ISSN: 2093-5374 / E-ISSN: 2093-5382

A Taxonomy Guideline for Blockchain Platforms

Ahmed Afif Monrat[1*], Olov Schelén[2], and Karl Andersson[3*]

[1*]Luleå University of Technology, Sweden.
ahmed.monrat@ltu.se, https://orcid.org/0000-0001-9801-7625

[2]Luleå University of Technology, Sweden.
olov.schelen@ltu.se, https://orcid.org/0000-0002-4031-2872

[3*]Luleå University of Technology, Sweden.
karl.andersson@ltu.se, https://orcid.org/0000-0003-0244-3561

Received: February 26, 2024; Revised: April 22, 2024; Accepted: May 26, 2024; Published: June 29, 2024

Abstract

Traditional methods of reaching consensus in monetary systems depend on centralized authorities that are considered trustworthy. Blockchain challenges the traditional model by establishing consensus through a decentralized network of peers, which is responsible for validating transactions and preserving a chronologically ordered ledger of transactions. Utilizing blockchain technology has extended beyond cryptocurrencies to encompass various industrial systems. Nevertheless, much ambiguity surrounds the benefits of employing blockchain technology compared to competing technological solutions. The limited adoption of blockchain-based systems can be attributed to the absence of clear guidelines on blockchain governance and the difficulty in evaluating the pros and cons of blockchain solutions. The existence of various blockchain variants, including permissionless and permissioned, can provide challenges in selecting an appropriate solution for a given use case. This article aims to tackle these difficulties by analyzing blockchain governance and its associated tradeoffs, encompassing energy usage, consensus mechanisms, performance, and security considerations. We present a taxonomy guideline that aims to offer valuable insights into the tradeoffs involved and assist in efficiently selecting the appropriate governance structure for blockchain-based solutions across different scenarios. The taxonomy under consideration examines several characteristics of blockchain technology, encompassing energy consumption, consensus techniques, performance, and security elements. These factors are analyzed to provide an appropriate governance model for a blockchain-based solution, such as permissionless, permissioned, or consortium. Moreover, this research study presents a comprehensive evaluation of various consensus mechanisms, including Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Authority (PoA), while taking into account significant characteristics.

Keywords: Blockchain Taxonomy, Consensus, Double Spending, Scalability, Smart Contract, Transaction Verification.

1 Introduction

The technological framework that underlies cryptocurrency is commonly referred to as blockchain (Ali et al., 2016; Garriga et al., 2021; Mas'ud et al., 2021). Users can engage in direct monetary transactions

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 15, number: 2 (June), pp. 286-308. DOI: *10.58346/JOWUA.2024.I2.019*

*Corresponding author: [1,3]Luleå University of Technology, Sweden.

without the involvement of conventional middlemen, such as banks or payment processing firms, thanks to decentralized peer-to-peer networks and cryptographic tools (Decker & Wattenhofer, 2013). Within a distributed ledger framework, a blockchain can authenticate and retain diverse types of transactions (Eyal et al., 2016), extending beyond financial transactions only (Udayakumar et al., 2023). The widespread interest in blockchain technology is seen in the rapid growth of blockchain networks and the convenient adoption facilitated by blockchain-as-a-service (Eyal & Sirer, 2018). Utilizing blockchain technology enables the development of decentralized applications and facilitates the achievement of interoperability. Consensus can be reached across a vast network of participants without mutual trust, courtesy of blockchain technology. This consensus is crucial for maintaining a decentralized ledger of transaction data. This obviates the need to depend on a solitary point of confidence, such as a reputable central entity with the ability to govern the system. Applications developed utilizing blockchain technology can benefit from transaction non-repudiation, global transaction order, equitable access, and data immutability (Gervais et al., 2016). The utilization of blockchain technology elicits a combination of optimistic expectations and cautious suspicion. This technological innovation has garnered considerable attention from diverse sectors following its notable achievements in cryptocurrencies, particularly in Ethereum and Bitcoin. Subsequently, many companies have undertaken trials with blockchain technology, including sectors such as pharmaceuticals and food production, banking and finance, and data security establishments (Sreenivasu et al., 2022). The absence of a third-party intermediary allows for the settlement of transactions through a decentralized peer-to-peer consensus mechanism, among other notable features. Another crucial characteristic involves maintaining an unchangeable transaction log encompassing an indisputable record of previously executed machine-driven smart contracts, which may be customized to fulfill certain criteria and constraints. Therefore, blockchain technology is often regarded as a "disruptive innovation" and is frequently referred to as Internet 2.0 within the blockchain community (Frizzo-Barker et al., 2020).

