UIT VNUHCM University of Information Technology

CHƯƠNG 6:
ĐẠI CƯƠNG VỀ BLOCKCHAIN

Khoa Khoa học và kỹ thuật thông tin
Bộ môn Thiết bị di động và Công nghệ Web

Nội dung

1. Khái niệm block chain.
2. Các thành phần của block chain.
3. Đặc điểm của Block chain.
4. Cơ chế đồng thuận.
5. Ứng dụng.

Khái niệm về Block chain

Đặt vấn đề

- Các giao dịch chuyển tiền giữa 2 cá nhân X (người gửi) và Y (người nhận) trên hệ thống ngân hàng hiện tại có đặc trưng sau.
- Cần một độ trễ nhất định để Y có thể nhận được tiền từ X.
- X hoặc Y cần đóng phí cho ngân hàng.
- **Người quản trị CSDL thấy được, thậm chí sửa được giao dịch này.**

➔ Làm sao để khắc phục vấn đề này.

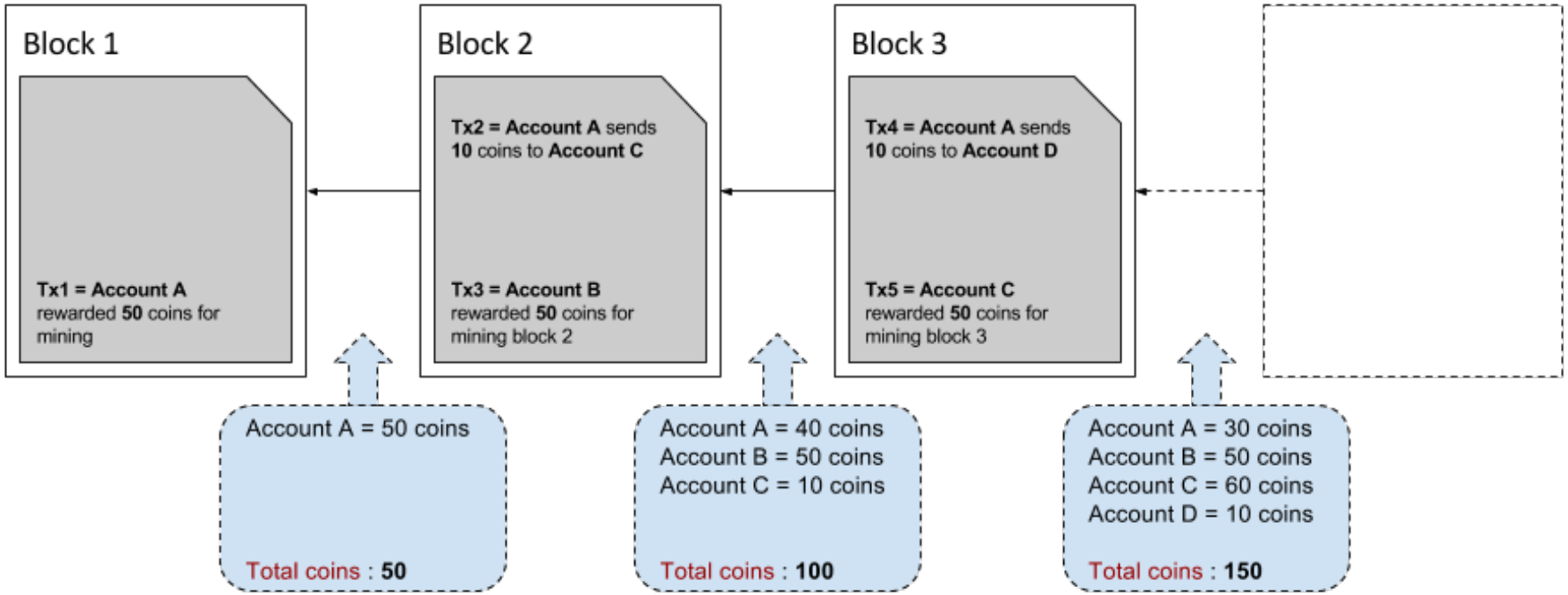
Khắc phục

- Xét ví dụ sau: bao gồm các giao tác chuyển tiền giữa 4 tài khoản A, B, C, D, và phần thưởng của hệ thống do A, B, C tạo ra các khối mới.
- Gt1: A được thưởng 50đ do tạo ra được khối 1 (kết quả chạy thuật toán). Gt2: A chuyển 10đ cho tài khoản C; Gt3: B được thưởng 50đ do tạo ra khối 2; Gt4: A chuyển 10đ cho tài khoản D; Gt5: C được thưởng 50đ do tạo ra khối 3;
- Nếu các giao dịch này là hợp lệ, một cuốn sổ cái sẽ ghi lại các giao tác trên, sổ cái này được phân bổ trên các node. Mỗi thao tác chuyển tiền tạo thành 1 khối, tất cả có 3 khối hình thành theo đúng thứ tự phát sinh theo thời gian và chúng tạo thành các mối liên kết .

Block chain

- 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 một mã thời gian và dữ liệu giao dịch.
