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

**4.2.2 Proof-of-Stake:**

Pos liên kết các block generation đến với proof of ownership của số tài sản số nhất định kết nối với blockchain. Xác suất để các block generation được chọn để xác minh khối tiếp theo phát triển liên quan đến phần tài sản họ có trong hệ thống. Giả định cơ bản là người dùng có tỷ lệ chia sẻ lớn của cải hệ thống có nhiều khả năng cung cấp thông tin đáng tin cậy liên quan đến quá trình xác minh và do đó được coi là một người xác thực đáng tin cậy hơn. 2 hình thức POS, đầu tiên là random nó sử dụng 1 phép tính tìm kiếm the lowest hash together with the stake size; do đó nó có phần xác định và mỗi nút có thể xác định độc lập khả năng được chọn trong tương lai. Thứ 2 là kết hợp thứ nhất với coin-age (có được bằng phép nhân số lượng tài sản và khoảng thời gian mà tài sản đó đã được nắm giữ). Mặc dù Pos giải quyết được 2 vấn đề của Pow: monopoly mining và resources wasted in mining process; nó bị ảnh hưởng bởi “nothing at stake”. Bỏi vì chi phí thấp trong làm việc với chains. 1 ng có thể lạm dụng hệ thống bằng cách bỏ phiếu cho nhiều lịch sử blockchain sẽ ngăn cản sự đồng thuận từ trước. Người forgers sẽ đc thưởng vì nghĩa vụ của họ và sẽ bị phạt nếu có hành động sai. Những người này sẽ được chọn bởi cơ chế của Proof-of-Authority.

**4.2.3 Proof-of-Authority**:

Người tham gia được yêu cầu sử dụng a hard-configured set of “authorities” empowered to collaborate “trustlessly”. Bởi vậy mà 1 số node sẽ được tạo ra block mới và bảo vệ blockchain, các cơ chế phù hợp tốt cho các mạng riêng của tập đoàn trong đó một sốcác thực thể được phép kiểm soát nội dung được thêm vào public registry. Node đó sẽ được cấp 1 tập private key sẽ được dùng để kí new block hoạt động như trusted signer.

**4.2.4 Proof-of-Capacity**:

Không tập trung vào sức mạnh của CPU mà nhằm vào khả năng lưu trữ. Node đc yêu cầu cài đặt a signature volume of their hard drive space to mining thay vì sử dụng CPU như trong POW. PoC sử dụng cây băm để cho phép xác minh một cách hiệu quả một thử thách mà không cần cất giữ cây. Điều này làm Poc công bằng và green hơn Pow. Nguyên nhân chủ yếu đến từ sự chênh lệch thấp hơn về thời gian truy cập bộ nhớ giữa các máy và chi phí năng lượng thấp hơn đạt được thông qua việc giảm số lượng tính toán cần thiết. Poc có a prover P và a verifier V. Thay vì P chứng minh cho V rằng một số công việc đã được hoàn thành, P chứng minh cho V rằng nó đã phân bổ một số số byte lưu trữ. Sau giai đoạn khởi tạo, P phải lưu trữ một số dữ liệu F có kích thước N. Thay vào đó, V chỉ chứa một số thông tin nhỏ. Bất cứ lúc nào sau đó tại thời điểm V có thể khởi tạo giai đoạn thực thi bằng chứng và ở cuối V đầu ra từ chối hoặc chấp nhận. Có 3 giai đoạn: N­0, N1, T, miner phải truy cập ít nhất N­0 bộ nhớ giữa lúc khởi tạo và thực thi, ít nhất N1 trong lúc thực thi, hoặc more than T trong lúc thực thi.

**4.2.5 Proof-of-Burn**

Miner prove họ đã burn 1 vài tài sản kĩ thuật số, burn bằng cách chuyển tài sản kĩ thuật số đến địa chỉ xác nhận mà ko tiêu sài được tài sản, giống với Pos, Pob nhằm giảm thiểu lượng giác thải của Pow, tất cả pob phương thức đều là burn tài sản pow đào được bởi vậy mà nó là tốn kém vì sử dụng nguyên liệu không thể tái chế được

**4.2.6 Hybrid**:

Các phương pháp bất biến đồng thuận và khả năng chịu lỗi kết hợp tiên tiến hơn là “PoB và PoS”, trong đó các khối Proof-of-Burn hoạt động như các trạm kiểm soát và “PoW và PoS” nơi các khối PoW hoạt động như các trạm kiểm soát không chứa giao dịch nhưng neo cả hai vào mỗi khác và chuỗi PoS. To solve the “nothing at stake” issue, Peercoin uses centrally-broadcast checkpoints (signed under the developer’s private key) theo đó ko có tổ chức blockcahin nào được phép xuống sâu hơn the last know checkpoint. Nhưng mà vì vậy thì developer sẽ là central authority kiểm soát blockchain.

