A Taxonomy of Blockchain Technologies:

Principles of Identification and Classification

**1. Giới thiệu**

**1.1 thông tin nền:** cơ bản là sự kết hợp của các công nghệ sẵn có (distributed ledger, public key, merkle tree hashing, consensus) đặt nền móng cho peer-validation decentrailised cryptocurrency BTC, nguyên bản được giới thiệu bởi Satoshi Nakamoto năm 2008, năm đó là năm đánh dấu cho thành công mới The blockchain, đồng í là blockchain có nhiều lợi ích hơn là BTC, nó cung cấp kiểu distributed software architechture được phát triên nơi mà mạng lưới gồm những untrusted participants có thể đồng í thực hiện việc chia sẻ state cho decentralised và transaction data theo 1 các bảo mật mà không cần đến điểm kiểm soát ở giữa hoặc việc giám sát thường xuyên. Blockchains đảm bảo sự tin tưởng giữa các đối tác ẩn danh trong các hệ thống phi tập trung - decentralised mà không cần các cơ quan giám sát trung ương chịu trách nhiệm xác minh tính đúng đắn của các ghi chép trong sổ cái ledger. Blockchains được công bố là một công nghệ đột phá đổi mới, nhưng trên thực tế không có đổi mới kỹ thuật thực sự trong Bitcoin và blockchain.

**1.2 Problem Statement and Research Method:** Ngành công nghiệp thúc đẩy các thiết kế mô hình khác nhau ưu tiên các khía cạnh chức năng và hiệu suất hơn các khía cạnh khác để đáp ứng các mục tiêu kinh doanh cụ thể. Hiện tại, có hàng nghìn dự án dựa trên blockchain trên toàn thế giới đang được phát triển. Một số trong số chúng là những nhánh đơn giản của các công nghệ thành công, chẳng hạn như Bitcoin hoặc Ethereum; khác đề xuất các chức năng và kiến trúc hoàn toàn mới. Chính vì lý do này, thay vì “Blockchain ”chúng tôi đề cập đến blockchains or blockchain technologies, nghĩa là, để bao gồm tất cả các cấu hình kiến trúc có thể có và vì đơn giản, cả gia đình lớn hơn distributed ledger technologies (DLT) Một sự phát triển không đồng nhất kết hợp thiếu khả năng tương tác có thể gây nguy hiểm cho việc áp dụng rộng rãi và thống nhất các blockchain trong hệ thống công nghệ và kinh tế xã hội của chúng ta. Hơn nữa, các biến thể trong thiết kế blockchain và các cấu hình có thể có của chúng đại diện cho một trở ngại đối với các kiến trúc và nhà phát triển phần mềm. Trong thực tế, nếu không có khả năng sử dụng một mô hình tham chiếu kỹ thuật, rất khó để đo lường và so sánh chất lượng và hiệu suất của các blockchain và ứng dụng khác nhau. Giải pháp cho những vấn đề này là thiết lập các kiến trúc tham chiếu phần mềm, nơi cấu trúc tiêu chuẩn hóa và các yếu tố và quan hệ tương ứng có thể cung cấp các mẫu cho kiến trúc blockchain cụ thể. Các tiêu chuẩn có thể xuất hiện một cách tự nhiên do sự chấp nhận của thị trường (theo định hướng của ngành) hoặc có thể được áp đặt bởi các viện và tổ chức. Nhìn chung, tiêu chuẩn hóa lâu dài của kiến trúc tham chiếu blockchain sẽ mang lại lợi ích cho mọi ngành. Một tiêu chuẩn cho kiến trúc tham chiếu phần mềm là cần thiết để cho phép một sân chơi bình đẳng, nơi mọi người chơi trong ngành và thành viên cộng đồng có thể thiết kế và áp dụng các sản phẩm hoặc dịch vụ hỗ trợ blockchain trong các điều kiện tương tự với khả năng có dữ liệu trao đổi. Các tiêu chuẩn Internet thúc đẩy khả năng tương tác của các hệ thống trên Internet bằng cách xác định các giao thức chính xác, định dạng thông báo, lược đồ và ngôn ngữ. Do đó, các phần cứng và phần mềm khác nhau có thể tương tác và làm việc cùng nhau một cách liền mạch. Trong the mid-to-long term việc thiếu các tiêu chuẩn có thể mang lại rủi ro liên quan đến quyền riêng tư, bảo mật, quản trị, khả năng tương tác và rủi ro cho người dùng và những người tham gia thị trường, có thể xuất hiện dưới dạng tội phạm mạng liên quan đến blockchain