- Blockchain được thiết kế để chống lại việc thay đổi của dữ liệu: Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được nó.

Ví dụ


Block 1
Tx1 = Account A rewarded 50 coins for mining
Block 2
Tx2 = Account A sends 10 coins to Account C
Tx3 = Account B rewarded 50 coins for mining block 2
Block 3
Tx4 = Account A sends 10 coins to Account D
Tx5 = Account C rewarded 50 coins for mining block 3
Account A = 50 coins
Total coins : 50
Account A = 40 coins
Account B = 50 coins
Account C = 10 coins
Total coins : 100
Account A = 30 coins
Account B = 50 coins
Account C = 60 coins
Account D = 10 coins
Total coins : 150

Phân loại blockchain

Các blockchain công cộng

- Các blockchain ban đầu như Bitcoin, Etherium, EOS, Litecoin, ... đều là các blockchain công cộng

Các blockchain riêng tư

- Của các cá nhân hoặc tổ chức, ví dụ bankchain (https://www.multichain.com/). Nó chỉ cho phép một số người tham gia, có sự kiểm soát về phân quyền. Gồm các quyền: được xem dữ liệu trên blockchain; quyền ghi dữ liệu giao dịch lên blockchain. Các mã nguồn hoặc thông tin kết nối đến hệ thống sẽ được giữ kín.
- Như vậy, tính chất minh bạch về dữ liệu không còn giữ như phiên bản ban đầu của blockchain.

Các blockchain của hiệp hội

- Đây là các blockchain riêng của nhiều tổ chức hợp lại để cùng khai thác và chia sẻ dữ liệu blockchain, như r3 (https://www.r3.com/), EWF (http://energyweb.org/).

