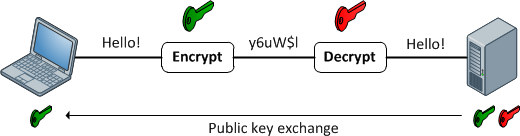
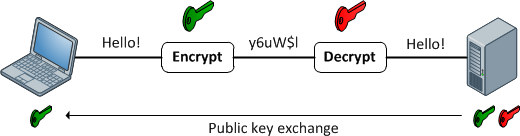
Mã hóa đối xứng (Symmetrical encryption)



* Symmetrical encryption là loại mã hóa trong đó chỉ có một khóa (secret key) được sử dụng để vừa mã hóa vừa giải mã thông tin ở cả trên host và client. Các thực thể giao tiếp thông qua mã hóa đối xứng phải trao đổi khóa để nó có thể được sử dụng trong quá trình giải mã. Phương pháp mã hóa này khác với asymmetrical encrytion sử dụng một cặp khóa, một khóa công khai (public key) và một khóa riêng tư (private key) được sử dụng để mã hóa và giải mã tin nhắn.

Mã hóa bất đối xứng (Asymmetrical encrytion) | public-key cryptography



* Quá trình sử dụng một cặp khóa liên quan – một khóa công khai (public key) và một khóa riêng (private key) – để mã hóa và giải mã một tin nhắn và bảo vệ nó khỏi bị truy cập hoặc sử dụng trái phép. Khóa công khai là một khóa mật mã có thể được sử dụng bởi bất kỳ người nào để mã hóa một tin nhắn sao cho nó chỉ có thể được giải mã bởi người nhận dự kiến bằng khóa riêng của họ. Khóa riêng tư – còn được gọi là khóa bí mật – chỉ được chia sẻ với người khởi tạo khóa.

Hashing

* Trong khi encryption là một quy trình gồm hai bước được sử dụng để mã hóa và sau đó giải mã một tin nhắn, Hashing sẽ cô đọng một tin nhắn thành một giá trị có độ dài cố định không thể thay đổi được hay còn gọi là hàm băm. Hai trong số các thuật toán Hashing phổ biến nhất trong network là MD5 và SHA-1.



* Trong SSH, các giá trị Hash chủ yếu được sử dụng để kiểm tra tính toàn vẹn của dữ liệu (dữ liệu không bị sửa đổi một cách vô tình hay cố ý) và để xác minh tính xác thực của giao tiếp. Việc sử dụng chính của các giá trị Hash trong SSH là với HMAC (Hashed Message Authentication Code). HMAC sử dụng các giá trị Hash để tạo mã HMAC. Chúng được sử dụng để đảm bảo rằng văn bản tin nhắn nhận được là nguyên vẹn và không bị sửa đổi.

HASH FUNCTION:

* Unique hash
* Commitment
* Puzzle friendly

BLOCKCHAIN LÀM GÌ ĐỂ BẢO MẬT?

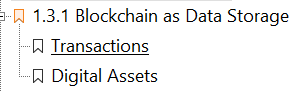
* Proof of work 🡪 làm cho mã HASH thêm khó giải thêm nhiều con số 0 ở đầu (cộng dồn)
* Thời gian giải từng block sẽ bị giới hạn và cần giải hết tất cả trong cùng 1 lúc (Không chỉ block riêng mà còn các máy chủ trên toàn thế giới nói chung ít nhất là 51%)
* Nếu như giải lâu sẽ giảm độ khó, giải nhanh sẽ tăng độ khó… có thể tăng giảm đi thời gian giải
* (Public Blockchain) it has an *open network* where nodes can join and leave as they please  
  without requiring permission from anyone; all full nodes in the network can *verify* each new piece of data added to the data structure, including blocks, transactions, and effects of transactions; its protocol includes an *incentive mechanism* that aims to ensure the correct operation of the blockchain system including that valid transactions  
  are processed and included in the ledger and that invalid transactions are  
  rejected
* Phân tán trên nhiều máy khác nhau (Distributed Ledger)

1. CƠ CHẾ NÀO GIÚP EM THAM GIA VÀO MẠNG LƯỚI BLOCKCHAIN VÀ LÀM SAO ĐỂ BẢO MẬT ĐC THÔNG TIN NG KHÁC

* Lưu trữ thông tin giao dịch trên cả block
* Incentive mechanism 🡪 cơ chế khuyến khích như tặng tiền
* Bảo mật tất cả các nodes đầy đủ xác minh mọi thứ