**1.3 Result** là một phân loại blockchain phổ quát cây nhóm các thành phần chính trong một cấu trúc phân cấp và xác định chức năng của chúng mối quan hệ và các mẫu thiết kế có thể có

Nói chung, rất khó để đánh giá liệu một đơn vị phân loại hay một bản thể là tốt hay xấu, đặc biệt nếu miền là một mục tiêu di động như blockchain. Đơn vị phân loại và bản thể học là thường được phát triển để hạn chế sự phức tạp và sắp xếp thông tin, nhưng tất cả đều phục vụ các mục đích khác nhau và thường phát triển theo thời gian, mục tiêu là nhằm góp phần thiết lập nền tảng cho việc phân loại các loại thành phần blockchain khác nhau. Không tuyên bố đại diện cho cấu trúc cuối cùng, phân loại được đề xuất có thể có tầm quan trọng thực tế trong nhiều trường hợp

**2. Background on Blockchain Technologies**

Kể từ khi Bitcoin ra đời vào năm 2009, nhiều kiến trúc phần mềm blockchain đã được triển khai để đáp ứng các tùy chọn thiết kế kỹ thuật, kinh doanh và pháp lý khác nhau. Với động lực phức tạp hiện tại của sự phát triển kiến trúc blockchain, nó sẽ không đầy đủ hoặc toàn diện đối với cung cấp một bức tranh về các công nghệ blockchain hiện có được phát triển cho đến nay. Do đó chỉ tập trung vào data decentralisation, transparency, security, immutability, and privacy

- decentralisation of consensus: The distributed nature of the network requires untrusted participants to reach a consensus, consensus can be based on “rules” or on the history of “transactions”. The decentralised consensus on transactions quản lý việc cập nhật ledger bằng chuyển giao trách nhiệm cho local node mà node độc lập xác thực transactions và thêm vào chuỗi dài nhất - the most cumulative computation throughput. No single point of trust and no single point of failure.

- Transparency: record có thể được kiểm tra bởi một nhóm người tham gia được xác định trước, mặc dù nhóm này có thể ít nhiều cởi mở. Ví dụ: trong các blockchains công cộng, mọi người có kết nối Internet đến mạng có quyền bình đẳng và khả năng truy cập ledger. The records are thus minh bạch-transparent and traceable. Hơn nữa, những người tham gia mạng có thể thực hiện các quyền cá nhân (weighted) của họ để cập nhập ledger. Người tham gia cũng có tùy chọn gộp các quyền có trọng số cá nhân lại với nhau

- Security: Blockchains are shared, tamper-proof, replicated ledgers nơi mà record không thể đảo ngược và không thể giả mạo nhờ các hàm băm mật mã một chiều. Mặc dù bảo mật là một khái niệm tương đối, chúng ta có thể nói rằng các blockchain tương đối an toàn vì người dùng chỉ có thể chuyển dữ liệu nếu họ sở private key. Private keys are used to generate a signature for each blockchain transaction a user sends out. This signature is used to confirm that the transaction has come from the user, and also to prevent the transaction from being altered by anyone once it has been issued.