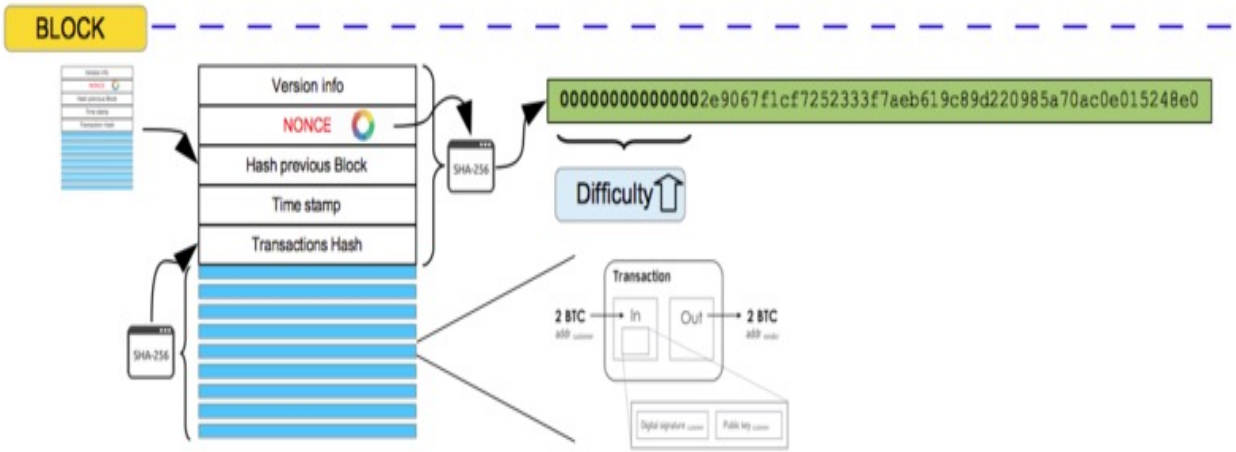
Các thành phần của Block chain

Thành phần của block chain

- Khối (block).
- Giao dịch (transaction).
- Hàm băm (hash function).
- Khoá (key).

Cấu trúc 1 khối

– Mỗi khối có các trường cơ bản sau: danh sách các giao dịch (dữ liệu), nhãn thời gian, Previous Hash, số Nonce, phiên bản blockchain.



Cấu trúc 1 khối (2)

- Danh sách giao dịch: chứa dữ liệu chi tiết của các giao dịch. Số các giao dịch trong một khối được qui định trong từng phiên bản của blockchain.
- Hàm hash các giao dịch (transactions hash) : được tạo ra theo cách sau
  + Dùng hàm băm để mã hóa từng giao dịch (các Txi).
  + Gộp 2 giao dịch thành 1 cặp, dùng hàm băm để tạo kết quả trung gian. Công việc này lặp lại cho đến khi được một kết quả cuối (root hash hoặc transaction hash). Nếu số giao dịch là lẻ trong một khối, thì giao dịch cuối được tính với chính nó.

Cấu trúc 1 khối (3)

- Hash: chứa mã băm của các thành phần gồm: *hàm hash của các dữ liệu của các giao dịch+mã băm của block kế+số thứ tự khối+ nonce+nhãn thời gian*.
- Previous Hash: Chứa kết quả của của hàm băm của block liền trước, nhờ vậy các khối tạo thành xâu liên kết với nhau giống 1 chuỗi.

Cấu trúc 1 khối (4)

Ngoài ra, 1 khối còn chứa các thuộc tính sau:

- **Nhãn thời gian**: tính tới giây, bắt đầu từ 1/1/1970, cho biết thời gian 1 khối mới được khởi tạo.
- **Nonce** (4 byte): Là một số bất kì, nó được người tạo khối phát hiện, thông qua việc chạy các lần lặp các giá trị từ 0 đến 2^32 nhằm giải 1 bài toán mã hóa thỏa điều kiện cho trước.
- **Phiên bản blockchain**: cho biết phiên bản của blockchain đang sử dụng.
- **Số thứ tự**: Các khối sẽ được đánh dấu bằng các số thứ tự liên tục.
- Kích thước tối đa của mỗi khối khoảng từ vài MB đến vài trăm MB được qui định rõ trong từng phiên bản.

Phân loại các node (1)

- **Hot node** là những node có chứa dữ liệu và chủ động liên kết đến các node khác trên hệ thống. Chúng còn là những nơi xử lí dữ liệu chính của Blockchain. Hot node chia làm 2 loại: Full node và Light node
- **Full node** là node chứa bản sao đầy đủ các dữ liệu Blockchain. Chỉ có các node này mới trực tiếp ghi dữ liệu vào Blockchain. Các node này hạt nhân của cả hệ thống Blockchain, chúng đảm bảo tính toàn vẹn dữ liệu của Blockchain.

