- Tìm hiểu Hash ( Hàm băm) dung de lam j trong blockchain.

- sổ cái.

- thế nào được gọi là 1 cái genesis block.

- Tìm hiểu CHuỗi khối (BlockChain)

- Tìm hiểu Ethereum

- Tìm hiểu Nonce

https://blogtienao.com/ethereum/

<https://www.linkedin.com/pulse/what-nonce-hash-hashing-mining-blockchain-muhammad-saad-masood>

<https://phanlonghi.com/ethereum-la-gi/>

[https://support.remitano.com/gi%E1%BB%9Bi-thi%E1%BB%87u-chung/etherium-eth/ethereum-eth-la-gi](https://support.remitano.com/giới-thiệu-chung/etherium-eth/ethereum-eth-la-gi)

[https://vi.wikipedia.org/wiki/Ethereum#M%C3%A1y\_%E1%BA%A3o\_Ethereum](https://vi.wikipedia.org/wiki/Ethereum#Máy_ảo_Ethereum)

<https://www.youtube.com/watch?v=X9nnIPBSO_k>

https://quantrimang.com/blockchain-la-gi-bong-bong-hay-cuoc-cach-mang-thuc-su-sau-internet-143099#mcetoc\_1bvf2kgf43

<https://www.youtube.com/watch?v=vgHVQ0rQaAc>

----------------------------------------------------------------------------------------------------------

1. **Tìm hiểu về Ethereum:**
2. **Khái niệm**



* Ethereum là một nền tảng điện toán có tính chất phân tán công cộng, mã nguồn mở, dựa trên công nghệ chuỗi khối Blockchain. Đặc trưng của Ethereum là hợp đồng thông minh SmartContract (nó tập trung vào các mạng như SmartContract, nhận diện vân tay ). Khả năng tự đưa ra điều khoản và thực thi thỏa thuận một cách chính xác của hệ thống máy tính mà không hề ngừng nghỉ, chịu sự tác động hay gian lận của bên thứ ba.
* Ethereum (ETH) không chỉ là một đồng tiền tệ mà nó còn là nền tảng tạo ra nhiều ứng dụng khác thông qua các ngôn ngữ lập trình của mình.
* Ethereum cũng cung cấp một đơn vị tiền mã hoá gọi là ETH. Có thể đựơc chuyển giữa các tài khoản và sử dụng để trả phí giao dịch hay dịch vụ tính toán trên mạng Ethereum.
* Ethereum đã được ra đời cuối 2013 bởi **Vitalik Buterin,** một nhà nghiên cứu tiền mã hóa và nhà lập trình.
* Việc phát triển Ethereum được tài tài trở qua hình thức tài trở đống băng, và đã nhanh chống thu hút được số tiền 156 triệu USD,
* Mặc dù giá trị của Ethereum có giá trị thấp hơn đồng tiền Bitcon, nhưng loại tiền ảo này được đánh giá có tiềm năng rất lớn nhờ những ưu điểm thời gian tạo khối và tiến hành giao dịch nhanh hơn, độ bảo mật cao và lượng.
* Ethereum không bị giảm giá trị trong các năm. Bên cạnh đó không chỉ là tiền ảo, Ethereum còn có thể tạo ra thị trường trực tuyến cho phép người dùng dễ dàng mua bán, trao đổi . Với những đặc tính này, Ethereum được coi là mục tiêu hấp dẫn với nhiều nhà đầu tư

