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