**4.3 Gossiping**: blockchain là decentralised, lưu trữ lặp lại, việc dư thừa này làm rất khó để hijack thông tin chưa trong chúng. Làm sao để thông tin đc chuyền trong network. Thiếu đi điểm giữa, nodes phải transmit thông tin nó xử lý – trong block mới; nó có thể là toàn bộ blockchain xử lý node mới được thêm vào network. Để đạt được điều này node cần process a list ò peer nodes. Khi mà block mới được thêm vào local blockchain của 1 node, nó chuyền block này đến node khác thông qua peer list của nó bằng gossiping.

**4.3.1 local**: gossiping thực hiện đầu tiên ở local cho đến khi đạt được consensus. Như trong ripple node có thể chia sẻ transaction record đến node khác và đạt được consensus mà không cần trực tiếp biết được tất cả các node trong network. Nỏi vậy mà hầu hết thông tin travels “locally” P2P network thì consensus dễ đạt được.

**4.3.2 global**: gossiping diễn ra trong list of peers được chọn và trong btc được gọi là fallback node. Những node này duy trì a list ò peer trong network. Dựa vào kết nối với node mới chúng submit a random list of peer cho node mới. Cấu trúc như vậy thiếu đi khái niệm về vùng lân cận hoặc vùng lân cận cục bộ, và do đó Gossiping có thể được gọi là toàn cầu.

**4.4 Consensus agreement**

Set of rule dưới những records được update độc lập bởi node trong distributed system. Điều này là quan trọng để hiểu distributed system có thể handle Byzantine failures, làm thế nào để hệ thống có n nodes đạt được consensus trong việc lưu trữ, trustworthy cho dù có sự hiện diện của các node độc hại hoặc những ng tham gia đang tung ra cuộc tấn công.

**4.4.1 Latency**

Mô tả quy tắc truyền bá tin nhắn trong các mạng

**- Synchronous Communication**: truyền tin đồng bộ, Các hệ thống đặt giới hạn trên trên "tốc độ xử lý khoảng thời gian" - process speed interval và "sự chậm trễ giao tiếp" - communication delay sao cho mọi thông điệp đến trong một khoảng thời gian nhất định đã biết, xác định trước, khoảng thời gian ∆. Điều này không loại trừ khả năng có sự chậm trễ tin nhắn do độ trễ mạng ngoại sinh, nhưng sự chậm trễ bị ràng buộc và bất kỳ thông điệp nào mất nhiều thời gian hơn ∆ đều bị loại bỏ

Một khối bị từ chối nếu chứa dấu thời gian: 1) thấp hơn (hoặc bằng) dấu thời gian trung bình của dấu thời gian trước đó mười một khối, 2) lớn hơn (hoặc bằng) "thời gian điều chỉnh mạng" cộng với 2 giờ

**- Asynchronous Communication**: Truyền thông không đồng bộ, Các hệ thống không đặt bất kỳ ràng buộc nào về "tốc độ xử lý khoảng thời gian" và "sự chậm trễ giao tiếp", sao cho mỗi tin nhắn / gói có thể mất một thời gian không xác định để đến nơi. Lợi thế : cuộc gọi/yêu cầu không cần phải được gửi đến các nút và nút hoạt động không cần phải có sẵn khi thông tin mới được gửi đến họ bởi peer. Nhược điểm chính của nó là thời gian phản ứng là không thể đoán trước và nó là khó khăn hơn để thiết kế các ứng dụng dựa trên chúng

**4.4.2 Finality**

liệu thông tin dự định được lưu trữ trong blockchain có thể được coi là lưu trữ vĩnh viễn một cách an toàn sau khi record được thực hiện hay không. Đối với blockchain hay distributed system điều này khó có thể đạt được, nó không phải là design principles. Trong 1 hệ thống mà block mới diffuse – khuếc tan qua gossiping, và rule ưu tiên chuỗi dài nhất ngay cả khi consensus đạt được ở mức globally, a priori - tiên nghiệm không có gì ngăn cản một tập hợp các nút mới xâm nhập vào hệ thống và ghi đè sự đồng thuận trước đó bằng cách cung cấp các phiên bản lịch sử dài hơn

