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(one time random number), 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.

**6. Native Currency/Tokenisation**

Thời điểm hiện tại thì tiền điện tử và transfer of property record là được ứng dụng nhiều nhất trong công nghệ blockchain. Trong tiền điện tử, system participants who contribute to the verification process—if selected by some rule to issue a new block into the blockchain—are awarded the possibility to issue a transaction without issuer (so called “coinbase”) to themselves, this is a customary way of introducing new assets into the system, it introduces an incentive for users to participate of the verification process which leads to an increased trustworthiness on the system.

Sẽ được cung cấp trong token có giá trị được chỉ định vì chi phí liên quan đến sản xuất của nó. Solutions like Bitcoin created their own (and single) asset class (the bitcoin) that can be used for transactions within the system

**- Native Asset**: Some systems implemented using blockchain technologies have an underlying native asset which are digital tokens whose owners assign a value and which allow for the daily activities on the platforms or in their respective communities. Opinions may vary on whether these cryptocurrenties ought to be considered fiat or commodity currencies and whether they may eventually be massively adopted replacing traditional ones. 3 layout for native assets

**+ None**: Private blockchain implementations do not require a native asset within to incentivise participation. In these cases, there is no native asset incorporated into the system

**+ Own Cryptocurrency**: Most implementations of cryptocurrencies only deal with transfer of property of its own tokens within the system. These technologies are limited to their own underlying digital currency, but can also have off-chain solutions to interoperate - tương tác with other currencies, in order to execute transactions or to make use of smart contracts. There are also solutions like coloured-coins

**+ Convertible Multiple Assets**: Other technologies like Counterparty and Ardor do have their own underlying currencies or tokens to execute tasks. However, these technologies also enable the possibility of exchange of assets expressed in others beside those native to the platform. This approach of multiple, convertible currencies has the advantage of allowing for exchange markets be directly incorporated- kết hợp into the system

**- Tokenisation**: A token acts as a digital bearer bond, whose ownership is determined by the data embedded in the blockchain. Ownership of the tokens is transferable between holders using other transactions with associated “transfer” metadata. This does not require the approval of any other authority. The possibility of tokenisation enables a range of possible use cases for blockchain technologies outside the purely financial world thế giới tài chính thuần túy.

**+ No Tokenisation Present**: Bitcoin does not have native technologies that enable tokenisation and requires third-party technologies

**+ Tokenisation Through Third-Party Add-Ons**: Bitcoin plus Colour-Coin enables the existence of tokenised transactions in the Bitcoin blockchain. Said solution is based on the cryptographic nature of Bitcoin addresses and the script language.

**+ Tokenisation**: Các khả năng mã hóa cùng với các phần mở rộng của siêu dữ liệu là có sẵn trong một số triển khai và tạo thành xương sống của nền tảng blockchain đăng ký tài sản. The most paradigmatic example is Ethereum, where the creation of a new token is produced by means of the creation of a smart contract. Nhờ vào tính linh hoạt này và khả năng mở rộng của một nền tảng như vậy, điều kiện để tạo ra các mã thông báo mới là vô số.

**- Asset Supply Management**: Quá trình của tài sản kỹ thuật số tạo nên sự khác nhau giữa các công nghệ blockchain khác nhau. Mỗi cách tiếp cận hướng đến những nền kinh tế khác nhau, trong hầu hết các trường hợp sửa chữa một chính sách tiền tệ cụ thể cho tương lai của một hệ thống cụ thể. It is also generally a pillar of the incentive – khuyến khích scheme that users have to participate (or not) in the validation process

**+ Limited Deterministic**: The most replicated system in the world of blockchain is the limited supply as introduced in Bitcoin. Not only does the supply grow sub-linearly over long periods of time but it is designed to have a well-defined limit. while this incentivizes – khuyến khích users to adopt the technology and contribute to the process of verification—for which they receive remuneration—on the other hand, it also creates an incentive to hoard the asset, limiting transactions

**+ Unlimited Deterministic**: Very few blockchain-based digital currencies have attempted to create an unlimited supply and those that have not seen wide acceptance.

