ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC - KỸ THUẬT MÁY TÍNH

CÔNG NGHỆ PHẦN MỀM (MỞ RỘNG)

Báo cáo

Ứng dụng Blockchain xây dựng từ điển bất động sản

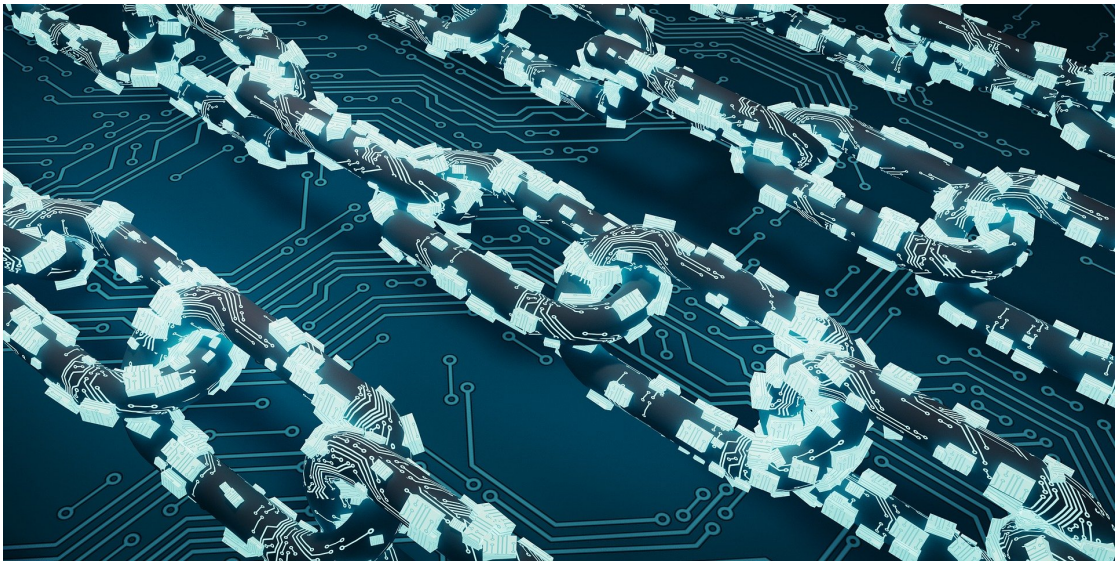
GVHD: Quản Thành Thơ
SV: Nguyễn Khoa Gia Cát 1912749
Huỳnh Tấn Luân 1914054
Trịnh Nguyên Bảo Tuấn 1912371

TP. HỒ CHÍ MINH, THÁNG 10/2021

Mục lục

1 Giới thiệu blockchain

Blockchain là một công nghệ dùng để lưu trữ thông tin đang ngày càng được phổ biến hiện nay do nhiều ưu điểm của nó. Blockchain nghĩa đen là chuỗi các khối, các khối ở đây lưu trữ dữ liệu và các khối này sẽ liên kết với nhau thành chuỗi. Trên thực tế, bởi vì sự liên kết đó nên nếu người ta thay đổi nội dung của một khối nào đó thì sẽ xung đột với những khối khác, do đó dữ liệu đã được chấp nhận thì sẽ coi như không chỉnh sửa được. Vì vậy, một trong những ưu điểm của công nghệ blockchain là chống việc gian lận dữ liệu, khiến blockchain phù hợp để ứng dụng vào việc ghi chép giao dịch, hồ sơ, công chứng...
Công nghệ blockchain kết hợp nhiều loại công nghệ khác nhau như mã hóa, mạng ngang hàng, các luật đồng thuận... Các loại mã hóa khiến cho dữ liệu được toàn vẹn, minh bạch. Mạng ngang hàng phân tán sẽ lưu trữ các bản sao dữ liệu, nếu có một máy tính trong mạng blockchain bị sập thì dữ liệu không bị mất đi.



