi một đơn hàng tới hay tự động chia cổ tức cho cổ đông khi lợi nhuận đạt tới một mức nhất định". Công nghệ Blockchain 2.0 đã vượt ra khỏi khuôn khổ giao dịch và cho phép "trao đổi giá trị mà không cần tới những bên

trung tâm đầy quyền lực hoạt động như những kẻ kiểm soát tiền và thông tin". Chúng được mong đợi sẽ cho phép mọi người tham gia vào nền kinh tế toàn cầu, bảo vệ quyền riêng tư của những người tham gia, cho phép mọi người "kiếm tiền từ thông tin của chính họ"và cung cấp khả năng đảm bảo những người tạo ra nội dung được trả thưởng cho tài sản trí tuệ họ làm ra. Công nghệ blockchan thế hệ thứ hai cho phép lưu trữ "ID số và diện mạo thay đổi liên tục"của từng cá nhân và cung cấp giải pháp giải quyết vấn đề bất bình đẳng xã hội bằng cách "thay đổi cách thức của cải được phân phối".

Vào năm 2016, Kho lưu ký chứng khoán trung tâm của Liên bang Nga (NSD) đã công bố một dự án thí điểm, dựa trên nền tảng blockchian 2.0 Nxt nhằm khai thác và đưa vào sử dụng hệ thống bầu cử tự động dựa trên nàng blockchain. IBM đã mở môt trung tâm nghiên cứu đổi mới blockchain tại Singapore vào tháng Bảy năm 2016. Một nhóm làm việc cho Diễn đàn Kinh tế Thế giiới đã gặp nhau vào tháng 11 năm 2016 để thảo luận sự phát triển các mô hình quản trị liên quan đến blockcchain. Theo Accenture, một ứng dụng của lý thuyết khuyến đại cải tiến (Diffusion of innovations), cho rằng blockchain đạt tỉ lệ 13,5% ứng dụng trong các dịch vụ tài chính năm 2016,. Các nhóm thương mại công nghiệp đã tham gia tạo ra Diễn đàn Blockchain thế giới, một sáng kiến của Phòng Thương mại Số Hoa Kỳ.

1.2 Double Spending: Vấn đề mà blockchain giải quyết

Trong suốt chiều dài lịch sử, các loại tiền tệ bằng kim loại hoặc giấy được sử dụng bởi nhiều nền văn minh trên khắp thế giới. Trong các giao dịch được thực hiện với các loại tiền ấy, một bên phải trả một lượng tiền cho bên thứ hai để nhận một lượng hàng hóa hoặc dịch vụ. Khi tiền thực được trao đổi, không có khả năng cùng một món tiền lại được trả bởi cùng một bên hai lần.

Ví dụ, với các loại tiền giấy hoặc kim loại, một người không thể trả một đô la cho một quả táo, và sau đó sử dụng đúng đồng đô la đó để mua quả cam. Đó là vì đồng đô la đã được chuyển cho người bán trong quá trình mua bán quả táo. Tuy nhiên, với tiền ảo, không có quá trình chuyển vật lý của tiền, tạo nên cái được goi là vấn đề vấn đề trả tiền hai lần.

vấn đề trả tiền hai lần là khi một người dùng cùng một món tiền cho hai giao dịch hoặc nhiều hơn. Trước khi có Bitcoin, đây là một vấn đề lớn vì nó xóa bỏ đặc trưng giới hạn về số lượng của các loại tiền ảo, vốn là đặc trưng cơ sở để một loại tiền

để có thể tồn tại. Nếu mỗi đơn vị tiền có thể được dùng một lượng vô hạn số lần, thì nó sẽ không có giá trị thực nào.

1.3 Theo bước Satoshi Nakamoto

Sau cuộc khủng hoảng tài chính 2008, một nhà tiên phong tên Satoshi Nakamoto đã tìm ra cách giải quyết cho vấn đề vấn đề trả tiền hai lần và tạo ra một loại tiền ảo không bị vấn đề trả tiền hai lần ảnh hưởng. Cho đến nay, không ai biết được danh tính thật sự của Satoshi. Satoshi Nakamoto chỉ là một bút danh.

Satoshi Nakamoto đã tạo ra một giải pháp độc nhất để ngăn chặn double sending. Giải quyết đó được goi là công nghệ blockchain. Chi tiết của cả Bitcoin và công nghệ blockchain được trình bày trong một sách trắng được phát hành bởi Satoshi Nakamoto vào tháng 11 năm 2008 tên là "Bitcoin: A Peer-to-Peer Electronic Cash System".