**+ Pre Mined**: Some altcoins have distributed all the assets before the starting of the system a reward system induces some kind of redistribution

7. Extensibility

Sự liên kết của khả năng tương tác, khả năng hoạt động nội bộ, quản trị và ngôn ngữ kịch bản xác định hệ sinh thái tương lai của mạng blockchain và khả năng tích hợp của một loạt các công nghệ liên quan đến blockchain

- Interoperability : Minh họa khả năng tổng thể của blockchain để trao đổi thông tin với các hệ thống khác, bên ngoài blockchain, Nó cho phép dòng chảy vào, dòng chảy ra, và truy xuất thông tin của các nhà cung cấp dữ liệu không nhất thiết phải là một hệ thống dựa trên blockchain

+ Implicit Interoperability: This occurs when the smart contracts that specify conditions under which a particular transaction (or event) is to take place can be written in a Turing complete blockchain script language. In this context, implicitly any kind of condition can be specified, even those involving specific statuses in other systems.

+ Explicit Interoperability: If the script language is not Turing complete or the system has specific tools implemented that enable interoperability – khả năng tương tác with the real world, then we term this explicit interoperability, as it is brought purportedly into the system as one of its design principles.

+ No Interoperability: A blockchain without any possibility for interacting – tương tác with other systems. Bitcoin trong trường hợp không có các giải pháp bên ngoài không có khả năng tương tác được thực hiện. It applies to most existing blockchain-based systems whose script language is not Turing complete.

- Intraoperability: minh họa khả năng tổng thể của blockchain để trao đổi thông tin với các blockchain khác. It allows inflow, outflow, and exchange of data between different blockchains

+ Implicit Intraoperability: This occurs when the smart contracts that specify conditions under which a particular transaction (or event) is to take place can be written in a Turing complete blockchain script language. In this context, implicitly any kind of condition can be specified, even those involving specific statuses in other blockchains.

+ Explicit Intraoperability: Nếu ngôn ngữ kịch bản không hoàn chỉnh mà cụ thể là ngôn ngữ được thiết kế để cho phép intraoperability, it is brought purportedly into the blockchain and is one of its design principle

+ No Intraoperability: A blockchain without any possibility for interaction with other blockchains. As implemented, Bitcoin in the absence of external solutions has no intraoperability implemented. Solutions for non-intraoperable blockchains rely on: 1) Trusted proxies to connect blockchains; 2) Pegged blockchain systems; 3) Distinguishing – phân biệt tokens within the same blockchain based system

- Governance: are crucial for the successful implementation of blockchains and for their capability to adapt, change and interact. As blockchain deployment structures (public chain, private chain, consortium chain) are different, their management patterns are also quite different. Rules: 1) technical rules of self-governance, defined by the participants. Technical rules are composed of software, protocols, procedures, algorithms, supporting facilities and other technical elements; 2) regulatory rules, defined by external regulatory bodies composed of regulatory frameworks, provisions, industry policies, and other components, Regulatory rules are by definition not technical in nature and therefore outside the scope of this taxonomy

+ Open-Source Community: open communities of protocol developers and validators coordinate upgrades and technical adjustments of the blockchain. Bitcoin is mainly maintained by a team of core developers who in coordination- hợp tác with miners agree on changing parameters or other settings of the Bitcoin network. Ethereum and Hyperledger also follow an open-source community model. Open-sources governance has been criticized for turning out to become sometimes too centralized and obstructive- tắc nghẽn.

+ Technical: Since blockchain technologies are very versatile-flexible and can be applied to many business cases, enterprises with a measure of technical strength have proposed themselves as technical solution providers for blockchain architectures. the technical rules of blockchain governance are dictated by the companies according to their business goals

+ Alliance: proposed by industry consortia-an organization composed of companies with common business or technological progress demands, has the scope to create shared technology platforms and to build common business models and standards. Only companies that meet certain criteria are given license to collaborate to set the technical rules of blockchain governance.