Hình 1: Nguồn ảnh: pixabay.com

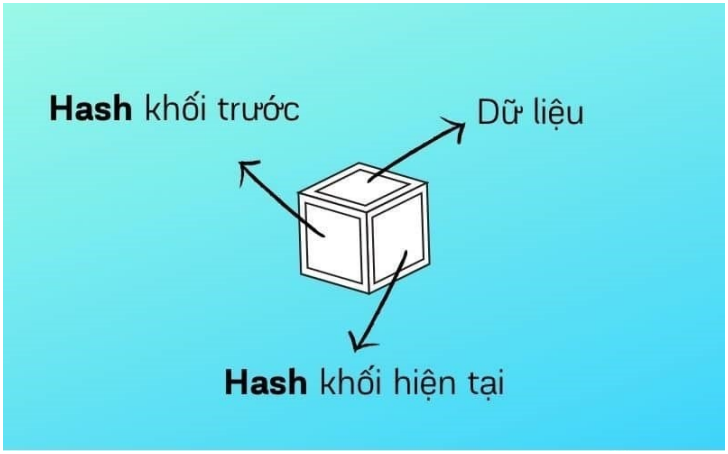
Hiện nay, ứng dụng được biết đến phổ biến của blockchain là hệ thống các đồng tiền điện tử (crypto-currency), cũng như để quản lý các giao dịch tài chính. Tuy nhiên, có nhiều ngành nghề khác cũng phù hợp để ứng dụng công nghệ này, chẳng hạn như:

- Dược phẩm: Công nghệ blockchain có thể ứng dụng để xây dựng hệ cơ sở dữ liệu của các dược phẩm đang lưu thông trên thị trường, chống việc giả mạo dược phẩm hay nguồn gốc xuất xứ của chúng.
- Bảo hiểm: Giúp bảo mật việc xác minh hay nhận tiền, đảm bảo sự minh bạch của hợp đồng.
- Bất động sản: Dữ liệu được công khai, minh bạch sẽ giúp ích cho người quan tâm đến bất động sản.

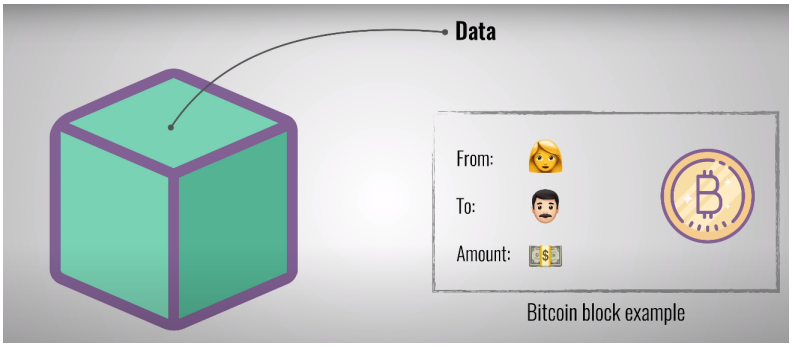
Từ đó, có thể thấy công nghệ blockchain có rất nhiều tiềm năng ứng dụng trong thực tiễn. Hiện nay và trong tương lai, yêu cầu bảo mật và toàn vẹn về dữ liệu là xu hướng tất yếu, cộng với sự phát triển của công nghệ, blockchain sẽ càng được ứng dụng rộng rãi hơn trong nhiều lĩnh vực.

2 Cấu trúc của của blockchain

- BlockChain là một chuỗi các Block. Mỗi Block sẽ được lưu trữ gồm 3 phần:
  - Dữ liệu
  - Hash của khối hiện tại
  - Hash khối trước