Trong sách trắng này, Nakamoto giải thích tại sao các giao dịch tài chính điện tử lúc đó vẫn phải phụ thuộc vào bên thứ ba được tin cậy (ví dụ như ngân hàng) để giải quyết vấn đề vấn đề trả tiền hai lần, và việc đó có thể được thay đổi với công nghệ blockchain ra sao.

1.4 Công nghệ blockchain

Công nghệ blockchain về cơ bản là một sổ cái công cộng ghi chép mọi giao dịch trên một bản ghi có thể mở rộng. Các giao dịch phải được chứng thực bởi các "thợ đào"để chúng được coi là hợp lệ và được thêm vào blockchain. Các thợ đào nhận được những khuyến khích để thực hiện việc chứng thực - một lượng Bitcoin nhất định cho một lần chứng thực giao dịch thành công.

Với phương thức này, ta không cần tới ngân hàng để ngăn chặn vấn đề trả tiền hai lần và mỗi giao dịch đều được xác minh để đảm bảo rằng không ai xài cùng một lượng Bitcoin quá một lần. Nếu có ai đó tìm cách xài cùng một lượng Bitcoin hai lần bằng cách thực hiện hai giao dịch khác nhau với cùng một đầu vào Bitcoin trên cùng một block, thì hai giao dịch sẽ không bao giờ được xác nhận trên hệ thống mạng. Nhờ đó mà cơ bản biến chúng thành các giao dịch không hợp lệ và chúng sẽ bị "hủy", qua đó ngăn chặn vấn đề trả tiền hai lần.

Các chi tiết về việc làm thế nào mà blockchain có thể ngăn chặn được vấn đề trả

tiền hai lần sẽ được trình bày ở các chương sau, liên quan đến cấu trúc dữ liệu của nó và các phương pháp mã hóa được ứng dụng trong công nghệ blockchain.

1.5 Các loại blockchain

Một blockchain có thể thuộc loai không cần cho phép (permissionless) ,như Bitcoin hoặc Ethereum; hoặc cần cho phép (permissioned). Một blockchain không cần cho phép, còn được gọi là một blockchain công cộng bởi vì bất kỳ ai đều có thể tham gia vào mạng. Một blockchain cần cho phép, hay blockchain riêng tư, yêu cầu có sự xác minh trước của các bên tham gia trong mạng, và các bên này thường đã biết nhau.

Sự lựa chọn giữa blockchain công cộng và riêng tư thường được quyết định bởi các ứng dụng cụ thể cần giải quyết. Một ví dụ mà các doanh nghiệp trao đổi thông tin với nhau là trong quản lý chuỗi cung ứng. Quản lý chuỗi cung ứng là một trường hợp lý tưởng để sử dụng blockchain riêng tư. Ta không muốn các công ty không mời tham gia vào mạng. Mỗi bên tham gia chuỗi cung ứng sẽ được yêu cầu quyền (permission) để thực hiện các giao dịch trong blockchain. Các giao dịch này sẽ cho phép các công ty khác biết một sản phẩm cụ thể đang nằm ở đâu.

Ngược lại, khi một mạng có thể tạo thuận lợi cho các bên giao dịch mà không nhất thiết phải xác minh danh tính của nhau, như blockchain Bitcoin, một blockchain công cộng phù hợp hơn. Một số ví dụ như bán hoặc phân phối sản phẩm trong một cộng đồng. Các loại tiền mã hóa (vốn không được các chính phủ ủng hộ) thường sử dụng blockchain công cộng.