- immutability: Blockchains are immutable because once data has been recorded in the ledger, it cannot be secretly altered ex-post without letting the network know it. In the blockchain context immutability is preserved thanks to the use of hashes. Each block includes the previous block’s hash as part of its data, creating a chain of blocks. The strength of a given blockchain’s immutability is relative, and relates to how hard the history of transactions is to change BUT “51% attack” the block-adding mechanism tends to be a little different, and instead of relying on expensive Proof-of-Work, the blockchain is only valid and accepted if the blocks are signed by a defined set of participants. This means that, in order to recreate the chain, one would need to know private keys from the other block-adders.

- Automation and smart contracts: Không cần sự tương tác của con người, xác minh, phần mềm được viết để các giao dịch xung đột hoặc kép không được viết vào blockchain. Mọi xung đột đều được tự động hòa giải và từng giao dịch hợp lệ chỉ được thêm vào một lần (không có mục kép)

- Storage: Không gian lưu trữ có sẵn trên các mạng blockchain có thể được sử dụng để lưu trữ và trao đổi cấu trúc dữ liệu tùy ý. Việc lưu trữ dữ liệu có thể có một số giới hạn về kích thước được đặt để tránh vấn đề "blockchain phình to". the storage of additional data can occur “off-chain” via a private cloud on the client’s infrastructure or on public (P2P or third-party) storage

**3. Taxaonomy of blockchain**

Sự đa dạng của nghiên cứu và phát triển blockchain tạo cơ hội cho việc áp dụng chéo các ý tưởng và sự sáng tạo, nhưng nó cũng có thể dẫn đến sự phân mảnh của lĩnh vực này và nhân đôi nỗ lực. 1 giải pháp là thiết lập mô hình kiến trúc tiêu chuẩn để gán field và promote coordinated research and development initiatives - thúc đẩy các sáng kiến phối hợp nghiên cứu và phát triển. Tính đến hiện nay kiến trúc về blockchain vx chưa đc đề xuất nhiều nhưng mà việc nhất quán kỹ thuật các hệ thống blockchain là 1 vấn đề lớn hơn cả. Giải pháp mà bài báo đưa ra là phân loại BlockChan dựa trên thành phần bắt đầu từ thành phần kết nối các chi tiết. Compartmentalizes the blockchian connector, thiết lập mối quan hệ giữa chúng theo cách thức phân cấp. Sử dụng 1 phương pháp thiết kế ngược để tách các blockchain và chia chúng thành các phần chính, mỗi thành phàn chính đó lại đc chia nhỏ sub và sub-sub, việc này giúp xác định the alternative modus operandi of the blockchains, and helps to develop the conceptual blockchain design and modelling

**4. Consensus**

Thành phần đầu tiên là consensus - tính đồng thuận, It relates to the set of rules and mechanics that allows for the maintainance and updating of the ledger and guarantees the trustworthiness of the records. with every consensus mechanism bringing advantages and disadvantages based on different characteristics: transaction speed, energy efficiency, scalability, censorship-resistence, and tamper resistance. The set of rules and mechanics compose the framework of the validation process that is necessary to overcome security issues during the validation, component Cosensus:

Consensus network topology

Consensus immutability and Failure tolerance

Gossiping

Consensus agreement

Latency

Finality

Tất cả những sub và sub-sub này đề là rất quan trọng khi thiết kế network consensus validation process nó sẽ quyết định how and when thì blockchian agreement đạt được và ledger update.

**4.1 Consensus network topology**

mô tả loại kết nối giữa các nút và loại luồng thông tin giữa chúng để giao dịch và / hoặc cho mục đích xác nhận. Vì mục đích hiệu quả mà hệ thống được thiết kế centralised, việc này làm giảm đáng kể chi phí cho cấu hình, bảo trì, điều chỉnh hệ thống vì tất cả đó chỉ được thực hiện ở điểm trung tâm, nhưng điều này sẽ gặp vấn đề khi điểm giữa gặp trục trặc bỏi vậy mà cơ chế centralised thường được hướng đến hierarchical- kế thừa, phân cấp thể hiện khả năng mở rộng lớn hơn và dự phòng nhiều hơn, trong khi vẫn giữ giao tiếp hiệu quả. Còn đối với decentralised thì nó đã đc phát triển rất lâu và trong đó các node được coi là bình đẳng với nhau. Như đã liệt kê ở bên trên thì có 3 layout cho consensus network toplogy:

4.1.1 Decentralised: Như trong BTC là 1 ví dụ điển hình, việc thiết lập mạng p2p cho phép chuyển trực tiếp các transaction trong các node có trong mạng. Công việc thẩm định trong mạng là decentralised thông qua miner và các node thẩm định các transaction trong mạng lưới được kết nối theo các random, as provided by super node.

4.1.2 Hierarchical : Trong Ripple network được chia thành tracking or stock và validating node. Tracking node là cửa để nộp transaction hoặc thực hiện các truy vấn đến ledger, chúng còn có thể đưa các transaction đến các mạng rộng hơn thông qua history sharding. Validating node hoạt động như tracking node nhưng nó còn cung cấp thứ tự đến ledger thông qua việc thẩm định, biểu quyết về fees and amendment – sửa đổi.

4.1.3 Centralised: trong 1 số trường hợp thì điểm giữa là được yêu cầu để quản lí cái gì sẽ được thêm vào ledger, giải pháp này cung cấp third layer điều này thường được sử dụng trong private blockchain.

**4.2 Consensus immutability and Failure tolerance**

Có rất nhiều loại failure và thường chúng rất tốn kém để cài đặt cho hệ thống fault-tolerant. Đối với blockchain là 1 hệ thống distributed – phân tán thì việc fault-tolerant là khi hệ thống hoạt động các chức năng bình thường như cung cấp độ tin cậy, tính hợp lệ và bảo mật của thông tin đươc lưu trong ledger. Blockchain là phương pháp ko điểm giữa mà thay vào đó mỗi là sự lặp lại bỏi đó mà mỗi server sẽ giữ 1 bản copy của ledger. Mỗi record sẽ rất tốn kém trong bước ghi nhưng lại có chi phí thấp trong việc xác định bởi peers

Tại thời điểm bài báo ra đời thì chỉ có 6 hình thức của consensus immutability and failure tolerance:

4.2.1 Proof-of-Work:

Thiết lập các thiết bị tính toán thường gọi là miner, kết nối với network thực hiện task validating những transaction được đề xuất nhằm hoàn thiện record của những transaction đã được valid, việc tạo ra block mới có thể đc thêm vào blockchain yêu cầu việc đảo ngược của phương thức mã hóa, điều này chỉ có thể được thực hiện cách thủ công. Trong pow, xác xuất mà 1 miner khai thác được 1 khối mới phụ thuộc vào sức mạnh tính toán của ng đó so với tổng sức mạnh của các miner kết nối với mạng. Bỏi vì miner phải tìm được giải pháp cho one-way hash của giá trị mới dựa vào the previous hash values contained in the message và new transaction in the block họ tạo ra và nonce(nonce chưa hiểu nghĩa nhưng đang nghĩ là số thứ tự), giải pháp sẽ đạt được khi new hash value bắt đầu với số số 0 bé hơn hoặc bằng target, SHA256. Điều thú vị là, khi hai đối thủ phối hợp với nhau, chỉ cần mỗi đối thủ giữ xung quanh là đủ 25% tổng sức mạnh tính toán để thực hiện một cuộc tấn công Trong bố cục này, tồn tại rủi ro khai thác độc quyền, gây ra bởi sự phối hợp lớn của các thợ mỏ trong một lần khai thác duy nhất nhóm, liên tục tăng lợi nhuận dự kiến của những người khác nếu họ tham gia khai thác nói trên pool. Trong tình huống giả định này, nhóm khai thác cho biết có thể kiểm duyệt các giao dịch cụ thể và chỉ định giao dịch nào được chấp nhận và giao dịch nào không