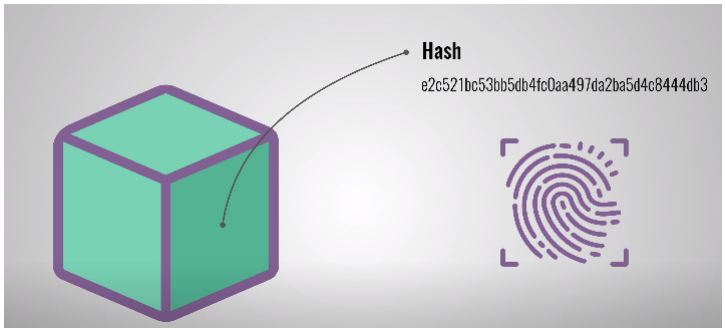


- Dữ liệu của một block phụ thuộc vào các loại blockchain

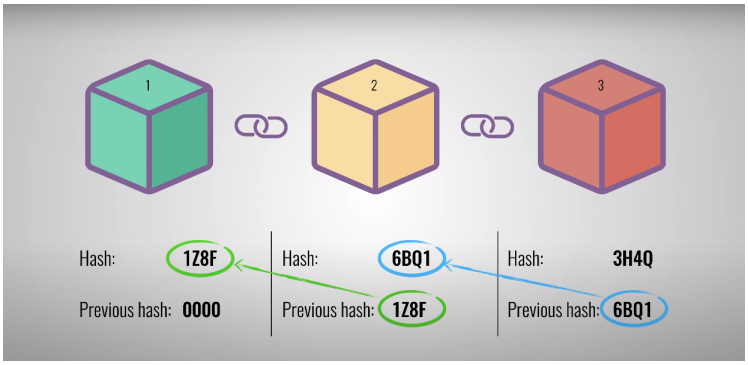


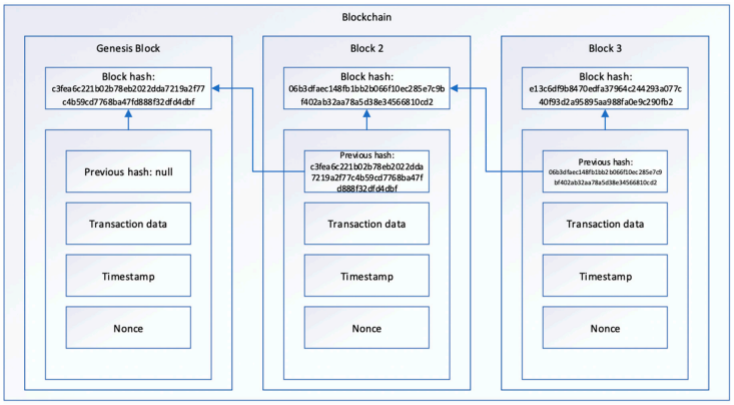
- Ví dụ Blockchain của Bitcoin sẽ chứa các dữ liệu về thông tin giao dịch như người gửi, người nhận, số tiền giao dịch,...

- Hash của một Block được tính dựa trên các thành phần có trong Block và xác định nó là duy nhất trong chuỗi. Bất cứ thay đổi dữ liệu nào trên Block điều làm Hash thay đổi



- Hash của Block trước được chứa trong Block hiện tại giúp hình thành một BlockChain. Hask của khối đầu luôn là 0 (Khối nguyên thủy)





3 Các đặc điểm của blockchain

Công nghệ blockchain có một số đặc điểm chính sau:

- Mạng blockchain được phân tán và đồng bộ, tùy theo loại blockchain (public, private hay permissioned) mà mạng blockchain sẽ có mức độ phân tán khác nhau. Càng phân tán thì các thực thể trong mạng càng ít quyền kiểm soát đối với mạng.
- Không phải mọi thao tác đều có thể được thực hiện đối với dữ liệu mà chỉ có một số thao tác được cho phép, những thao tác đó được lưu trữ ở blockchain dưới dạng smart contract, giúp kiểm soát việc quản lý dữ liệu.
- Block được tạo ra cần phải có sự đồng thuận của các đối tượng khác trong mạng để tránh tình trạng giả mạo.
- Dữ liệu khi đã được đồng thuận và ghi lại thì coi như không thể thay đổi được (nếu cố tình thay đổi sẽ để lại dấu vết).
- Block (hay giao dịch) có thể được tạo ra mà không để lộ danh tính thực sự. Điều này đảm bảo tính riêng tư của hệ thống.
- Dữ liệu được lưu trữ có tính minh bạch (mọi người đều có thể truy cập vào dữ liệu), tùy theo loại blockchain mà mức độ minh bạch sẽ khác nhau.

4 Các loại blockchain

4.1 Public Blockchain

Dữ liệu trên Public Blockchain được công khai để mỗi người có thể theo dõi được dữ liệu nếu họ muốn. Public blockchain không có giới hạn truy cập và bất kỳ ai cũng có thể gửi và xác thực các transaction. Public blockchain thường sử dụng cho mục đích kinh tế, nhất là khi xác thực các transaction và sử dụng thuật toán đồng thuận, chẳng hạn như PoW.
Trong public blockchain, dữ liệu thường minh bạch (transparent) và không thể giả mạo nhưng độ phức tạp cao, thời gian tính toán chậm và có chi phí tính toán cao.

4.2 Private Blockchain

Trong private blockchain, quyền truy xuất dữ liệu lưu trong block của các bên tham gia (peer) thường bị hạn chế. Chỉ có tổ chức điều hành và các yếu tố xác định được tham gia vào các nghiệp vụ trong hệ thống.
Hệ thống private blockchain phân phối dữ liệu mang tính tập trung hơn, bù lại thường có tốc độ truy xuất cao, chi phí tính toán ít.