2. Lợi ích của Ethereum

* Vì mạng Blockchain Ethereum được vận hàng bởi hàng ngàn máy tính trên khắp thế giới, các ứng dụng có thể được vận hàng nhờ công suất tính toán của một mạng lưới máy tính toàn cầu đồ sộ.
* Một trong những vấn đề với mạng lưới Bitcoin là, dù mạng này mạnh hơn cả những siêu máy tính hàng đầu thế giới cộng lại nhưng công suất xử lý của nó lại bị lãng phí vào việc tạo ra những số ngẫu nhiên để thêm các khối vào Blockchain.
* Ethereum đưa toàn bộ các máy tính trong mạng lưới kết nối lại với nhau và công suất xử lý của chúng lên mức hiệu dụng cao hơn. Từ đó, giúp các lập trình viên tạo ra nhiều ứng dụng vận hàng nhờ công xuất xử lý gộp của mạng lưới cùng công nghệ Blockchain. Các lập trình viên không cần tạo lập Blockchain của riêng họ và kết nối máy tính vào đó. Ethereum đã xây dựng mạng lưới các máy tính trên Blockchain Ethereum.
* Vitalik Buterin, người sáng lập Ethereum, đã tạo ra một cách tiếp cận độc đáo để phát triển [Blockchain](https://phanlonghi.com/7-cach-blockchain-co-the-bao-ve-moi-truong-va-ngan-can-viec-bien-doi-khi-hau/), EVM. Máy ảo Ethereum (EVM) là một phần mềm hoàn chỉnh Turing chạy trên Blockchain Ethereum. Do đó, thay vì phải xây dựng blockchain riêng biệt cho mọi ứng dụng, các nhà phát triển có thể đơn giản sử dụng mạng Ethereum hiện có và chạy ứng dụng của sự lựa chọn.
* Nền tảng Ethereum còn có máy ảo Ethereum và ngôn ngữ lập trình Solidity. Solidity có thể được sử dụng để sáng tạo nên những ứng dụng phi tập trung hoặc các hợp đồng thông minh mà sau đó được Máy ảo Ethereum thông dịch và vận hành trên Blockchain.

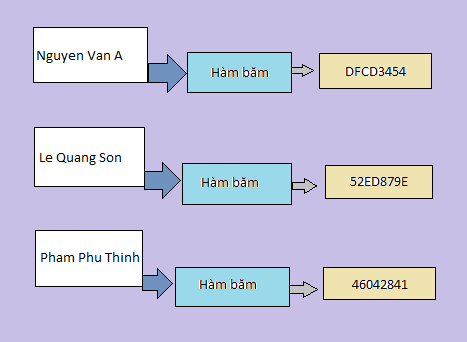
3. Những rủi ro khi giao dịch Ethereum

Vì toàn bộ giao dịch Ethereum đều phải thông qua mạng Internet khiến cho vấn đề an toàn đảm bảo uy tín khi mua bán trở thành một vấn đề vô cùng quan trọng. Những sai sót trong giao dịch, những lỗi bảo mật thông tin sẽ tạo điều kiện cho tội phạm lừa đảo hoặc các hacker khai thác để chiếm đoạt tài sản. Chính vì vậy các nhà đầu tư phải tìm cho mình được một nơi cung cấp, *mua bán Ethereum an toàn* để đầu tư. Đối với những người mới nên ưu tiên thiết lập giao dịch với bạn bè, người thân hoặc các địa chỉ uy tín có tiếng trên thị trường.

**II. Tìm hiểu Hash Function(Hàm Băm)**

1. Khái niệm

* Hash function (hàm băm): tạo ra giá trị băm cho các tương ứng với dữ liệu đầu vào.
* Giá trị băm được xem như là một khóa để phân biệt giữa các dữ liệu đầu vào.
* Mục đích của hàm băm là từ một dữ liệu đầu vào (input) với dung lượng bất kỳ nó sẽ mã hóa dữ liệu này về một dữ liệu khác với dung lượng nhất định



- Tuy nhiên vẫn còn xảy ra hiện tượng trùng khóa khi sử dụng hàm băm.

* Hàm băm thường được dùng trong bảng băm.

-Bảng băm (hash table): là một loại cấu trúc dữ liệu mà mỗi phần tử trong bảng băm là một cặp (khóa, giá trị).

-Hàm băm (hash function): có thể thự hiện nhanh.

-Độ phức tạp của thuật toán là O(n).

-Hàm băm (hash function): dùng để xây dựng cấu trúc dữ liệu.