1. LÀM THẾ NÀO ĐỂ BLOCKCHAIN GIAO DỊCH AN TOÀN? 🡪 TRANSACTION…

Diagram

Description automatically generated

* the transaction is signed with the signature of the transaction’s initiator,
* A signed transaction should contain all the information needed to be executed.
* A proposed transaction is sent to a node connected to the blockchain network, which checks the validity of the transaction. Invalid transactions are discarded.
* To ensure that the transaction propagates, senders do not need to trust any individual node they send the transaction to, as long as they send it to enough other nodes. Recipients do not need to trust senders, because all transactions are signed and can be independently validated by any node
* New blocks are broadcast across the whole network, so that each full node holds a replica of the whole ledger

***Blockchain as Data Storage***

Là một cấu trúc dữ liệu, chuỗi khối là một danh sách các khối được sắp xếp theo thứ tự, trong đó mỗi khối chứa một danh sách giao dịch nhỏ (có thể trống). Mỗi khối trong một chuỗi khối được 'xâu chuỗi' trở lại khối trước đó, bằng cách chứa một hàm băm đại diện cho khối trước đó. Do đó, các giao dịch lịch sử trong chuỗi khối có thể không bị xóa hoặc thay đổi mà không làm mất hiệu lực chuỗi băm. Kết hợp với các ràng buộc tính toán và các chương trình khuyến khích trong việc tạo các khối, điều này trên thực tế có thể ngăn chặn việc giả mạo và sửa đổi thông tin được lưu trữ trong chuỗi khối. Là một cơ sở lưu trữ dữ liệu, thông tin trong chuỗi khối được ghi lại trong các giao dịch và trong các khối. Các danh mục thông tin quan trọng là giao dịch về tiền điện tử và giao dịch liên quan đến mã thông báo cho các loại tài sản khác.

***Smart Contracts***

A picture containing text, orange

Description automatically generated

1. CHỮ KÝ BẤT ĐỐI XỨNG LÀ GÌ? NGƯỜI KHÁC CÓ THỂ LẤY CHỮ KÍ ĐƯỢC KHÔNG?

Chữ ký bất đối xứng cho phép người dùng xác nhận tính chính xác của một giao dịch hoặc tin nhắn. Nó sử dụng một cặp khóa mã hóa để tạo ra một chữ ký dữ liệu mà chỉ có người sở hữu khóa công khai mới có thể xác thực.

Với chữ ký bất đối xứng, người gửi giao dịch sẽ sử dụng khóa riêng của mình để ký vào giao dịch và người nhận sẽ sử dụng khóa công khai để xác minh tính chính xác của chữ ký.

Điều này giúp đảm bảo rằng giao dịch chỉ có thể được thực hiện bởi người có quyển hạn và tránh việc giao dịch bị sửa đổi hoặc giả mạo bởi bên thứ 3.

1. CÓ MẤY LOẠI CHỮ KÍ BẤT ĐỐI XỨNG?

* Chữ ký số (digital signature): Là chữ ký bất đối xứng được sử dụng để **xác thực tính toàn vẹn và nguồn gốc của một tài liệu điện tử.** Chữ ký số được tạo ra bằng **cách áp dụng thuật toán băm (hashing algorithm)** cho tài liệu cần ký, sau đó **sử dụng khóa riêng tư để mã hóa** giá trị băm đó, tạo thành chữ ký số. Chữ ký số **cho phép người nhận kiểm tra tính toàn vẹn của tài liệu và đảm bảo rằng nó không bị thay đổi sau khi được ký**.
* Chứng thư số (digital certificate): Là chữ ký bất đối xứng được **sử dụng để xác thực danh tính của một thực thể trên internet**, ví dụ như một trang web hoặc một máy chủ email. Chứng thư số bao gồm thông tin về danh tính của thực thể và khóa công khai của nó, được chứng nhận bởi một cơ quan chứng thực uy tín. Khi bạn truy cập một trang web bảo mật, **trình duyệt web sẽ sử dụng chứng thư số để xác nhận rằng trang web đó thuộc về một thực thể đáng tin cậy và không bị giả mạo.**

Ngoài hai loại chữ ký bất đối xứng phổ biến là chữ ký số và chứng thư số, còn một số loại chữ ký bất đối xứng khác như sau:

* Chữ ký số hóa (digital signature): Tương tự như chữ ký số, chữ ký số hóa cũng được sử dụng để xác thực tính toàn vẹn và nguồn gốc của một tài liệu điện tử. Tuy nhiên, chữ ký số hóa được tạo ra bằng cách sử dụng một chữ ký số đã được cấp phép thay vì sử dụng khóa riêng tư để mã hóa giá trị băm của tài liệu.
* Chữ ký số biến đổi (transformed digital signature): Là một loại chữ ký bất đối xứng được sử dụng trong hệ thống chữ ký điện tử Tiền điện tử (Cryptocurrency). Chữ ký số biến đổi sử dụng một phép biến đổi số học đặc biệt để mã hóa thông tin của giao dịch Tiền điện tử.
* Chữ ký số quang học (quantum digital signature): Là một loại chữ ký bất đối xứng mới nhất được phát triển trên cơ sở các kỹ thuật mật mã học sử dụng quang học. Chữ ký số quang học được sử dụng để xác thực tính toàn vẹn và nguồn gốc của thông tin được truyền đi trên các kênh truyền thông có tính bảo mật cao sử dụng công nghệ quang học.

1. HIỂU THÊM VỀ CHỮ KÍ…

A private key is a **secret code that only the owner** of a cryptocurrency account knows. It is **used to authorize transactions** on the blockchain12. A public key is **a code that is derived** from the private key and can be shared with others. It is **used to receive cryptocurrencies on an address**13. The public key and the private key **are mathematically linked,** but it is very hard to guess the private key from the public key2.

Trong khi cả khóa công khai và khóa riêng tư đều cố gắng bảo mật giao dịch, chúng có sự khác biệt rõ ràng, tương ứng với mục đích của chúng. Khi so sánh chúng song song với nhau, khóa công khai được sử dụng để xác minh giao dịch sau khi giao dịch đã được yêu cầu. Thông thường, khóa công khai cũng được dịch là 'địa chỉ' để nhận tiền điện tử. Trong khi đó, khóa riêng tư liên quan đến tài khoản tiền điện tử tập trung vào việc ủy quyền giao dịch.

1. ELIPTICURVE / RSA512 / THUẬT TOÁN MÃ HÓA

Elliptic Curve Cryptography (ECC) is a **modern public-key encryption** technique famous for being smaller, faster, and more efficient than incumbents. Bitcoin, for example, uses ECC as its asymmetric cryptosystem because it is so lightweight**. The mathematical entity** that makes all of this possible is the elliptic curve, so read on to learn how these curves enable some of the most advanced cryptography in the world.

Mật mã học đường cong elliptic (ECC) là một kỹ thuật mã hóa khóa công khai dựa trên lý thuyết đường cong elliptic có thể được sử dụng để tạo ra các khóa mật mã học nhanh hơn, nhỏ hơn và hiệu quả hơn. ECC tạo ra các khóa thông qua các thuộc tính của phương trình đường cong elliptic thay vì phương pháp truyền thống là tích của các số nguyên tố rất lớn.

Trong ECC, một đường cong được xác định trên một trường hữu hạn và hai số nguyên tố lớn được chọn: một để xác định kích thước của trường và một để xác định thứ tự của đường cong. Một điểm cơ sở trên đường cong cũng được chọn. Khóa riêng tư trong ECC là một số được chọn ngẫu nhiên và khóa công khai được tính bằng cách nhân điểm cơ sở với khóa riêng tư. Sự an toàn của ECC dựa vào sự khó khăn trong việc giải quyết Vấn đề Logarithm Rời rạc Đường cong Elliptic (ECDLP), tức là tìm khóa riêng tư khi biết điểm cơ sở và khóa công khai.

RSA is a public-key encryption algorithm that was first described in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT. It is widely used in electronic commerce and is considered secure with a sufficiently large key length[**1**](https://bing.com/search?q=ELIPTICURVE+RSA512+THU%E1%BA%ACT+TO%C3%81N+M%C3%83+H%C3%93A).

Elliptic Curve Cryptography (ECC) is a new asymmetric encryption algorithm that is superior to RSA, the most commonly used algorithm today. [It has been proposed to apply this algorithm to build a Smart-Auto Parking system with higher security than existing systems on the marke](https://tailieumienphi.vn/doc/thuat-toan-ma-hoa-elliptic-curve-cryptography-ecc-va-ung-dung-trong-xay-dung-he--uymeuq.html)

RSA512: RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission.

The biggest difference between ECC and RSA/DSA is the greater cryptographic strength that ECC offers for equivalent key size. An ECC key is more secure than an RSA or DSA key of the same size.

RSA works by using a key pair that is mathematically linked to encrypt and decrypt data. [A private and public key are created, with the public key being accessible to anyone and the private key being kept secret by the owner](https://www.encryptionconsulting.com/education-center/what-is-rsa/)

thuật toán mã hóa

vs số 5 thì ngta sẽ mã hóa như nào.