Nevertheless, blockchain technology is subject to certain technical constraints. The potential erosion of network privacy arises from information stored on a blockchain being readily accessible to all nodes within the network through a shared ledger. When considering scalability and throughput, it is observed that certain public blockchain platforms have a limited capacity to handle approximately 320 transactions per second on average. In contrast, widely used payment systems like VISA can process thousands of transactions per second (Rodrigo et al., 2020). Therefore, the conventional blockchain network is inadequate in fulfilling the demands of many usage scenarios, particularly those involving real-time processing. In designing applications based on blockchain technology, it is imperative to assess the characteristics and setups of the blockchain system and subsequently examine their impact on the overall quality attributes of the system. In practical terms, the lack of dependable resources for technology assessment greatly complicates such comparisons. A notable finding pertains to the challenge faced by numerous organizations in assessing the necessity of implementing blockchain technology inside their applications, as well as determining the specific form of blockchain that would effectively address their existing issues.

This work aims to present a taxonomy that effectively categorizes significant architecturally relevant attributes of diverse blockchains. The purpose of this document is to serve as a foundation for designing systems that utilize blockchain technology. During the design phase, the taxonomy elucidates the tradeoffs that emerge from design choices pertaining to blockchain systems (Kumar et al., 2023). The taxonomy was formulated by an extensive review of scholarly articles, existing blockchain-based solutions, technical forums, and our research expertise in blockchain. The tradeoff analysis encompasses various factors such as governance, energy usage, consensus, performance, and security. The tradeoff study encompasses an examination of the energy implications associated with different consensus approaches, namely Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Authority (PoA), while considering significant features. This study presents several notable contributions:

- Tradeoff analysis regarding governance and roles.
- Tradeoff analysis regarding energy consumption, consensus, security, and performance.
- The taxonomy guideline on the above tradeoffs.

Section II provides background on blockchain technology. Section III discusses the related works, while Section IV describes the development and details of our taxonomy. Section V presents a precise tradeoff analysis considering the properties of the proposed taxonomy architecture. Section VI concludes the article and provides insights into the future scope.

2 Background

A blockchain is an organized set of blocks, each containing a number of transactions (Signorini et al., 2020). Each block carries a hash representation of the preceding block in a blockchain, which links them together. Existing transaction data cannot be altered without invalidating the hash chain; hence, deleting or updating it is impossible. When coupled with technical limitations and block creation incentive schemes, this may prevent manipulation and change of data stored in the blockchain. The first blockchain, Bitcoin, acted as a public ledger for recording financial transactions that were cryptographically signed (Puthal et al., 2018).

Digital signatures and public-key cryptography are commonly employed to authenticate accounts and ensure the authorization of transactions carried out on a blockchain (Fill & Härer, 2018). Transactions are bundles of data encompassing function calls, such as smart contracts and parameters, which may involve monetary value when utilizing Bitcoin. Cryptographic techniques and algorithmic protocols are utilized to guarantee the integrity of a transaction. Transferring digital assets across nodes within a blockchain network is commonly called a transaction (Meunier, 2018). While executing a transaction within a decentralized blockchain network, the sender initially employs a digital signature to authenticate the transaction. Subsequently, all executed transactions are transmitted to an unverified transaction pool. The peer nodes select a subset of these transactions and endeavor to validate their legitimacy by applying predetermined rules and referencing the transaction history and account balances. The procedure effectively mitigates the risk of double-spending vulnerabilities. A double-spending problem arises when a node initiates two transactions with the same input or without sufficient cash, as documented in reference (Akbar et al., 2021). Miners engage in the process of incorporating validated transactions into a block. Miners are the nodes that allocate their computer resources towards the validation of blocks (Kalinin et al., 2024). When building a new block, a miner commits various resources, such as CPU power, cash, or reputation, as determined by the consensus mechanism. The individual responsible for processing the block will ultimately be compensated with transaction fees and a reward for creating the block. The remaining nodes within the network engage in a consensus process to authenticate the newly formed block. This procedure serves as a mechanism for a decentralized network to establish a consensus regarding the block's integrity collectively.