1. **Hàm băm mật mã (cryptographic hash functions).**

-Là một hàm băm có tính bảo mật, có thể sử dụng hàm băm mật mã trong bảo mật thông tin.

-Các hàm băm thông dụng nhất là MD5 và SHA.

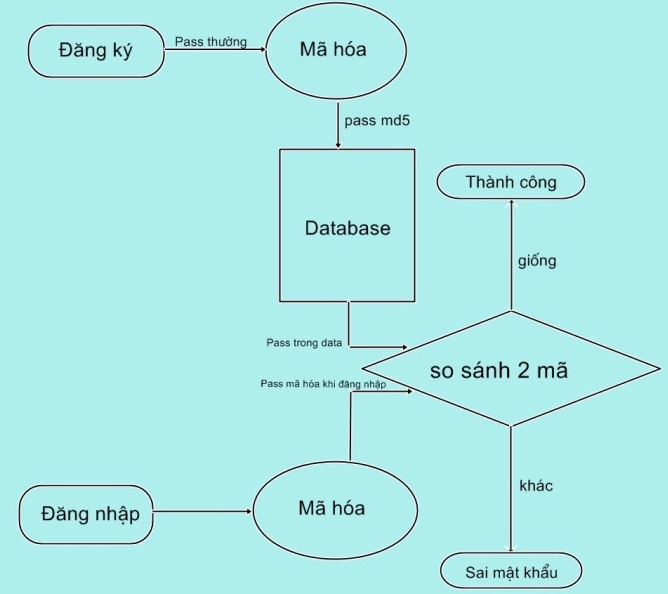
1. MD5

-MD5 là hàm băm mật mã được sử dụng phổ biến với giá trị hash là 128bit. Được thiết kế bởi Ronald Rivest vào năm 1991.

-MD5 được dùng trong các ứng dụng bảo mật cũng như dùng để kiểm tra tính toàn vẹn của thông tin, lưu trữ mật khẩu.

-Giá trị sau khi băm qua MD5 là di nhất và không thể suy ngược lại giá trị ban đầu hay nói một cách khác là hàm băm MD5 không có phần giải mã.

-Ví dụ: Hệ thống sử dụng MD5 để băm mật khẩu của người dùng trước khi lưu vào database. Khi người dùng đăng nhập thì mật khẩu của người dùng nhập trên giao diện đăng nhập sẽ được băm và so sánh với mật khẩu trong database xem có hợp lệ hay không.



1. SHA.

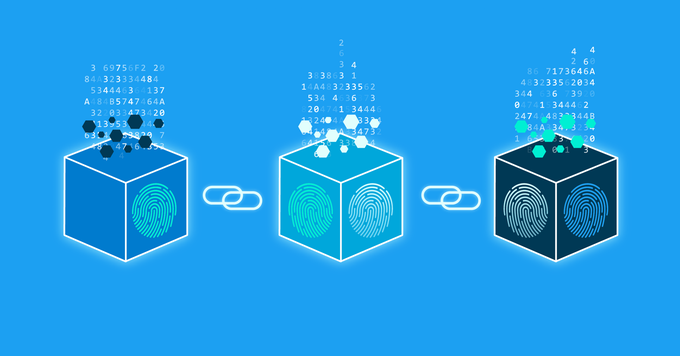
-SHA là giải thuật băm an toàn. SHA là năm giải thuật được chấp nhận bởi FIPS dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi.

-Năm giải thuật SHA là:

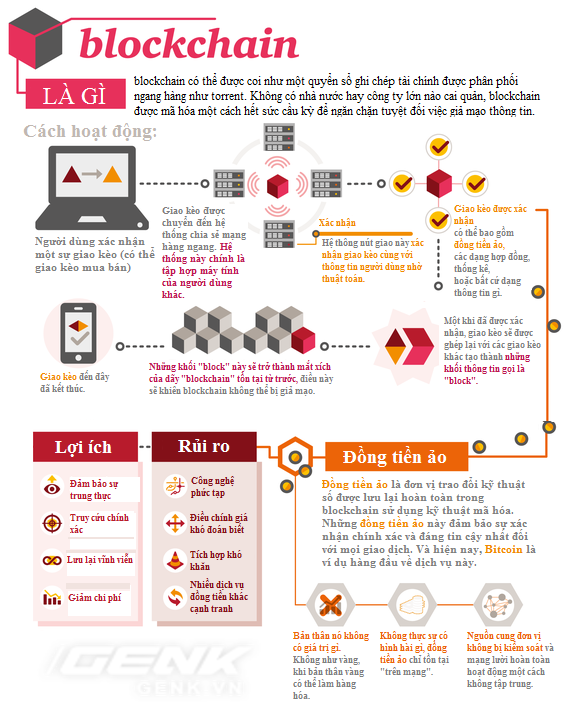
* SHA-1 trả về kết quả 160 bit.
* SHA-224 trả về kết quả 224 bit.
* SHA-256 trả về kết quả 256 bit.
* SHA-384 trả về kết quả 384 bit.
* SHA-512 trả về kết quả 512 bit.
* SHA được phát triển bởi cục an ninh quốc gia Mỹ (National Security Agency hay NSA) và được xuất bản thành chuẩn của chính phủ Mĩ bởi viện công nghệ và quốc gia Mỹ (National Institute of Standards and Technology hay NIST).
* SHA-224, SHA-256, SHA-384, SHA-512: được gọi chung là SHA-2
* SHA-1 được sử dụng rộng rãi trong nhiều ứng dụng và giao thức an ninh khác nhau. SHA-1 được xem là giải thuật thay thế cho MD5.
* Hiện nay thì SHA-1 không còn được xem là an toàn nữa. Ba nhà mật mã học người Trung Quốc đã phát triển thành công một giải thuật dùng để tìm được hai đoạn dữ liệu nhất định có cùng kết quả băm tạo ra bởi SHA-1.