**- Non-Deterministic**: không quyết định, the consensus agreement “cuối cùng sẽ giải quyết”, sử dụng random hoặc xác suất đồng thuận vốn có trong đó xác xuất không đồng thuận giảm theo thời gian. Trong BTC tần xuất block được điều chỉnh để giảm thiểu xác xuất forks. Hơn thế, việc tuyên truyền các khối thông qua mạng có

sự chậm trễ đặc trưng và thậm chí trong sự hiện diện của chỉ các nút trung thực the fork probability không thể loại trừ đơn giản vì các nút khác nhau có thể tìm thấy các khối cạnh tranh của cùng chiều cao trước khi người được tìm thấy đầu tiên đạt đến mạng hoàn chỉnh. Điều này không thể được ngăn chặn ngay cả khi có cơ chế kiểm soát đồng thời, cái mà mục đích là để sử kết quả cho các hoạt động đồng thời. Mặc dù có widespread heuristic “wait until 6 confirmed blocks are appended to the chain” làm giảm đi khả năng transaction bị ghi đè sau này, nó ko loại bỏ hoàn toàn khả năng block đã được thẩm định bị cắt và loại bỏ khỏi blockchain trong tương lai.

**- Deterministic**: quyết định, consensus agreemen hội tụ với sự chắc chắn các transaction ngya lập tức đc xác nhận/ từ chối bỏi blockchain. Nó tốt cho smart contract nơi sử dụng state-machine replication, phù hợp với việc thực hiện các hợp đồng có thể đạt được trên nhiều nodes

5. Transaction Capabilities

Yếu tố quan trọng thứ 2, rất quan trọng để minh họa khả năng mở rộng của

giao dịch và khả năng sử dụng trong các ứng dụng và nền tảng có thể. Muốn tăng thông lượng giao dịch để cạnh tranh với các giải pháp đã có sẵn trên thị trường; nhằm để đạt được thì quantitative parameters cần được thiết kế để đạt được cải thiện này. Những component của Transaction Capability:

Data Structure in the Blockheader

Transaction Model

Server Storage

Block Storage

Limits to Scalability

Transactions

Users

Nodes

Confirmation Time

5.1 Data Structure in the Blockheader

The data stored in the block header has different functions, it includes the transaction hashes for validation purposes; it contains additional information for different application layers or blockchain technology platforms. describes the capabilities of the system to store transaction information. 2 layout:

- Binary Merkle Tree: The information in the block header in the Merkle tree structure contains a hash of the previous header, timestamp, mining difficulty value, proof of work nonce, and root hash for the Merkle tree containing the transactions for that block, which are used for the verification process to scale up the transactions speed

- Patricia Merkle Tree: (Practical Algorithm To Retrieve Information Coded In Alphanumeric) allows activities like inserting, editing or deleting information referring to the balance and nonce of accounts, which enables faster and more flexible validation of transactions than the binary Merkle tree. it has the important advantage of allowing for verification of specific branches of the tree. Importantly, this technology allows even blocks outside the longest chain to contribute to the validation process, building a confirmation system that is less centralized (Ghost rule)

5.2 Transaction Model

The transaction model can be imagined as an accounting ledger which tracks the inputs and outputs of each transaction. The transaction model describes how the nodes connected to the P2P network store and update the user information in the distributed ledger. Bài toán là prevent data that ought not to be trusted by the parties connected to the system, 2 possible transaction model:

- The unspent transaction output: includes a refractory number of blocks (currently 100 for Bitcoin) during which network participants are prevented from using the transaction output in new transactions it forbids miners from spending transactions fees and block rewards before stable validation status of the block chain. This measure prevents the forking problem of blockchains

- Traditional Ledger: In particular, Stellar lists every single transaction in the Stellar distributed ledger history. Also, Ripple uses the traditional ledger transaction model to register increments/decrements of balance and clear all account balances. In Ethereum some transactions are used to execute actions in smart contracts defined in specific atomic records in the blockchain. Those transactions can be seen as order executions of stakeholders which perform the actions out of said smart contracts.

5.3 Server Storage:

At the core of blockchain-based systems is their decentralised nature. This requires that nodes connected to the peer-to-peer network are indistiguishable from each other. This concept, however, cannot be fully realized when the storage needs, computing power, or bandwidth constraints - ràng buộc of the network nodes do not permit it. different nodes have access to different layers of information, and those which do not store the information fully are “thin clients” connected to the peer-to-peer network. 2 layout for Server Storage:

- Full Node Only: All nodes connected to the network, and which are part of the validation process, are of the same kind. This is a genuinely peer-to-peer network where all the nodes are equivalent-tương đương in terms of information contained. This property creates a large degree of information redundancy, which makes the system more resilient to attacks or malfunctioning.