Every verified block will be appended to the current chain and each participant's individual copy of the unchangeable ledger. The new block will be assigned a position within the chain about the prior block through the utilization of a cryptographic hash pointer. Following this procedure, the preceding blocks will undergo reconfirmation whenever a novel block is added to the preexisting chain. The finality of a block is achieved once it has received a minimum of six confirmations (Del Castillo, 2017).

In constructing subsequent blocks, it is customary to designate the longest chain of validated blocks as the prevailing chain, disregarding shorter branches or unauthorized blocks. The time it takes to create a block in a global network successfully is contingent upon the consensus procedure (Nguyen et al., 2019). A blockchain network encompasses several consensus techniques, such as proof-of-work (PoW), proof-of-stake (PoS), and Practical Byzantine Fault Tolerant (PBFT), among other alternatives. By the stipulated assurances and the consensus-based methodology, several concepts can be contemplated concerning transactions that can be verified, finalized, and thus rendered unalterable.

The second generation of blockchains enables the establishment of a publicly accessible ledger that records the outcomes of computational processes. Smart contracts refer to computer programs that can be deployed and executed on a blockchain network (Destefanis et al., 2018). Including triggers, conditions, and business logic in smart contracts allows for implementing more complex programmed transactions (Liu et al., 2018). Escrow is a straightforward illustration of a contract-based service that facilitates the retention of funds until the conditions specified in the smart contract are fulfilled. Nevertheless, it is common for them to bear minimal relevance to formal agreements. Ethereum is commonly acknowledged as a prominent blockchain platform that enables the implementation of smart contracts across various sectors.

3 Related Work

The following studies of Blockchain taxonomy and decision-making theories for choosing a Blockchain application were found to be within the study's purview. A taxonomy of decentralized consensus systems was published (Glaser & Bezzenberger, 2015). This makes it possible to analyze and categorize the new technology in this setting. Six dimensions make up Glaser and Bezzenberger's taxonomy. Underlying Value, Community, Service Focus, Code Basis, and Token Usage are these dimensions. The dimensions are also given attributes, allowing for even more separation between the dimensions. By creating an ontology, (De Kruijff & Weigand, 2017) outlined the language used in Blockchain technology. The six aspects in their terminology—Type, Consensus, Governance, Trust, Scalability, and Use—are used to derive kinds of the Blockchain once more. In their article (Lai & Chuen, 2018), the blockchain technology. Their objective is to determine the differences and affinities among various Blockchain kinds. They concentrate on achieving unanimity while they accomplish this. Distributed Consensus Protocols, Liveness and Safety, No Correlation Between Nodes Failures, Resiliency, Types of Fault, Synchrony, Authentication and Non-repudiation, Scalability and Performance, Turing-Complete, Smart Contract, and Smart Contract Oracle are among the eleven qualities they identify.

Distributed ledger technology (DLT) uses, and effects were examined (Maull et al., 2017). The main topic of this article is the decision-making process that goes into choosing how to employ DLT in a certain application scenario. A summary of the classification of Blockchain designs was released (Mattila, 2016) as part of their research on the technology's potential for disruption. He employs the Participation Restriction and Specificity of the Interpretation aspects for this. Meijer & Ubacht, (2018). taxonomy of Blockchain technology was derived to capture the effects of blockchain implementation. He claimed that blockchain should be divided into Public/Private and Permissionless/Permitted categories. The degree of decentralization of the network under consideration was cited (Klein & Prinz, 2018) as the key categorization characteristic of Blockchain technology. As a result, the Blockchain is typically thought of as a type of decentralized database. A Blockchain taxonomy with a tree topology was released (Tasca & Tessone, 2017). Only the so-called key components are covered here due to the Blockchain taxonomy's extensive and extremely deep definition. The eight main components listed by the authors are: Identity Management, Native Currency/Tokenization, Extensibility, Transaction Capabilities, Consensus, Charging and Reward System, and Security and Privacy (Monrat et al., 2022).