Phân loại các node (2)

- **Light node** là giải pháp để tiết kiệm tài nguyên của hệ thống. Light node chỉ chứa một phần dữ liệu của Blockchain, thường chỉ chứa một phần dữ liệu liên tục từ quá khứ gần đến hiện tại. Một light-node cần được liên kết đến ít nhất một full-node để nhờ nó mà nó có thể thêm một giao dịch vào hệ thống.
- **Cold node** là những node không chứa dữ liệu của hệ thống. Nó kết nối đến các hot node để đọc dữ liệu. Khi cần ghi dữ liệu, nó sẽ gửi đến các hot node để nhờ xử lí và ghi dữ liệu vào Blockchain. Các cold node chỉ dùng để chứa thông tin tài khoản của người dùng. Cold node là một giao diện tương tác của người dùng đến Blockchain nên việc tiêu hao tài nguyên được giảm đáng kể

Giao dịch

- Giao dịch trong blockchain tạm chia làm 3 loại: giao dịch thuộc về khối đầu tiên của Blockchain; giao dịch thưởng cho những người tạo ra được khối mới; giao dịch thông thường.
- Giao dịch thuộc về khối đầu tiên của Blockchain sẽ được chèn vào trong mã nguồn của Blockchain tại khối đầu tiên của blockchain. Trong các ứng dụng tiền ảo, nó được dùng để tạo một số lượng tiền có hạn định trong hệ thống Blockchain ban đầu.
- Giao dịch thưởng cho những người dùng đã tạo ra khối mới do hệ thống Blockchain tạo tự động và sẽ chuyển số tiền thưởng cho người tạo ra khối mới.
- Giao dịch thông thường là những giao dịch được tạo bởi những người dùng trong hệ thống khác với 2 loại giao dịch kể trên.

Đầu vào của giao dịch (1)

- Với giao dịch bình thường thì dữ liệu đầu vào gồm:
  + Giá trị của hàm băm của một giao dịch đã có kề trước, nó đóng vai trò như là một con trỏ để liên kết giữa 2 giao dịch liền kề.
  + Khóa công khai và chữ kí của người ghi. Khóa công khai và chữ kí sẽ được kiểm chứng danh tính. Khi thực hiện các bước mã hóa thì khóa công khai, chữ kí, thông tin người dùng từ đầu ra của giao dịch trước phải khớp nhau.

Đầu vào của giao dịch (2)

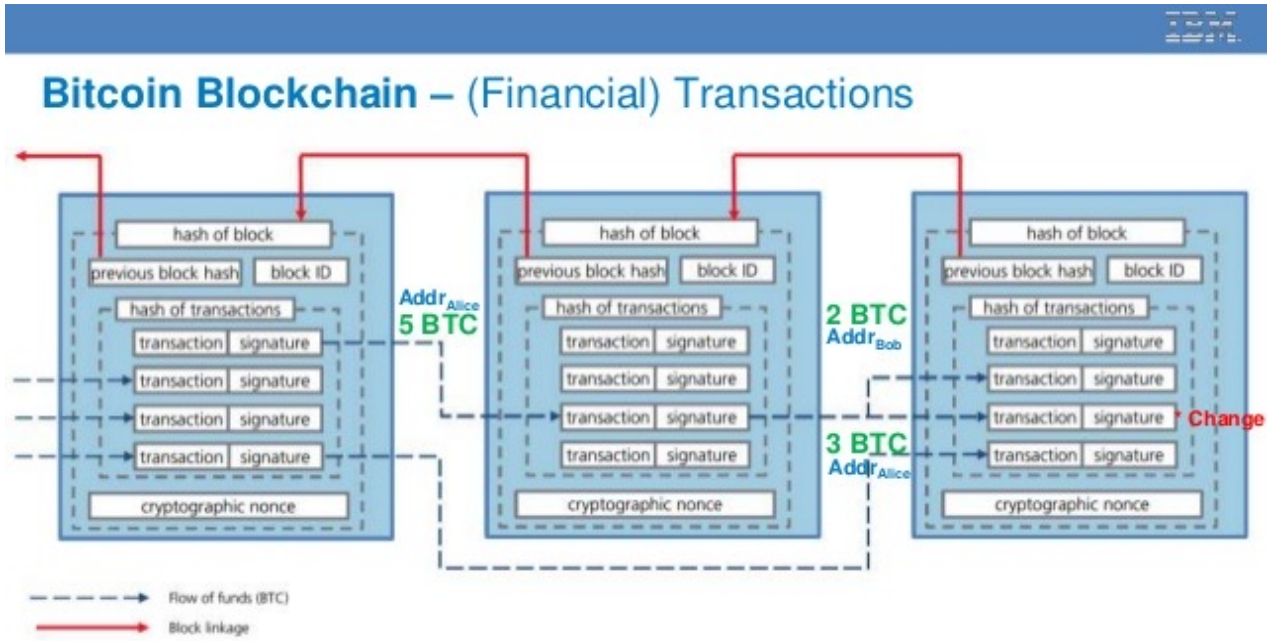
- Với hai loại giao dịch còn lại thì đầu vào chỉ có một chuỗi dữ liệu đặc biệt. Nó đánh dấu để mang hàm ý: một giao dịch không có dữ liệu đầu vào.
- Trong giao dịch thưởng cho những người tạo ra được khối mới sẽ có một chuỗi kí tự, nó vô nghĩa, hàm ý đánh dấu đây là một giao dịch thưởng.