**III. Tìm hiểu về BlockChain**

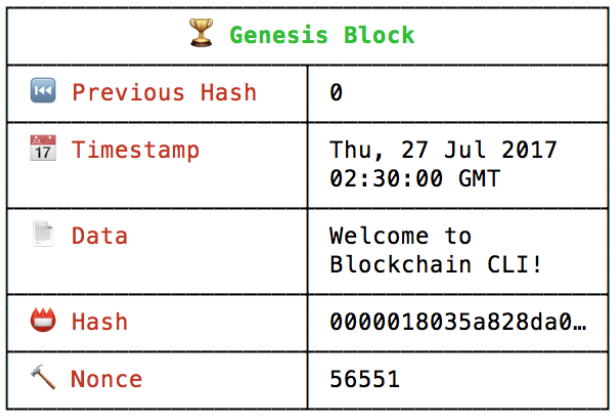
1.Khái niệm



* Blockchain là hệ thống lưu trữ thông tin trên mạng máy tính cá nhân(database) giúp cho dữ liệu không chỉ được phân phối đến người dùng mà còn được phân nhánh.
* Nó giống như là một cuốn sổ cái.
* Nhưng điều đặc biệt của BlockChain đó là cở sở dữ liệu này được phân phối phi tập trung trên mạng Internet. Điều đó có nghĩa là cơ sở dữ liệu này được trải khắp thế giới, được sở hữu bởi tất cả máy tính trong mạng lưới ngang hang. Không có một máy chủ tập trung nào host cơ sở dữ liệu này. Một khi dữ liệu được ghi vào cuốn sổ cái này, không ai có thể xóa, hay thay đổi nó. Nó không thể bị hack.
* BlockChain giúp mọi người tin tưởng được nội dung của cơ sở dữ liệu(cuốn sổ cái) mà không cần biết những người tham gia khác vào mạng lưới ngang hang này là ai, ai đang viết vào cơ sở dữ liệu này…
* BlockChain giúp người tham gia đạt được sự thỏa thuận về thông tin mà không cần thông qua một bên thứ ba.
* Mọi thông tin, mọi giao dịch đều được ghi lại trong các **block**, đều gọi là **Khối**. Một khối sẽ chứa các thông tin sau:
* Index: Chỉ số vị trí của block trong BlockChain.
* Hash: Mã hash là sự kết hợp của các thông tin như dữ liệu, mã hask của các khối trước đó, index.
* Previous hask: Mã hask của khối trước đó.
* Data: Thông tin chứa trong Block, như thông tin giao dịch, hợp đồng…
* Timestamp: Thời gian Block được thêm vào BlockChain.
* Nonce: Một chuỗi (tùy ý) được thêm vào hàm băm của block để thist lập bằng chứng xử lý, yêu cầu đưa các node cạnh tranh đi đến một thảo thuận chung để chấp nhận block nào trong bước tiếp theo của một block phát triển.
* Loại dữ liệu được lưu trữ bên trong một khối phụ thuộc vào loại BlockChain(Vào vấn đề mà BolckChain đang giải quyết. )
* Điểm nổi bật của BlockChain là đảm bảo rằng các khối đã được ghi lại mọi thông tin thì sẽ không bao giờ bị giả mạo hoặc thay đổi bởi bất kì ai.
* Mỗi một khối mới xuất hiện, cả mạng lưới sẽ biết ngay lập tức. Tính năng này đảm bảo tính công bằng và minh bạch cho cả hệ thống.
* Một khối cũng gần giống như một cơ sở dữ liệu nhưng nó được công khai.
* BlockChain lưu giữ thông tin trên một mạng gồm hàng trăm hàng nghìn máy tính cá nhân khiến cơ sở dữ liệu không chỉ phân cấp mà còn phân tán độc lập. Khi dữ liệu được lưu vào một khối thì nó được mã hóa một cách phức tạp để ngăn chặn việc giả mạo thông tin.
* Hệ thống BlockChain không có máy chủ, khả năng truyền tải dữ liệu mà không đòi hỏi trung gian để xác nhận thông tin. Không có quyền sở hữu bởi 1 ai,mà mọi người có trong hệ thống đều có quyền hạn tương đương và giúp vận hành hệ thống.
* BlockChain có tính bảo mật cao, Vì không có máy chủ và dữ liệu được phân tán độc lập nên khi một máy bị tấn công thì chỉ có máy đó bị ảnh hưởng, phần còn lại của hệ thống vẫn được bảo toàn.



Genesis block (khối “nguyên thủy”):Mỗi blockchain sẽ bắt đầu với block Genesis. Mỗi khối trên Blockchain phụ thuộc vào khối trước đó.



**Sổ cái:**

* Sổ cái của blockchain sử dụng mạng lưới peer-to-peer, có tính phân quyền. (mạng lưới ngang hàng peer-to-peer tức là các node truyền thông tin ngang nhau. Mỗi điểm note đều có thể biết ở đâu diễn ra hoạt động gì và chúng được thực hiện như thế nào, thông tin minh bạch hoàn toàn)
* Mọi người đều có quyền ghi thông tin và sử dụng chúng.
* Sổ cái của blockchain cho phép người tham gia hệ thống có thể dùng chung thông tin.
* Tính phân quyền của blockchain làm cho các thông tin được thực hiện trong mạng lưới được rõ ràng và minh bạch hơn.
* Cơ sở dữ liệu phân tán chính là điểm khác biệt của blockchain. Đây cũng chính là đặc tính riêng biệt và quan trọng nhất của công nghệ blockchain.
* Một sổ cái phân tán là một cơ sở dữ liệu được tổ chức và cập nhật một cách độc lập bởi từng cá nhân tham gia (hay node) trong một mạng lớn. Sự phân phối này là độc nhất: các bản ghi không được truyền đến các node khác, mà thay vào đó là được xây dựng độc lập và tổ chức bởi từng node. Nghĩa là, mỗi node trên mạng xử lý từng giao dịch, đưa ra kết luận của riêng mình và sau đó bỏ phiếu cho những kết luận này để chắc chắn rằng đa số đồng thuận với kết luận đó. Khi đã đồng thuận, sổ cái phân tán sẽ được cập nhật, bản ghi phổ biến nhất sẽ trở thành bản ghi chính thức trên sổ cái.