- Script Language: Widespread programming languages are Turing-complete, which in formal terms refers to the fact that it is possible to implement an algorithm on it to simulate any Turing machine. These are therefore general purpose languages, in which arbitrary- tùy ý computations can be performed. Languages that are not of this kind, are so because of design reasons which aim to prevent specific behaviours of code execution, like undefined termination

Blockchain systems make it possible to modify the conditions under which certain information will be included in the public record. These conditions must be specified in an algorithmic manner, and in some contexts are termed smart contracts. These algorithms are elicited- gợi ra in a scripting language designed purely for this purpose. Therefore the intended flexibility given to the users, with respect to the scope that the algorithm can develop, affects tremendously the degree of freedom to create conditions for some actions to occur and the hypothetical computational effort that may be necessary to assess if a particular condition is fulfilled or not.

+ Turing Complete: Ethereum refers to a suite of protocols that define a platform for decentralised applications. With respect to scripting languages, on the one end of the spectrum, the Ethereum Virtual Machine (EVM) can execute code of arbitrary algorithmic complexity, developers can create applications that run on the EVM

+ Generic Non-Turing Complete: When designing Bitcoin, a decision was made to keep the scripting language limited in scope, to reduce the impact of these calculations on the efficiency – hiệu quả of the system. It is therefore a non-Turing complete language, and most blockchain implementations have followed this path

+ Application-Specific Non-Turing Complete: here are some non-Turing complete languages that are more expressive than the generic ones and purposely designed for certain cases. By restricting the language to be only able to write programs relevant to specific limited cases, the potential outputs of those programs become predictable. This allows those outputs to be queried and easily analysed

+ Non-Turing Complete + External Data: There exists a third category, barely used so far, that (while keeping the nature of the scripting language non-Turing complete) allows for the existence of oracles. These oracles are considered trustful sources and add a layer of simplification to the validation to be performed by the language, empowering above Turing-completeness.

8. Security and Privacy

The recent evolution and new implementations of blockchain systems bring risks, both technical and operational, associated with security and privacy.

Security of blockchain systems is a matter of significant concern. Cryptocurrencies, the most widely deployed application of blockchain systems, have suffered from cyberattacks which became possible because of the mismanagement of sensitive data and the flawed design of the systems. Without going into the detailed distinction between “risks,” “threats,” “attack surfaces,” and “vulnerabilities,” the security of blockchain systems generally comprises: Information mismanagement; Implementation vulnerabilities; Cryptographic mechanism mismanagement; User privilege mismanagement. For a recent comprehensive – toàn diện survey specifically detailing the security and privacy aspects of Bitcoin and its related concepts, we refer the readers to Conti “A Survey on Security and Privacy Issues of Bitcoin”.

When we speak of privacy we are referring to “freedom from intrusion- xâm nhập into the private life or affairs of an individual when that intrusion results from undue- thái quá or illegal gathering and use of data about that individual”

8.1 data encryption:

Cryptographic primitives (cryptographic algorithms) are used to ensure authenticity, integrity, and order of events. For example, Bitcoin blockchain uses the ECDSA digital signature scheme for authenticity and integrity, and the SHA-2 hash function for integrity – sự toàn vẹn and order of events

- SHA -2: SHA stands for Secure Hash Algorithm, SHA-256 and SHA-512 are the most widely-used for hashing functions, likely stemming from its use in Bitcoin, When applied to hash transactions, it requires a piece of information from the issuer the public key for the validation to take place.

- ZK-SHARKS: The Zero-Knowledge—Succinct Non-interactive Argument of Knowledge is a newer technology where no data has to be provided to validate a specific hash but the hash itself serves as proof. Therefore both the hashed message and the encrypted one are sufficient proof of existence.