Dữ liệu đầu ra của giao dịch

Dữ liệu đầu ra của giao dịch gồm có 2 dạng:

- Trong ứng dụng tiền ảo, giao dịch chuyển tiền gồm có: khóa công khai của người nhận và số tiền được nhận. Và dữ liệu đầu ra này được dùng làm dữ liệu vào cho một giao dịch khác và chỉ được dùng đúng một lần. Một người chỉ có thể gửi số tiền nhỏ hơn hoặc bằng số tiền họ có.
- Đầu ra trong một giao dịch lưu trữ chỉ bao gồm dữ liệu lưu trữ dưới dạng chuỗi cơ số 16 được ghi vào Blockchain và không có thêm thông tin gửi tiền. Dữ liệu lưu trữ có thể chứa địa chỉ nhận hoặc không. Đầu ra này không thể được dùng làm đầu vào cho một giao dịch khác.

Ví dụ về thực hiện 1 giao dịch tài chính



* The process of unlocking and spending funds, you expose the private key – To preserve unused funds (BTC) the client generates a new Bitcoin address, and sends the difference back to this address. This is known as **change**.

UBS - Global banks: Is FinTech a threat or an opportunity? – July 2016

Hàm băm (hash)

- Hash là một hàm toán học, nhằm mã hóa dữ liệu (a) đầu vào. Dữ liệu a là một chuỗi ký tự có độ dài bất kỳ. Đầu ra của hàm băm là 1 chuỗi dữ liệu có độ dài cố định. Hàm băm có chi phí thời gian thực hiện thấp và có độ phức tạp ít - hàm hash trên một chuỗi n-bit, có độ phức tạp của thuật toán là O(n).
- Blockchain xây dựng trên lý thuyết của mật mã học để tạo và kiểm soát các liên kết dữ liệu trong hệ thống.
- Nó sử dụng các phương thức tính toán trong ngành mật mã học để hoạt động. Các ứng dụng giao dịch tiền tệ trên nền blockchain như: bitcoin, enthereum … còn được gọi là tiền mật mã.

Đặc điểm hàm băm trong blockchain

- Không bị đụng độ (Collision resistance): không thể tìm được 2 chuỗi đầu vào x và y khác nhau (x≠y) nhưng H(x)=H(y).
- Che dấu dữ liệu một chiều (hiding one-way): nếu giả sử biết y (H(x)=y), thì không thể tìm được x. Để thỏa đặc điểm này, hàm hash sẽ dùng thêm một giá trị bí mật r, với r được chọn ngẫu nhiên, để việc phối hợp giữa x và r làm cho việc đi tìm là khó khả thi x.
- Thân thiện với Puzzle (puzzle-friendliness): Cho một giá trị z với độ dài n bit và một giá trị được chọn ngẫu nhiên r, rất khó tìm được giá trị x để mà H(r||x)=z trong một khoảng thời gian nhất định, thường là 2^n giây.