**Hàm băm (hash fuction) sử dụng trong blockchain**

1. **Blockchian.**

**-**  Hàm băm được sử dụng để xác định nội dung duy nhất của một block.

**-**Sử dụng thuật toán SHA-256 từ tất cả các thành phần của block trước đó:

**+** Hàm băm

+ Index

+ Data

+ Timestamp

+ Nonce (Là một số được sử dụng để tìm một hash hợp lệ)

**-**Thuật toán SHA-256 sinh ra các mã băm 256-bit kích thước cố định. Nó sẽ tính toán một hàm hash duy nhất, cho các giá trị input. Các giá trị input sẽ trả lại cùng một hash.

**-**Một mã băm bí mật dùng phương thức mã hóa nhằm bảo vệ dữ liệu của mình một cách an toàn nhất.

**-**Mã băm được tạo ra luôn có cùng độ dài.

**-**Nếu bạn thay đổi một ký tự trong chuổi ban đầu thì mã băm cũng sẽ bị thay đổi theo.

**-**Mã băm được tạo ra một cách ngẫu nhiên mà không cần quan tâm đến dữ liệu đầu vào.

**-**Hàm băm không có hàm giải mã nên bạn sẽ không thể biết được dữ liệu ban đầu trừ khi bạn biết dữ liệu ban đầu.

**-**ví dụ: sử dụng thuật toán SHA-256 đển băm các dữ liệu đầu vào khác nhau.

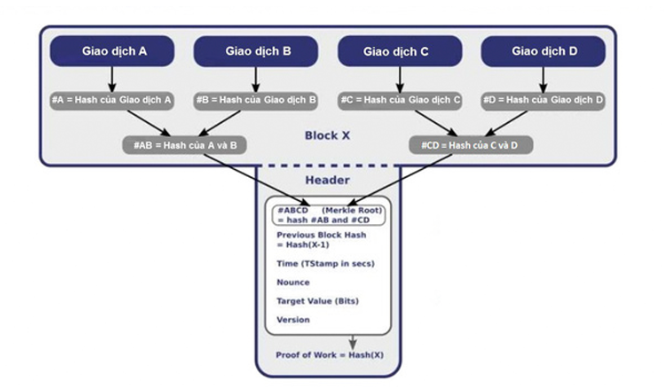
* Mã băm của từ “PhamPhuThinh” với chữ P, T viết hoa (SHA256: PhamPhuThinh)
* 43C4297F14533B91BD11D4106A1AA46DF9253634BD56A6916148315C63B85975
* Mã băm của từ “PhamPhuThinh” với chữ T viết hoa (SHA256: phamphuThinh)
* 46BA1567C30644EDE0E91DE651231D7D05663390A89CB1F5EC2766617D2FE715
* Mã băm của từ “PhamPhuThinh” với chữ “Pham”, “Phu” và “Thinh” viết cách (SHA256: Pham Phu Thinh):
* EBD374853B60EA664FFEA785BC98D4C0A50708DC4CF5BBA6216043C1D20286F5
* Mật mã băm với đoạn văn bản ngẫu nhiên: “JavaScript is the programming language of HTML and the Web. JavaScript is easy to learn This tutorial will teach you JavaScript from basic to advanced”.
* 18160D6E22B0703DBC746A03FF44521869217EF1B2732E87C589C4B32744B5D7
* Qua các ví dụ trên chúng ta nhận thấy SHA-256 sẽ tạo ra chuỗi sau khi băm cố định là 256 bit mà không cần quan tâm đến dữ liệu đầu vào.
* Hàm băm giúp tăng cường tính bảo mật cho tất cả các block.