8.2 Data Privacy:

Although public/private key infrastructures and other measures like hashing functions should ensure that only the intended recipient – người nhận can read the message and have access to the content of the transaction, the research shows that blockchain transactions can be linked together in order to extract additional information and eventually also the identity of the participants. Indeed, there exists an inevitable – không thể tránh khỏi tradeoff between a decentralised peer-validated system and the security and privacy of information. Obfuscation is a way of turning any program into a “black box”, it runs the same “internal logic” and provides the same outputs for the same inputs, but information on the data and processes is inaccessible:

- Built-In Data Privacy: With built-in data privacy we include all those blockchains that by default provide obfuscation of information. For example ZeroCash uses built-in zero-knowledge cryptography to encrypt the payment information in the transactions.81 Although ZeroCash payments are published on a public blockchain, the sender, recipient, and amount of a transaction remain private. blockchains like Enigma (a project that seeks to implement the “secret sharing” DAO concept) uses built-in secure multi-party computation guaranteed by a verifiable secret sharing scheme. In this case, the data can be split among N parties in such a way that M < N are needed to cooperate in order to either complete the computation or reveal any internal data in the program or the state. But M-1 parties cannot recover any information at all. Finally, CORDA by R3 proposes a Node to Node (N-to-N) system characterised by encrypted transactions where only the parties involved in the transaction have access to the data. This is suitable for financial transactions where a high degree of confidentiality is required. Third parties like central banks or other market authorities may have access to the data by invitation only.

- Add-On Data Privacy: In this case, pseudonymous or public blockchains must resort to external solutions in order to obfuscate the information. One method is the mixing service like Coinjoin. The principle behind this method is quite simple: several transactions are grouped together so to become a unique M-to-N transaction. If for example, Alice wants to send one coin to Bob, and Carla wants to send one coin to David, a mixing transaction could be established whereby the addresses of Alice and Carla are both listed as inputs, and the addresses of Bob and David are listed as outputs in one unique transaction. Alternative to mixing services, secret sharing allows data to be stored in a decentralised way across N parties such that any K parties can work together to reconstruct the data, but K-1 parties cannot recover any information at all. Alternative – thay thế add-on data privacy tools include ring signatures and stealth addresses which hide the recipient of a transaction and can be used by any blockchain. Ring signatures—firstly introduced by Rivest, Shamir, and Tauman in “How to Leak a Secret” (2001) and its variant, linkable ring signatures, allow users to hide transactions within a set of others’ transactions. In this case the transaction is tied to multiple senders’ private keys but only one of them is the initiator – người khỏi xướng. Thus, the verifier may only identify that one of them was a signer, but not who exactly that was. In the case of stealth addresses, a receiver generates a new dedicated address and a “secret key” and then sends this address to someone who he wants payment from. The sender use the address generated by the receiver plus a “nonce” (one time random number) in order to generate the address he/she will send funds to. The sender communicates the nonce to the receiver who can unlock the address by using the nonce and the secret key generated earlier. Monero is an example of a blockchain that aims to achieve privacy through the use of traceable ring signatures and stealth addresses.

9.Codebase

The codebase of blockchain technologies delivers information about which challenges a developer could face and what kind of changes the underlying programming language could undergo. Therefore the main component ‘Codebase’ is essential to align – căn chỉnh and increase the efficiency of blockchain-related IT architectures

9.1 Coding language:

Coding language illustrates – minh họa the interconnectivity – kết nối of programming languages of blockchain technologies

- Single Language: Bitcoin has released Bitcoin Core version 0.13.1 in the underlying coding language C++, As Bitcoin is open source, implementations occurred in different languages.

- Multiple language: Ethereum uses C++, Ethereum Virtual Machine Language, and Go, which enables more interaction – tương tác with other languages.