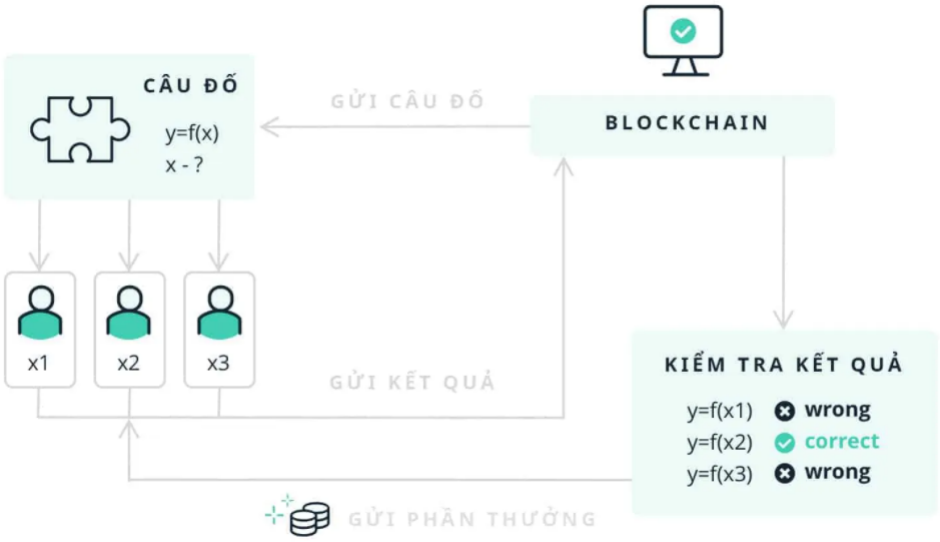
4.3 Permissioned/ Hybrid Blockchain

Hybrid blockchain được xem như một sự hợp nhất của hai loại public và private, mục đích để kết hợp các ưu điểm của cả hai loại đồng thời cố gắng hạn chế các khuyết điểm.
Trong hybrid blockchain, public blockchain có thể được sử dụng để công chúng có thể truy cập các lịch sử giao dịch, đồng thời sử dụng private blockchain để kiểm soát ai có thể tạo giao dịch. Do đó, cách tiếp cận này kết hợp các lợi ích về quyền riêng tư của loại private blockchain và sự bảo mật, minh bạch của public blockchain. Điều này giúp các công ty, tổ chức linh hoạt hơn. Họ có thể chọn những dữ liệu nào muốn công khai hoặc thông tin nào muốn giữ nội bộ.

5 Các cơ chế đồng thuận trong blockchain

5.1 Proof of Work

- Proof of Work (POW) là thuật toán đồng thuận đầu tiên được tạo ra trong mạng Blockchain. Được sử dụng để xác nhận giao dịch và sản xuất các block mới trong chuỗi.
- Khi một giao dịch được thực hiện trên Blockchain, nó sẽ được gom vào một Block cùng một số giao dịch khác. Các miner sẽ sử dụng hệ thống gồm nhiều máy tính mạnh để xác minh giao dịch.
- Một câu đố toán học phức tạp sẽ được hệ thống đưa ra. Nhiệm vụ của miner là sử dụng sức mạnh của hệ thống mining để tìm ra câu trả lời, sau khi tìm được sẽ thông báo cho các miner còn lại.
- Khi phần lớn thành viên xác nhận đó là câu trả lời đúng, Block mới sẽ được tạo ra, giao dịch được xác nhận.
- Khi hoàn thành, miner sẽ nhận được phần thưởng là phí giao dịch và phần thưởng khối. Tuy nhiên, đây là quá trình sử dụng rất nhiều tài nguyên, điện, thời gian.



- Nếu câu đố quá khó, sẽ mất rất nhiều thời gian để tìm ra câu trả lời, khiến Block mới không được tạo ra, hệ thống sẽ bị tắc nghẽn, giao dịch không thể thực hiện.
- Nhưng nếu câu đố quá dễ, hệ thống sẽ dễ bị tấn công, các giao dịch có khả năng bị làm giả
- PoW giải quyết vấn đề này bằng một thuật toán điều chỉnh độ khó phù hợp với tốc độ khai thác của các miner, sao cho Block mới sẽ sinh ra trong một khoảng thời gian cố định.