1. **Giao dịch mã băm trong Blockchain.**

**-** Khối đầu tiên trong Blockchain là khối 0, hay còn gọi là khối nguyên thủy (Genesis Block).

**-Khối 0:** khối đầu tiên giao dịch chứa nội dung.

* “Thịnh nhận 100 bitcoin Sơn nhận 50 bitcoin Nam nhận 10 bitcoin Hải nhận 10 bitcoin”.
* Mã băm 0 = 0000641727781545e50c0235823c9ae0785d419499cc5a5dcdff2332a53f0f7f
* Đầu tiên thông tin về giao dịch sẽ được tạo ra và đưa vào trong một khối(block).
* Sau đó thông tin này được mã hóa bằng thuật toán SHA-256.
* kết quả sau khi được mã hóa có độ dài 256 bit tương đương với 64 ký tự bao gồm chữ và số.
* Kết quả này sau đó tiếp tục được ghép với kết quả mã hóa của một giao dịch khác kế tiếp bằng thuật toán SHA-256. Ghép các kết quả mã hóa lại với nhau cho đến khi còn lại hai hashing của các giao dịch trong block này sau khi mã hóa.
* Sau đó:  hai kết quả này được ghép lại và mã hóa để tạo thành một kết quả hashing sau cùng.



* Kết quả hashing sau cùng này được ghép cùng các thông tin khác trong block (cây nhị phân Merkle), bao gồm:
* Kết quả hashing của block trước đó.
* Thời gian khởi tạo block.
* Tham số chạy Nounce. Nonce là một số được dùng để tạo ra mã băm (hash) hợp lệ theo yêu cầu hệ thống Blockchain.

-**Khối 1:** Giao dịch khối thứ 2:

* Nội dung: “Thịnh gửi Sơn 100 bitcoin, Sơn gửi Nam 20 bitcoin”.
* Mỗi giao dịch sẽ được chủ tài khoản gửi Bitcoin xác nhận bằng một khóa cá nhân. Mạng lưới sẽ không thể thấy được khóa cá nhân nhưng họ có thể kiểm nghiệm khóa cá nhân được cấp quyền gửi Bitcoin đã sử dụng:
* Khối sẽ còn chứa mã băm của khối trước.
* Mã băm 1: 0000ed29ee4097b79e194adb355b18c500a900ffb3a1670dec4673eac2abdd07
* Tham số Nonce: xxxxxx.
* Nhãn thời gian.

- **Khối 2:** Khối giao dịch thứ 3 chứa các giao dịch đã được xác nhận bên dưới, mã băm khối trước đó, nhãn thời gian cùng tham số Nonce:

* Nội dung:” Sơn gửi Nam 30 bitcoin Thịnh gửi Hải 50 bitcoin”.
* Mã băm 2: 0000d5cada28a39cb0511cc871d550fe0c4ba704a93ad33db37936c6ab40caf
* Liên kết các khối này lại, chúng ta có một **Blockchain.**

Tìm hiểu Nonce:

* “Nonce” là một trường dài 32 bit (4 byte), giá trị được thiết lập để hash của block sẽ bao gồm một chuỗi các bit = 0 chạy ở đầu.
* Bất kỳ thay đổi nào đối với dữ liệu block (như nonce) sẽ dẫn tới block hash bị thay đổi hoàn toàn. Không thể dự đoán được tổ hợp bit nào sẽ cho ra một hash hợp lệ, cho nên rất nhiều nonce khác nhau sẽ được thử, với mỗi giá trị nonce khác nhau, hash sẽ được tính toán lại cho đến khi hash cuối cùng chứa số lượng bit 0 thích hợp. Số lượng bit 0 thích hợp được đánh giá dựa trên difficulty.
* Hash sinh ra phải có giá trị nhỏ hơn difficulty hiện tại và do đó phải chứa vài bit 0 ở đầu để nhỏ hơn yêu cầu đánh giá đó. Quy trình tính toán lặp đi lặp lại này đòi hỏi thời gian và công sức. Do đó block mới với giá trị nonce đúng sẽ cấu thành nên proof of work.