9.2 Code License:

The Code License illustrates – minh họa the possibility of changes to the source code of the underlying technology:

- Open- Sources: Regardless of the exact licence used for specific projects, we refer only to the openness in the source code as the only differentiating factor. Bitcoin core developers have continuously licenced the source code under the MIT licence prevents multiple implementations. It also allows for continued development, more code growth, and adoption at a faster pace.

- Closed- Sources: For private implementations of blockchain-based systems, the source code is not necessarily openly distributed, most the blockchains running on the Ethereum Enterprise Alliance (rather than on the public Ethereum blockchain) use closed-source codes, có nguy cơ tồn tại các lỗi chưa được khắc phục hoặc các đặc điểm không được báo cáo có thể vi phạm các điều kiện sử dụng và hoạt động dự kiến, the code may be kept outside of reach for users.

9.3 Sofware Architecture:

The Software Architecture refers to the high level structures of the blockchain system. Each structure is composed of software elements, the relations between them, and the properties that emerge from those elements and relations. The choice of the software architecture is very important in order to better manage changes once implemented.

- Monolithic Design: all the aspects of a decentralised ledger tivity – sự thận trọng, the “mempool” broadcasting of transactions, criterion for consensus on the most recent block, account balances, nature of smart contracts, user-level permissions are handled by a blockchain built as a single-tier software application without modularity – mô đun.

- Polylithic Design: The Polylithic approach decouples the consensus engine and P2P layers from the details of the application state of the particular blockchain application Between the application process and its application-agnostic “consensus engine” (TenderminCore), it offers a very simple API which enables it to run Byzantine fault-tolerant applications, written in any programming language, not just the one the consensus engine is written in also Hyperledger Fabric follows a polylithic design as it is composed of interchangeable modules representing different components of blockchain technologies.

10: Idenity Management

Ensures secure access to sensitive data to establish a suitable governance model for the blockchain, This is a complex matter, as different levels of authority, accountability and responsibility are attached to different type of participants. Generally, the set of rules are defined and enforced through mechanisms intrinsic- nội tại to the system itself. The subcomponents also eventually determine the concept of digital identity that users end up having within the systems.

10.1 Access and Control Layer:

When establishing the right governance structure for a blockchain it is important to consider the ledger construction. Depending on its purpose, the ledger could be run by a central authority and governed by it, or it could be run in a decentralised fashion according to a set of governance rules adhered – dính chặt to and enforced by participants on the blockchain network. The governance structure determines the authorisation and the control policy management functions. Those rules provide permission for users to access to or use blockchain resources. Those are a set of rules that manage user, system and node permissions that must be followed in security-related activities. Blockchains may have different permissions according to different levels of access to and control of data. The distinguishing features must answer to the following questions: Which users have “read” access? Which users have “write” access? Is it there anyone who can “manage consensus”. On one side, private blockchains are generally those with a set of constrained “read/write” access alongside a consensus algorithm which allows only a pre-selected group of people to contribute and maintain blockchain integrity – sự toàn vẹn. Instead, public blockchains do not control “read/write” access or in the consensus algorithm for any given set of participants:

- Pubic blockchain: In this case, there is no preference in access or in managing consensus. All participants (nodes), have “read/write” access and without any control can contribute to the update and management of the ledger.

- Permissioned Public Blockchain: In this case “read” access is enabled for all users, however “write” access and/or “consensus management” require permission by a pre-selected set of nodes.

- Permissioned Private Blockchain: In this case, “read/write” and “consensus management” rights can only be granted by a centralised organisation. One example of this type is Monax (formerly known as Eris).

10.2 Identity Layer:

The onboarding and offboarding of nodes / entities to a blockchain network is handled differently by various software solutions. By identification we mean the capability to identify an entity uniquely in a given context. Digital identity can be defined as a set of identifying attributes of an entity that together enable the unique identification of the entity in a context (UID) A vital part of any identity system (and most information systems) is that a UID is managed throughout the entity’s lifecycle to protect it from negligence and fraud, and to preserve the UID’s uniqueness. A UID can then be assigned to the identity and used to link or bind the entity to the claimed identity and to any digital credential issued to the entity. This digital credential – chứng chỉ acts a trusted proxy for the physical or logical entity and is used to support a wide range of personal and trust-related functions such as authentication, encryption, digital signatures, application logins and physical access control.