- Thin Node: some nodes connected to the network contain only a selected subset of all the information contained in the blockchain. This creates more scalable systems, but may deteriorate-suy giảm the resiliency-khả năng hồi phục as only a fraction of the nodes contain the complete blockchain information.

5.4 Block Storage:

The information stored in the blockchain determines the scalability of the system across some dimensions, Nó cũng cho phép chúng ta hiểu làm thế nào thông tin đồng thời từ người dùng được trừu tượng hóa trong hệ thống:

- Transaction: In systems like Bitcoin, only the transactions are stored. They contain a set of inputs and outputs that help to identify the emitter(s) and receiver(s) of a specific transaction. This kind of approach works not only for cryptocurrency applications, but also underlies all property-transfer-like applications.

- User Balance: In systems like Ripple, the decentralised storage also contains information about user balances. This approach may limit the storage needs of the system, but at the same time reduces accountability and the possibility to roll back transactions.

5.5 Limits to Scalability

Sự dencentralised và concomitant redundancy in storage áp đặt các loại giới hạn khác nhau đối với cách thức mà một cụ thể quy mô thực hiện với quy mô hệ thống: System size có thể hiểu là số lượng node kết nối đến network, số lượng các transaction. the limiting factor of a particular blockchain system may vary over time. Because blockchain technologies are rapidly evolving at present, these limits are often changed in the course of platform development. Một ví dụ về sự thay đổi trong khả năng mở rộng do sự tiến hóa công nghệ mang lại là việc áp dụng Segregated Witness (Segwit), Công nghệ này (dưới tên BIP141) đã cung cấp một giải pháp cho vấn đề này tính linh hoạt của giao dịch- transaction malleability và cho phép lưu trữ nhiều giao dịch hơn cho mỗi khối. Although some exponents of the Bitcoin community criticized Segwit to be a non-sufficient short-term scaling solution, it triggered interesting side consequences for the Bitcoin system: first, the implementation of micropayment channels where the transactions are not necessarily recorded in the blockchain but take place off-chain between multiple trusted parties and second, the proposal of SegWit2x, which would have enabled an alternative approach to store information in the transactions, modifying the scalability properties of the platform by increasing the block size to two megabytes.

Scaling is a property that specifies how growth will influence its overall performance. If every node has a small—limited—number of connections, then the total network traffic will scale linearly with the number of nodes. In mathematical terms it will be O(N). However, if every node is connected to each other, then the traffic will be O(N2)

- Number of Transactions: trong Bitcoin, có giới hạn về số lượng giao dịch mà nó có thể xử lý trong mỗi khối vì giới hạn mã cứng đối với kích thước khối trong byte. Given that new blocks appear (on average) every ten minutes, this means that the number of transactions that can be included in a given time window is limited. Therefore the layout “Number ofTransactions” refers— regardless of the information stored in the blockchain—to the specific implementations where the number of operations that can be included in the blockchain is severely limited by design.

- Number of User: Ripple stores not only transactions, but also the state of the Ripple accounts it is the number of users of the system that limits its scalability. A similar problem occurs in Ethereum where the system will be constrained by the number of DAOs that it will contain, as these are the actors that generate activity in the system. Therefore, the term “Number of Users” for this layout is a broad reference to the number of objects with stored states this layout is somewhat linked to the first, in that the number of transactions will depend on the number of users

- Number of Node: The number of nodes connected to the network, acting as verifiers for the information that is stored on the blockchain, presupposes a limiting factor because of the mechanism of information diffusion – sự phổ biến adopted. Gossiping is a process that requires larger times in decentralised networks to propagate into a consensus state, and may even reach a point—when the relative time taken by network traffic is very long—where consensus cannot longer be reached and the blockchain naturally forks.

- Possible Values: The possible values that each layout can have are divided into four: i) indifferent, (ii) at most linear, (iii) at most quadratic, and (iv) worse than quadratic. Giá trị đầu tiên mô tả khi các đặc điểm toàn cầu có liên quan của một hệ thống độc lập với số lượng các lớp cụ thể ; the other three categorical values depend on the number of elements in said class.

- Confirmation Time: The time it takes a specific action to be confirmed ultimately depends on the time it takes for it to be added to the blockchain , and to be validated by further blocks later appended to it. Different approaches can be taken to this process: deterministic addition of new blocks at regular intervals (taken by Peercoin) and stochastic addition like in Bitcoin where the process of mining induces an exponential - hàm mũ distribution of inter-block discovery time.