CHƯƠNG 2

Cách thức hoạt động của blockchain

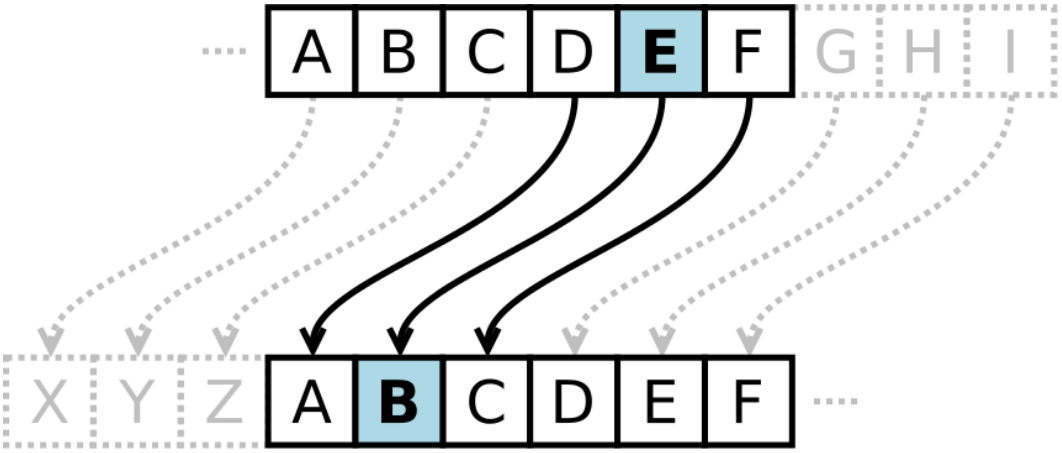
2.1 Mật mã trong blockchain

Mật mã học là những phương pháp giúp che giấu và lộ diện, hay còn gọi là mã hóa và giải mã, thông tin thông qua các phương pháp toán học phức tạp. Điều này có nghĩa là thông tin không thể được xem bởi bất kỳ ai ngoại trừ những người nhận được định trước. Các phương pháp bao gồm lấy các thông tin chưa được mã hóa như một đoạn văn bản, và mã hóa nó bằng cách sử dụng một thuật toán (tiếng Anh gọi là cypher). Nó tạo nên một văn bản đã mã hóa (ciphetext), một mẩu thông tin hoàn toàn vô dụng và vô nghĩa chi đến khi được giải mã. Phương pháp mã hóa này được gọi là mã hóa chìa khóa đối xứng (symmetric-key cryptography).

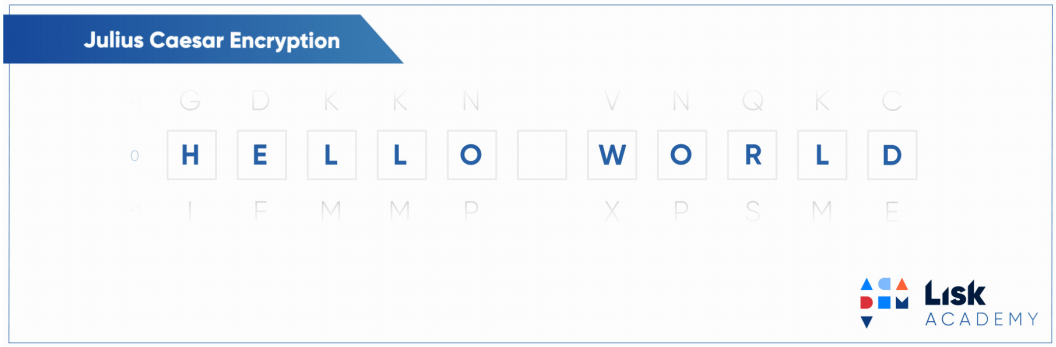
Một ví dụ về mật mã xuất hiện sớm trên thế giới là mật mã Caesar (Caesar cipher), được sử dụng bởi Julius Caesar để bảo vệ các bí mật quan sự của Roman. Mỗi chữ cái trong một tin nhắn được thay thế với chữ cái đứng trước nó 3 chữ cái về phía bên trái trong bảng chữ cái, thông tin này về cơ bản chính là chìa khóa để giải mã tin nhắn. Các tướng của Caesar biết rằng để giải (decode) các chữ cái họ chỉ phải dịch mỗi chữ về phía phải (bảng chữ cái) ba lần, trong khi thông tin sẽ được giữ an toàn nếu bị chặn bởi kẻ thù của Caesar. Mật mã học hiện đại hoạt động tương tự, nhưng với độ phức tạp cao hơn rất nhiều.

Mã nền (codebase) của phần lớn các thuật toán dùng trong mật mã là các dự án mã nguồn mở, nghĩa là code của chúng có thể được xem xét bởi bất kì ai. Thuật toán (cipher) được sử dụng rộng rãi nhất trên thế giới là AES, cho phép bất kì ai đều có thể sử dụng và code của nó được mở để cộng đồng có thể xem. Kết quả là nó đã được nghiên cứu chi tiết và cho đến nay chưa có lỗ hỗng nào được phát hiện. Thuật toán này cũng được sử dụng bởi NSA, cơ quan tình báo Hoa Kỳ, như một công cụ được chọn để mã hóa thông tin. Vì vậy, có thể nói thông tin được ghi lại trên blockchain được bảo mật với cùng mức độ như bảo mật những bí mật nhạy cảm nhất thế giới.