- KYC/AML: Know-Your-Customer (KYC) and Anti-Money-Laundering (AML)-compliant blockchains have the ability to validate organisations and their attribute data from authoritative sources to ensure the quality of data written to the blockchain and linked to identifiers in the blockchain.

- Anonymous: A common misunderstanding regarding the level of anonymity within Bitcoin networks is that the majority of the users do not distinguish between anonymity and pseudonymity. The Bitcoin protocol has no identity layer to identify the users, which could lead to misuse of Bitcoins and money laundering activities through its blockchain network, but to control approaches to anonymity in Bitcoin and other cryptocurrencies.

11. Charging and Rewarding System

Blockchain systems incur- gánh chịu operational and maintenance costs that are generally absorbed -hấp thụ by the participants in the network. Different kinds of cost models are applied according to: 1) the architectural configuration design; 2) the governance system; and 3) the data structure and the computation required on-chain. One of the costs common to the wide majority of blockchains is the verification cost. This is required to sustain – duy trì the validation process of the transactions that compete to be appended to (and never removed from) the ledger.

11.1 Reward System

This subcomponent illustrates – mô tả the reward mechanisms automatically put in place and triggered by the systems in order to compensate – đền bù active members contributing to data storage or transaction validation and verification:

- Lump-Sum Reward: Individuals taking part in the storage, validation, and/or verification processes may be rewarded for their action

- Block + Security Reward: In other blockchain-based technologies, like Ethereum, the blockchain rewarding system includes, besides the block reward, a reward for including forked blocks that are still valid in the validation. The purpose of the design is to incentivize – khuyến khích cross-validation of transactions

11.2 Fee System

A different kind of reward is that provided directly by the users to other participants in the system when launching any request in the network for storage, data retrieval, or computation and validation

- Fee Reward: is composed of the fees that users are required to contribute when using a blockchain. The fee system has been shown to play an important role in the way verifiers behave. This kind of design-time consideration ought not to be neglected – bỏ mặc, though it often is

+ Optional Fees: In Bitcoin and related technologies users can optionally pay a voluntary fee for the validation process. This fee is optional, but it is assumed that the larger the fee is, the lower the processing time for a transaction, as miners will be more incentivized – khuyến khích to include it in a block. Moreover, given that the coinbase reward halves approximately every four years, currently, the reference Bitcoin client refuses to relay transactions with a zero transaction fee value

+ Mandatory Fees. Some systems like Stellar force all users to include fees in any transaction added into the system.

+ No Fees. In comparison, Hyperledger Fabric is a blockchain solution for businesses, which combines a permissioned network and an identity layer without any transaction fees.

- Fee Structure: When provided by the system, fees can follow either a fixed or a variable structure

+ Variable Fees: the fee is somehow linked to the “size” of the request. the larger the transaction size, the higher the fee the user will pay in order to compensate – đền bù for taking up space inside the block. Miners usually include transactions with the highest fee-per-byte value first The user can decide how many “Satoshis” to pay per byte of transaction a Satoshi is 0.00000001 Bitcoins. At the time of writing, this implies that the transaction will be included in the next 2 blocks. However, to avoid queuing, the user can opt to increase the fee. At the time of writing, the fastest and cheapest transaction fee is currently 360 Satoshis/byte.

+ Fixed Fees: In this case, the fee is linked to the request, not to its “size.” For example, in Enigma every request in the network for storage, data retrieval, or computation has a fixed price, similar to the concept of Gas in Ethereum. However, since Enigma is a Turing-complete system, the fee can be different depending on the specific request.