8

Blockchains make use of two types of cryptographic algorithms, asymmetric-key algorithms, and hash functions. Hash functions are used to provide the functionality of a single view of blockchain to every participant. Blockchains generally use the SHA-256 hashing algorithm as their hash function.

**MD5**

The MD5 hash function produces a 128-bit hash value. It was designed for use in cryptography, but vulnerabilities were discovered over the course of time, so it is no longer recommended for that purpose. However, it is still used for database partitioning and computing checksums to validate files transfers.

**SHA-1**

SHA stands for Secure Hash Algorithm. The first version of the algorithm was SHA-1, and was later followed by SHA-2 (see below).

Whereas MD5 produces a 128-bit hash, SHA1 generates 160-bit hash (20 bytes). In hexadecimal format, it is an integer 40 digits long. Like MD5, it was designed for cryptology applications, but was soon found to have vulnerabilities also. As of today, it is no longer considered to be any less resistant to attack than MD5.

**SHA-2**

The second version of SHA, called SHA-2, has many variants. Probably the one most commonly used is SHA-256, which the National Institute of Standards and Technology (NIST) recommends using instead of MD5 or SHA-1.

The SHA-256 algorithm returns hash value of 256-bits, or 64 hexadecimal digits. While not quite perfect, current research indicates it is considerably more secure than either MD5 or SHA-1.

Performance-wise, a SHA-256 hash is about 20-30% slower to calculate than either MD5 or SHA-1 hashes.

**SHA-3**

This hash method was developed in late 2015, and has not seen widespread use yet. Its algorithm is unrelated to the one used by its predecessor, SHA-2.

The SHA3-256 algorithm is a variant with equivalent applicability to that of the earlier SHA-256, with the former taking slightly longer to calculate than the later

**What is SHA-512? (Definition)**

SHA-512 is a hashing algorithm used in cryptography, based on SHA-2 with the 512-bit variant. It works on the same principle as SHA-256, except that it calculates a 512-bit digital fingerprint - 128 hexadecimal characters.

**How to encrypt a character string using SHA512?**

SHA512 encryption is similar to SHA256, but with 512 bits.

Example: dCode has for fingerprint f825e3e0ebc4f343a7575b319236755dfe6dfb489be11d7c359118be03b5c5ed0113131f4235e22e8e0d226b65ec5abb47d9112b624b573ffb3e154056d62d09

The main difference with SHA-256 is the size of the processed data (1024 bits is twice as large) and the use of 64-bit words and calculations (better suited to 64-bit architectures).

SHA-512 là một thuật toán băm (hash function) được sử dụng để tạo ra một mã băm (hash) độc nhất từ một chuỗi dữ liệu đầu vào (input data). SHA-512 là phiên bản nâng cao của thuật toán SHA-256 với độ dài mã băm lên tới 512 bit. Thuật toán SHA-512 được sử dụng rộng rãi trong các ứng dụng bảo mật, bao gồm cả các hệ thống mật mã, chứng thực, xác thực và bảo mật mạng. Nó cũng được sử dụng trong các ứng dụng lưu trữ, xử lý và truyền dữ liệu. Thuật toán SHA-512 là một thuật toán băm không đổi (deterministic), có nghĩa là cùng một đầu vào sẽ cho ra cùng một mã băm, và có khả năng chống lại các cuộc tấn công băm ngược (reversal attacks). Thuật toán này cũng có thể xử lý các chuỗi dữ liệu lớn hơn so với phiên bản trước đó của nó, SHA-256. Tuy nhiên, việc sử dụng thuật toán SHA-512 cần được cân nhắc đối với các ứng dụng có tài nguyên hạn chế, do độ phức tạp của nó cao hơn so với các thuật toán băm khác với độ dài mã băm thấp hơn.

RSA(Rivest-Shamir-Adleman) is an Asymmetric encryption technique that uses two different keys as public and private keys to perform the encryption and decryption. With RSA, you can encrypt sensitive information with a public key and a matching private key is used to decrypt the encrypted message. Asymmetric encryption is mostly used when there are 2 different endpoints are involved such as VPN client and server, SSH, etc.

1. ELIPTICURVE - HIỂU SÂU

Nguồn:

* <https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/>
* <https://vitalik.ca/general/2017/01/14/exploring_ecp.html>

+ Modern cryptography is founded on the idea that the key that you use to encrypt your data can be made public while the key that is used to to decrypt your data can be kept private.