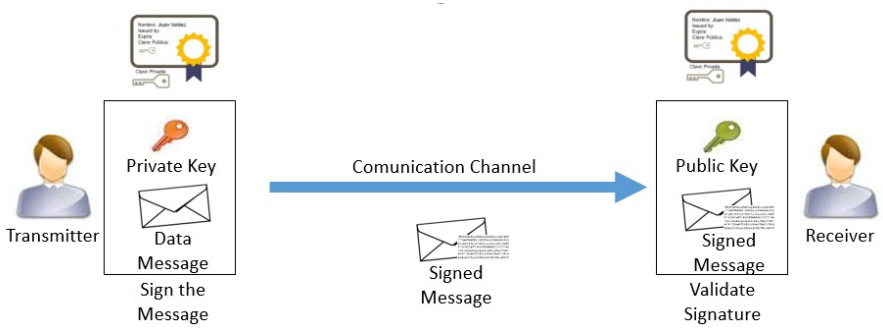
Các hàm hash thường dùng

- **SHA-256** là một hàm hash nhận một chuỗi có độ dài tùy ý và mã hóa thành dữ liệu đầu ra dạng hex với độ dài 256 bit.

- **RIPEMD-160** là một dạng hàm hash nhận vào một chuỗi dữ liệu có độ dài tùy ý và mã hóa thành 1 chuỗi dữ liệu đầu ra dạng hex với độ dài 160 bit.

Hệ mã khoá công khai

- Gồm 2 thành phần chính:
  - + Khoá bí mật (private key).
  - + Khoá công khai (public key).
- Hệ mã khoá công khai nổi tiếng nhất được sử dụng hiện nay là RSA, do Ronald Rivest và các đồng sự phát minh năm 1977 tại MIT.



Ronald Rivest

Các cơ chế đồng thuận

Cơ chế đồng thuận PoW (Proof of Work)

- Cơ chế do chính tác giả của hệ thống blockchain đặt ra. Cơ chế này chỉ cho phép các node thành viên nào chứng minh được, bản thân đã tham gia vào hoạt động được qui định bởi blockchain, mới có thể ghi một giao dịch.
- Các thành viên cùng tham gia để giữ tính an ninh của dữ liệu trên hệ thống.
- Qui định trong PoW như sau: 1 bài toán được phát biểu chung cho các thành viên. Người nào giải đúng đáp số đầu tiên, người đó có quyền ghi lên sổ cái.
- Bài toán như sau: Cho biết điều kiện C, hãy tìm giá trị X, sao cho ghép nối X với 1 chuỗi biết S trước, nhờ vào hàm băm, cho ra giá trị Y, và Y thỏa C. Bài toán càng khó phụ thuộc vào điều kiện C. Và C là thay đổi theo thời gian, thông thương sau khi một số khối đã được sinh ra, C sẽ thay đổi nhằm tăng độ khó..

Cơ chế đồng thuận PoS (Proof of stake)

- Cơ chế này buộc người tham gia đề nghị ghi dữ liệu phải lấy số tiền trong tài khoản của bản thân ra đặt cược cho các thuật toán như trên (PoW).
- Số tiền đặt càng cao, thì bài toán giải càng dễ, nghĩa là xác suất tìm được đáp số càng cao. Người tham gia hệ thống đầu từ càng nhiều (nhiều cổ phần), thì khả năng người đó phá hệ thống của chính mình là càng nhỏ.
- Khi người tham gia đặt cược với chính cổ phần của mình, thì càng được khuyến khích sự trung thực, nếu không số cổ phần đó sẽ bị khóa.
- Điện năng tiêu thụ cho các thuật toán trong PoS cũng giảm đi đáng kể. Node tìm ra lời giải sẽ nhận phần thưởng từ tiền phí của các giao dịch.

Cơ chế đồng thuận PoA (Proof of Authority)

- Là cơ chế đồng thuận các node được xác định trước và được công bố danh tính sẽ thay phiên nhau tạo ra các khối để thêm vào Blockchain.
- Các node này được xem như Admin của hệ thống.
- Cơ chế đồng thuận PoA thường được sử dụng cho các Private Blockchain.