Trong blockchain, mật mã được sử dụng chủ yếu cho hai mục đích: Bảo vệ nhận



Hình 2.1: Cách thức hoạt động của một mật mã Caesar là thay thế mỗi chữ cái với một chữ khác cách một khoảng cố định trên bảng chữ cái



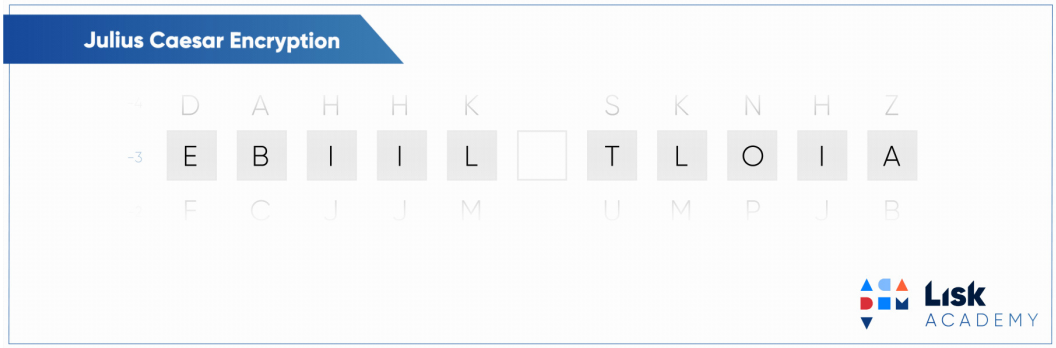
Hình 2.2: Câu "Hello World"trước khi mã hóa

dạng (identities) của người gửi giao dịch Đảm bảo các ghi chép trong quá khứ không thể bị giả mạo

Công nghệ blockchain sử dụng mật mã như một phương tiện để bảo vệ nhận dạng của người dùng, đảm bảo giao dịch được thực hiện một cách an toàn và bảo mật mọi thông tin và giá trị lưu trữ. Vì vậy, bất kì ai sử dụng blockchain đều có thể hoàn toàn tự tin rằng thông tin khi đã được ghi trên blockchain thì hoàn toàn hợp lệ và bảo mật.

Mặc dù được xây dựng trên một khuôn khổ tương tự, nhưng mật mã khóa công khai (public-key cryptography), loại mật mã được dùng trong blockchain, phù hợp với các chức năng liên quan đến blockchain hơn so với mật mã khóa đối xứng.

Public-Key Cryptography, còn được gọi là asymmetric cryptography là một cải tiến trên nền tảng mật mã khóa đối xứng chuẩn: nó cho phép thông tin được truyền nhờ vào một khóa công khai có thể được chia sẽ với bất kỳ ai



Hình 2.3: Câu "Hello World"sau khi mã hóa bằng mật mã Caesar

Thay vì sử dụng một chìa khóa duy nhất cho cả việc mã hóa và giảm mã, như với trường hợp của mật mã khóa đối xứng, trong mật mã khóa công khai, các chìa khóa riêng rẽ (một khóa công khai và một khóa riêng tư) được sử dụng.

Sự kết hợp giữa khóa công khai và riêng tư của người dùng giúp mã hóa thông tin, còn khóa riêng tư của người nhận và khóa công khai của người gửi giúp giải mã nó. Không thể tìm ra khóa riêng tư dựa trên khóa công khai. Vì vậy, một người dùng có thể gửi khóa công khai của họ đến bất kỳ ai mà không sợ rằng ai đó sẽ có quyền truy cập vào khóa riêng tư của họ. Người gửi có thể mã hóa tập tin và chắc chắn rằng những tập tin đó sẽ chỉ có thể bị giải mã bởi bên được định trước.

Thêm vào đó, thông qua mật mã khóa công khai, một chữ ký điện tử được tạo ra, bảo vệ sự toàn vẹn của dữ liệu. Điều này được thực hiện bằng cách kết hợp chìa khóa riêng tư của người dùng với dữ liệu mà họ muốn kí, thông qua thuật toán nhất định.