5.2 Proof of Stake

- Proof of Stake (POS) được tạo ra thay thế cho Proof of Work (POW). Được sử dụng để xác nhận giao dịch và thêm các block mới vào chuỗi.
- Proof-of-Stake đạt được sự đồng thuận bằng cách yêu cầu người dùng đóng góp một lượng token của họ để có cơ hội được chọn để xác thực các block giao dịch và được thưởng vì đã làm như vậy.

- Trong PoS, các block được "rèn" thay vì được khai thác. Yếu tố đầu tiên được xem xét trong quá trình lựa chọn này là cổ phần (stake) của người dùng.
- Mỗi người muốn tham gia vào quá trình phải sở hữu một cổ phần trong mạng. Staking liên quan đến việc khóa một số tiền nhất định vào mạng làm cổ phần của họ. Sử dụng nó làm tài sản thế chấp để chứng minh cho block.
- Càng nhiều người dùng đặt cược, cơ hội được lựa chọn của họ càng cao. Số lượng cổ phần (stake) quyết định cơ hội mà node được chọn làm người xác thực để rèn block kế tiếp. Cổ phần càng lớn, thì cơ hội càng lớn so với người đặt cược (staking) ít hơn.
- Trong PoS, khuyến khích tham gia xác thực các khối phần thưởng là một khoản thanh toán dưới dạng phí giao dịch. Trái ngược với tiền tệ mới được tạo ra trong các hệ thống PoW.
- Để tránh việc nghĩ đây là cơ hội cho những node giàu có trong mạng. Ngày càng nhiều phương thức độc nhất được thêm vào quá trình lựa chọn. Chìa khóa ở đây là bao gồm một mức độ cơ hội cho quá trình lựa chọn để tránh trường hợp người dùng giàu nhất luôn được chọn để xác thực các giao dịch, luôn gặt hái những phần thưởng và ngày càng giàu hơn.
- Hai phương thức được sử dụng phổ biến nhất là Lựa chọn block ngẫu nhiên và Lựa chọn tuổi Coin:
  - Lựa chọn block ngẫu nhiên: Thuật toán Proof-of-Stake sẽ lựa chọn validator kiểm định block tiếp theo một cách ngẫu nhiên. Bằng cách sử dụng công thức tìm kiếm Hashrate thấp nhất, kết hợp với khoản đặt cược cao nhất (stake).
  - Lựa chọn tuổi Coin: Các node được chọn dựa trên thời gian mà các token của họ đã được lưu giữ làm cổ phần. Tuổi đồng coin được tính bằng cách nhân số ngày các coin được giữ làm cổ phần với số lượng các coin đó.

6 Một số nền tảng dựa trên Blockchain hiện nay

6.1 Ethereum

- Sau sự thành công của Bitcoin, một loại tiền điện tử khác cũng gây tiếng vang trong thị trường số hiện nay là Ethereum. Ethereum cho phép mọi người xây dựng và sử dụng các ứng dụng phi tập trung dựa trên công nghệ Blockchain. Nó là dự án mã nguồn mở, có thể chuyển đổi và linh hoạt hơn Bitcoin.
- Ethereum có các đặc điểm sau:
  - Là mạng mở
  - Sử dụng mô hình đồng thuận bằng chứng công việc
  - Có lượng người theo dõi trên Github cao
  - Hỗ trợ các ngôn ngữ như C++, Go và Python

6.2 Hyperledger Fabric

- Đây là một trong những nền tảng Blockchain phát triển gần đây nhất và được biết đến như là cuốn siêu sổ cái vào năm 2016, do Linux Foundation tạo ra. Mục tiêu của nó là đẩy nhanh sử dụng công nghệ Blockchain trong các ngành công nghiệp khác nhau như tài chính ngân hàng, IoT, chuỗi cung ứng...
- Hyperledger Fabric có các đặc điểm sau:
  - Có thể sử dụng cho mục đích mở hoặc đóng
  - Tích cực cập nhật trên Github
  - Sử dụng mô hình đồng thuận Pluggable
  - Hỗ trợ ngôn ngữ Python