Ứng dụng

Yêu cầu của ứng dụng Block chain

- Một ứng dụng cơ sở dữ liệu triển khai trên công nghệ Blockchain là phù hợp khi người dùng muốn kiểm soát được dữ liệu của chính họ và không bị một bên thứ ba nào có thể thay đổi, tác động dữ liệu này.
- Blockchain còn phù hợp cho những hệ thống ứng dụng mà yêu cầu sự ổn định, bền vững của dữ liệu rất cao. Do sác xuất cùng một lúc, tất cả các node trong một mạng bị hư hỏng dữ liệu cùng 1 thời điểm gần như bằng không, đặc tính này của blockchain là hơn CSDL tập trung rất nhiều, và cao hơn CSDLPT khá nhiều. Đây là đặc tính nguyên thủy, phổ biến của Blockchain.

Một số ứng dụng

- Bầu cử: blockchain có thể ứng dụng cho việc bầu cử ở các cấp quốc gia, tỉnh thành, hoặc 1 tổ chức bất kỳ. Công nghệ này đảm bảo tính chính xác của phiếu bầu mà không sợ bị thay đổi chủ ý hoặc vô ý. Ngoài ra người dùng có thể ngồi tại nha để bỏ phiếu
- Chứng nhận quyền sở hữu: Do tính an toàn của dữ liệu trên blockchain, nên khi người A đăng ký quyền sở hữu 1 sản phẩm, nó đảm bảo không bị giả mạo hoặc chỉnh sửa bởi bất kỳ ai trong hoặc ngoài hệ thống

Một số ứng dụng (2)

- Chính phủ điện tử: hiện nay Estonia là quốc gia đi đầu về lãnh vực này, nhờ nó hàng năm Estonia tiết kiệm khoảng 2% GDP, cung cấp khoảng 4000 dịch vụ trên hệ thống. Bộ Khoa học và công nghệ Việt Nam hiện đang chủ trì dự án "chính phủ điện tử với công nghệ blockchain".
- Quản lý chuỗi cung ứng: 1 sản phẩm hoàn thiện A có thể có sự tham gia của nhiều nhà sản xuất cho các linh kiện hoặc từng nhóm nhỏ bộ phận. Blockchain có nhiệm vụ liên kết các nhà cung ứng, nhắm chứng thực cho sản phẩm của mình đến người tiêu dùng

Một số ứng dụng (3)

- Thanh toán quốc tế: với tính chất độ trên của giao dịch gần như bằng không; miễn phí và tính minh bạch của dữ liệu, các ứng dụng thanh toán quốc tế là phù hợp với công nghệ blockchain.
- Hợp đồng thông minh: Những giao dịch được thực hiện bằng các hợp đồng thông minh rất minh bạch, có thể dễ dàng truy xuất được và không thể bị can thiệp hoặc đảo chiều. Các điều khoản trong Smart Contract tương đương với một hợp đồng có pháp lý và được ghi lại dưới ngôn ngữ của lập trình.

TÀI LIỆU THAM KHẢO

1. Nguyễn Gia Tuấn Anh, Trương Châu Long, *Bài tập và bài giải SQL Server*, NXB Thanh niên (2005).
2. Đỗ Phúc, Nguyễn Đăng Tỵ, *Cơ sở dữ liệu*, NXB Đại học quốc gia TPHCM (2010).
3. *Nguyễn Gia Tuấn Anh, Mai Văn Cường, Bùi Danh Hường, Cơ sở dữ liệu nâng cao*, NXB Đại học quốc gia TPHCM (2019).
4. Itzik Ben-Gan, *Microsoft SQL Server 2012- TSQL Fundamentals*.


Q
A

Bài tập

Bài 1. Tìm hiểu ngôn ngữ solidity để lập trình với công nghệ blockchain

Bài 2. Tìm hiểu cộng đồng blockchain đã xây dựng các hệ thống blockchain nào chia sẻ cho cộng đồng?

Bài 3. Tìm hiểu các ứng dụng blockchain mà cộng đồng đã chia sẻ công khai, hãy triển khai 1 ứng dụng trên nền tảng này.

Bài 4. Cho biết các ứng dụng nào là không phù hợp với công nghệ blockchain? Tại sao?