Do bản thân dữ liệu là một phần của chữ kí số, hệ thống mạng sẽ không ghi nhận nó là hợp lệ nếu bất kì phần nào của nó bị giả mạo. Việc chỉnh sửa kể cả nhỏ nhất cũng sẽ làm thay đổi toàn bộ chữ kí, làm cho nó sai khác đi và không dùng được nữa. Thông qua đó, công nghệ blockchain có khả năng đảm bảo rằng bất kì dữ liệu nào đã được ghi vào là đúng, chính xác và không bị giảm mạo. Chữ kí số tạo nên tính bất khả đổi của dữ liệu được khi trong một blockchain.

2.2 Chữ kí số

Chữ kí số đúng như tên gọi của nó: nó cung cấp sự xác nhận và chứng thực tương tự như chữ kí bình thường, ở dạng số hóa. Phân đoạn này sẽ thảo luận cách chúng

hoạt động cũng như cách đa chữ kí (multisignatures) được sử dụng để tăng thêm một lớp bảo mật.

Chữ kí số là một trong những phương tiện chính để đảm bảo tính an toàn và toàn vẹn của dữ liệu được ghi trên một blockchain. Chúng là một bộ phận tiêu chuẩn trong giao thức blockchain, được dùng chủ yếu để bảo vệ giao dịch và khối giao dịch, sự chuyển các thông tin nhạy cảm, phân phối phần mềm, quản lý hợp đồng và các trường hợp khác khi việc phát hiện và ngăn chặn các hành động làm giả mạo từ bên ngoài. Chữ ký số sử dụng mật mã bất đồng bộ, nghĩa là thông tin có thể được chia sẽ với bất kỳ ai bằng cách sử dụng chìa khóa công khai.

Ở nhiều nơi trên thế giới, chữ ký điện tử có cùng ràng buộc pháp lý như chữ kí thường. Ví dụ về các quốc gia và thực thể công nhận chúng bao gồm: Liên Minh Châu Âu, Liên Hợp Quốc, Liên Hợp Quốc, Hoa Kỳ, Brazil, Mexico, India, Indonesia, Turkey và Saudi Arabia.

Chữ kí số cung cấp ba lợi thế cho việc lưu trữ và truyền thông tin trên một blockchain. Đầu tiên, chúng đảm bảo tính toàn vẹn. Về lý thuyết, dữ liệu (đã được mã hóa) được gửi đi tuy không thể bị nhìn thấy nhưng có thể bị thay đổi bởi tin tặc. Tuy nhiên nếu điều này xảy ra, chữ kí của nó cũng sẽ bị thay đổi. Vì vậy dữ liệu đã được kí số không chỉ an toàn do không bị nhìn thấy mà còn tiết lộ nếu nó đã giả mạo.

Chữ kí số không chỉ bảo vệ dữ liệu mà còn bảo vệ nhận dạng của người gửi. Chỉ có chủ nhân của chữ kí số mới nắm và dùng được chữ kí số đó và do đó, một người có thể chắc chắn rằng họ đang liên lạc với người mà họ muốn (liên lạc).

Khi sử dụng công nghệ blockchain, một người dùng có một chìa khóa công khai và một chìa khóa riêng tư, cả hai đều có dạng chuỗi các số và chữ ngẫu nhiên. Có thể coi chìa khóa công khai này, hay đôi khi còn được gọi là địa chỉ công khai, như một địa chỉ email và khóa riêng tư như là mật khẩu. Điều rất quan trọng là không được chia sẻ chìa khóa riêng tư với bất kì ai.

Cuối cùng, chữ kí số mang tính không thể chối bỏ do chìa khóa riêng tư gắn liền với ngươi dùng. Điều này có nghĩa là nếu cái gì đó đã được kí số bởi một người dùng, nó đã được ràng buộc về mặt pháp lý và hoàn toàn liên kết với cá nhân đó. Như đã chỉ ra ở trên, điều này phụ thuộc nhiều vào không có nghi ngờ về việc chìa khóa riêng tư dùng để kí dữ liệu không bị xâm phạm, sử dụng và nhìn thấy bởi bất kỳ ai ngoài chủ sở hữu của nó.