6.3 IBM Blockchain

- Là công ty tiên phong liên doanh Blockchain vì vậy mà nó có thể tạo một nền tảng điều hành kinh doanh minh bạch. IBM tự hào về một cơ chế đồng thuận hiệu quả hơn, tạo sự chú ý cho nhiều người.
- IBM Blockchain có các đặc điểm sau:
  - Nó thuộc về mạng Blockchain đóng, do đó có sự bảo mật cao
  - Phổ biến ở mức trung bình nhưng tích cực cập nhật trên Github
  - Phiên bản miễn phí hạn chế, có thể nâng cấp lên gói Doanh nghiệp
  - Hỗ trợ các ngôn ngữ như Go và Javascript

6.4 Multichain

- Multichain là nền tảng Blockchain mã nguồn mở, được dùng trong mạng Blockchain đóng. Nó được sử dụng trong các doanh nghiệp khác nhau. Bằng cách cung cấp quyền riêng tư và sự kiểm soát mạng ngang hàng, nó như là sự cải thiện của Bitcoin cho các giao dịch tài chính riêng tư.
- Multichain có các đặc điểm sau:
  - Là mạng mang tính chất đóng
  - Phổ biến ở mức trung bình nhưng tích cực cập nhật trên Github
  - Miễn phí và mã nguồn mở
  - Hỗ trợ các ngôn ngữ như Python, C#, JavaScript , PHP, Ruby

6.5 Hydrachain

- Hydrachain là một sáng kiến hợp tác giữa Ethereum và công nghệ brainbot. Nó được dùng để tạo một sổ cái riêng tư hữu ích cho doanh nghiệp mặc dù nó không được phổ biến.
- Hydrachain có các đặc điểm sau:
  - Sử dụng giao thức Ethereum
  - Là mạng đóng
  - Ít phổ biến hơn nhưng tích cực cập nhật trên Github
  - Hỗ trợ ngôn ngữ Python.

6.6 Openchain

- Openhain là một nền tảng mã nguồn mở, cực kỳ hữu ích cho các công ty đang tìm kiếm giải pháp quản lý tài sản kỹ thuật số. Nó còn cho phép tùy biến quyền theo các mức độ khác nhau.
- OpenChain có các đặc điểm sau:
  - Dùng cho mạng đóng
  - Phổ biến ở mức trung bình nhưng tích cực cập nhật trên Github
  - Hỗ trợ ngôn ngữ JavaScript
  - Sử dụng mô hình đồng thuận phân vùng

6.7 BigchainDB

- BigchainDB là một nền tảng mã nguồn mở. Là một cơ sở dữ liệu nhưng mang các tính chất của Blockchain.
- BigchainDB có các đặc điểm sau:
  - Tùy biến tài sản
  - Không tích hợp sẵn tiền ảo
  - Có thể dùng cho cả mạng đóng và mở
  - Hỗ trợ các ngôn ngữ như Java, Python, Javascript và các ngôn ngữ khác do cộng đồng hỗ trợ

7 BigChainDB

7.1 BigChainDB là gì

BigchainDB là 1 trong nhiều nền tảng Blockchain (Blockchain platform), được thiết kế với ý tưởng kế thừa và kết hợp blockchain với cơ sở dữ liệu phân tán (cụ thể là MongoDB). Có thể xem BigchainDB như là 1 cơ sở dữ liệu blockchain giúp xây dựng một ứng dụng phi tập trung mà không cần tạo một blockchain riêng biệt từ đầu.

BigchainDB giúp bổ sung các đặc điểm của blockchain, bao gồm tính bất biến, kiểm soát phi tập trung và chuyển giao tài sản kỹ thuật số. Do đó BigchainDB có để được sử dụng để triển khai các ứng dụng quy mô lớn vào nhiều ngành khác nhau, từ lĩnh vực sở hữu trí tuệ cho đến quản lý chuỗi cung ứng và Internet-of-Things.

7.2 Ưu điểm của BigchainDB

Nhờ vào sự kế thừa và kết hợp giữa Blockchain và MongoDB, BigChain có các thế mạnh sau:

- Kiểm soát phi tập trung. BigchainDB không tồn tại điểm kiểm soát duy nhất (single point of control). Do sự kiểm soát phi tập trung nhờ vào liên kết của các nút ngang hàng, nó tạo thành một mạng P2P.
- Cho phép truy vấn dữ liệu. BigChainDB Được hỗ trợ bởi MongoDB nên chúng ta có thể viết và chạy bất kỳ truy vấn MongoDB nào, tìm kiếm các phần tử liên quan đến các giao dịch, siêu dữ liệu, nội dung trong các block.
- Tính bất biến: Dữ liệu không thể bị thay đổi.
- Khả năng thích nghi của Byzantine (BFT). Nếu không may mắn, một số nút trong mạng đang gặp lỗi, phần còn lại của mạng vẫn đi đến quy trình đồng thuận trên khối tiếp theo.
- Cung cấp độ trễ thấp. Mất khoảng một giây để đi đến quá trình đồng thuận trên một block mới, làm cho việc hoàn tất giao dịch diễn ra cực kỳ nhanh chóng.