Mỗi người có một chữ kí duy nhất và nó được tạo ra bằng cách sử dụng ba thuật toán sau:

- Một thuật toán tạo chìa khóa, cung cấp một chìa khóa công khai và một chìa khóa riêng tư.
- Một thuật toán kí giúp kết hợp dữ liệu và khóa riêng tư để tạo thành một chữ kí
- Một thuật toán giúp xác thực chữ kí và xác định xem tin nhắn đó có đáng tin hay không dựa trên tin nhắn, khóa công khai và chữ kí.

Tính năng quan trọng nhất của những thuật toán đó là:

- Khiến việc tạo ra khóa riêng tư dựa trên khóa công khai hoặc dữ liệu mà nó mã hóa trở nên bất khả thi.
- Đảm bảo tính xác thực của một chữ kí dựa trên tin nhắn và khóa riêng tư, được xác thực thông qua khóa công khai.

2.2.1 Đa chữ kí

Đa chữ ký (Multisignature), đôi khi được rút ngắn thành multisig, là một chương trình chữ kí số đòi hỏi nhiều hơn một người kí để một giao dịch được chấp thuận. Khái niệm về hệ thống đa chữ kí không phải được tạo ra chỉ để dùng cho tiền ảo mà đã xuất hiện từ hàng ngàn năm trước. Những tu sĩ ở núi Athos đã bảo vệ hầm mộ của nó với nhiều chìa khóa và cần nhiều hơn một chìa để mở khóa hầm mộ. Điều này có nghĩa là không một tu sĩ đơn lẻ nào có thể tiếp cập các di tích quý giá mà không cần ít nhất một tu sĩ khác.

Multisig được sử dụng bởi nhiều loại tiền ảo, bao gồm Bitcoin[1] và List, như một phương tiện để cải thiện độ bảo mật cũng như chia khả năng đưa ra quyết định cho nhiều hơn một bên.

Ví dụ, với đa chữ kí ta có thể tạo một dịch vụ giao kèo 2 trên 3, nghĩa là để xác nhận một giao dịch đòi hỏi cần phải có sự chấp nhận của hai trong số ba bên để thực hiện. Một ví dụ về trường hợp đa chữ kí hữu ích là tài khoản tiết kiệm cho một đứa trẻ, khi cả đứa trẻ và ít nhất một trong số bố mẹ nó cần đồng thuận cách tiền trong đó được rút ra và xài. Nó cũng mở ra tùy chọn mà các quyết định quan trọng được đưa ra chỉ từ phía phụ huynh, miễn là cả hai đều đồng ý.

Chữ kí số là thành phần tối quan trọng trong việc bảo vệ dữ liệu trên một blockchain.

[1]Đồng tiền ảo mã nguồn mở, phi tập trung đầu tiên thành công chạy trên một mạng ngang hàng (P2P)

2.3 Nút

2.3.1 Khái niệm về nút

Một nút là một thiết bị trên một hệ thống mạng blocchain, và về bản chất chính là nền tảng của công nghệ này: nó giúp blockchain hoạt động và tồn tại. Các nút được phân bố trên một mạng lưới rộng khắp và thực hiện nhiều tác vụ khác nhau.

Một nút có thể là một thiết bị điện tử bất kỳ, bao gồm máy tính, điện thoại hoặc thậm chí là máy in, miễn là nó được kết nối với Internet và do đó có một địa chỉ IP. Vai trò của một nút là hỗ trợ hệ thống mạng bằng cách duy trì một bản sao của blockchain và trong một số trường hợp, giúp xử lí các giao dịch. Nút thường có dạng cấu trúc cây nhị phân. Mỗi loại tiền ảo có nút của riêng nó, duy trì các bản ghi chép giao dịch của đồng tiền đó.

Các nút là những thành phần đơn lẻ của một cấu trúc lớn hơn: blockchain. Chủ sở hữu của các nút sẵn sàng đóng góp tài nguyên tính toán của họ để lưu trữ và xác thực các giao dịch và do đó họ có cơ hội nhận được phí giao dịch và nhận phần thưởng cho công việc ấy.

Việc xử lý các giao dịch đòi hỏi một lượng lớn sức mạnh tính toán và xử lý, nghĩa là năng lực của một máy tính bình thường không đáp ứng yêu cầu. Generally, professional miners tend to invest in extremely powerful computing devices known as CPUs (central processing units) or GPUs (graphics processing units) in order to keep up with the demand for processing power that is required for them to validate transactions and as such earn the rewards that comes with doing so.