- Linh hoạt. BigchainDB cho phép phát triển mạng riêng của người dùng với các thông tin tùy chỉnh, đảm bảo sự linh hoạt trong cấp quyền (permissions), giao dịch và tính minh bạch.
- Mã nguồn mở
- Triển khai các mạng Private hoặc Public. BigchainDB cho phép chúng ta triển khai các hệ thống mạng Private hoặc Public, tùy cơ ứng biến cho các trường hợp sử dụng cụ thể.

7.3 Một vài Ứng dụng của BigchainDB

Nhiều trường hợp sử dụng BigchainDB giống như mô hình blockchain truyền thống; khi đó bỏ qua các lợi thế của BigchainDB như thông lượng cao hơn, nhiều dung lượng hơn, độ trễ thấp hơn, truy vấn tốt hơn hoặc cấp phép phong phú hơn.

Bên cạnh đó, cũng có một số trường hợp dùng BigchainDB như 1 cơ sở dữ liệu phân tán truyền thống, ngoại trừ việc tập trung vào nơi các đặc điểm của blockchain có thể được tận dụng. Ví dụ: cải thiện độ tin cậy của DataBase bằng cách không có một điểm lỗi nào hoặc lưu trữ tài liệu mật một cách an toàn.

Cụ thể các trường hợp sử dụng BigchainDB:

- Các hợp đồng ràng buộc về mặt pháp lý có thể được lưu trữ trực tiếp trên BigchainDB bên cạnh giao dịch, ở định dạng mà con người lẫn máy tính có thể đọc được.
- Tạo và di chuyển theo thời gian thực của các dữ liệu có khối lượng lớn. Chỉ chủ sở hữu của nội dung mới có thể di chuyển dữ liệu. Khả năng này giúp giảm chi phí, giảm thiểu độ trễ giao dịch và hỗ trợ các ứng dụng khác.
- Theo dõi các tài sản vật chất có khối lượng lớn dựa theo toàn bộ chuỗi cung ứng. BigchainDB có thể giúp giảm gian lận, tiết kiệm chi phí lớn.
- Theo dõi các tài sản sở hữu trí tuệ. BigchainDB có thể giảm chi phí, thời gian cấp phép trong các kênh, hệ thống kết nối các tác giả với khán giả và cung cấp nguồn gốc rõ ràng cho các tài sản kỹ thuật số. Ví dụ: Giả sử cần một dịch vụ âm nhạc có hàng triệu bài hát - BigchainDB có thể lưu trữ thông tin này trong tích tắc, cùng với thông tin bản quyền về từng bài hát và thông tin về giấy phép sử dụng của người đăng ký.
- Giảm thời gian đóng dấu, chứng nhận, công chứng. BigchainDB làm giảm xung đột pháp lý bằng cách cung cấp bằng chứng hợp pháp, chặt chẽ về các hành vi trên không gian mạng.
- Cải thiện độ tin cậy của cơ sở dữ liệu truyền thống bằng cách tạo ra khả năng chống lại các điểm lỗi đơn lẻ (single points of failure). Việc tăng cường bảo mật này sẽ giúp đề phòng các nguy cơ mà một lần hack dẫn đến mất mát dữ liệu lớn như vụ việc Sony 2014.

Tài liệu

[bdb1] BigchainDB. (n.d.-a). *Basic Usage Examples*. BigchainDB Python Driver 0.6.2 Documentation. Truy cập ngày 27 tháng 10, 2021, từ http://docs.bigchaindb.com/projects/py-driver/en/latest/usage.html

[bdb2] BigchainDB. (n.d.-b). *Quickstart / Installation*. BigchainDB Python Driver 0.6.2 Documentation. Truy cập ngày 27 tháng 10, 2021, từ http://docs.bigchaindb.com/projects/py-driver/en/latest/quickstart.html