A comparison of the three Blockchain types—Public, Private, and Permissioned—was published in 2018 (Wieninger et al., 2019) based on seven criteria: cost per transaction, performance throughput, performance delay, system trust, scalability, maintenance, and openness. They employ a relative classification in high, medium, and low to evaluate the types in the relevant criteria. A decision aid is published (Wüst & Gervais, 2018) to determine whether and which sort of Blockchain should be utilized for a project. Given that the potential recommendations are almost identical, the decision tree is comparable to that of Maull et al. Nevertheless, these recommendations are not similar to the decision-making questions that led to them. A Blockchain taxonomy that includes all of the key features of Blockchain technology is presented by Xu et al. in their article (Liu et al., 2018). The taxonomy is broken down into five 'design decisions': the New Blockchain, the Consensus Protocol, the Consensus Protocol Structure, the Blockchain Scope, and the Structure. Security and Scalability are the two descriptive groups into which the design choices Consensus Protocol, Protocol Configuration, and New Blockchain are split. A taxonomy for so-called decentralized consensus systems is described (Yeow et al., 2017) Not just Blockchain technology but also non-Blockchain-based technologies are taken into account. The work aims to determine the benefits and drawbacks of the current systems in use. Three categories—Data Structure, Scalable Consensus Ledger, and Transaction Model—make up their taxonomy. From the literature, (Zheng et al., 2018) recognized the three types of blockchain: Public, Consortium, and Private and evaluated them in terms of specific qualities. Consensus Determination, Read Permission, Immutability, Efficiency, Centralized, and Consensus Process are the six essential qualities that the authors develop.

However, these studies only partially address the tradeoffs and difficulties in establishing an appropriate blockchain governance framework that aligns with the objectives of certain use-case situations. Our taxonomy aims to fill this research void by examining blockchain governance and its associated tradeoffs, such as energy consumption, consensus, performance, and security. This analysis helps identify a blockchain-based solution's most appropriate governance structure in different scenarios.

4 Taxonomy Architecture of Blockchain

Taxonomies are employed in software architecture to enhance comprehension of existing technology. To build a taxonomy, it is crucial to categorize previous work inside a clear framework that enables an architect to methodically explore the design possibilities, making it easier to compare and evaluate different design solutions comprehensively. Our taxonomy offers a structured system for classifying and defining the different features and categories that can describe blockchains and their use in diverse systems. This tool aims to aid software architects in evaluating and comparing various blockchains. Furthermore, its objective is to streamline research on architectural decision-making frameworks inside blockchains and blockchain-based systems. We have established a design classification system that considers blockchain technology's characteristics and management aspects, as illustrated in Figure 1. The taxonomy is formulated by an extensive review of scholarly articles (Xu et al., 2017; Ismail et al., 2019; Tasca & Tessone, 2017; Weking et al., 2020; Hussien et al., 2019; Labazova et al., 2019), existing blockchain-based solutions, technical forums, and our research expertise on blockchain, as well as the development of prototypes.

Blockchain Taxonomy Properties

The taxonomy properties refer to the features which could define the governance model needed for different use-case scenarios. Considering the trade-offs among these features an organization or consortium could decide whether to adopt permissionless or permissioned governance architecture for their business model. For the proposed taxonomy architecture, we have considered the following properties:

Energy Consumption: Energy consumption denotes the quantity of energy or electricity the blockchain technology utilizes. The computing power used for the consensus or mining process directly impacts how much energy a blockchain or cryptocurrency network uses. Bitcoin utilizes Proof of Work (PoW) consensus, in which miners compete to generate a new block from a certain set of pending transactions to discover a hash value that meets the required criteria. This process, called mining, demands intensive use of computational resources, which consumes much electricity. A Bitcoin transaction requires 1,173 kilowatt-hours (kWh) of electricity, enough to run a normal American house for six weeks (Chohan, 2022). Conversely, a blockchain network that utilizes PBFT consensus requires far less energy than PoW but sacrifices scalability regarding the number of miners.

Incentive for mining: Every legitimate block provides an economic incentive for the mining process (Monrat et al., 2019). Usually, the reward is made up of a particular quantity of the related cryptocurrency as well as the transaction costs (Podvalny et al., 2021). For instance, several miners may be engaged in confirming transactions and constructing a block in Bitcoin, but the winner usually discovers the hash first. The block creation incentive, which is presently 6.25 BTC, is given to the miner who invests significant computational power into publishing a block. The miner is also eligible to get transaction fees and the block reward. But not all blockchain platforms—especially the permissioned ones—follow the same protocol. Most permissioned blockchain systems don't offer incentives for block mining or validation tasks.

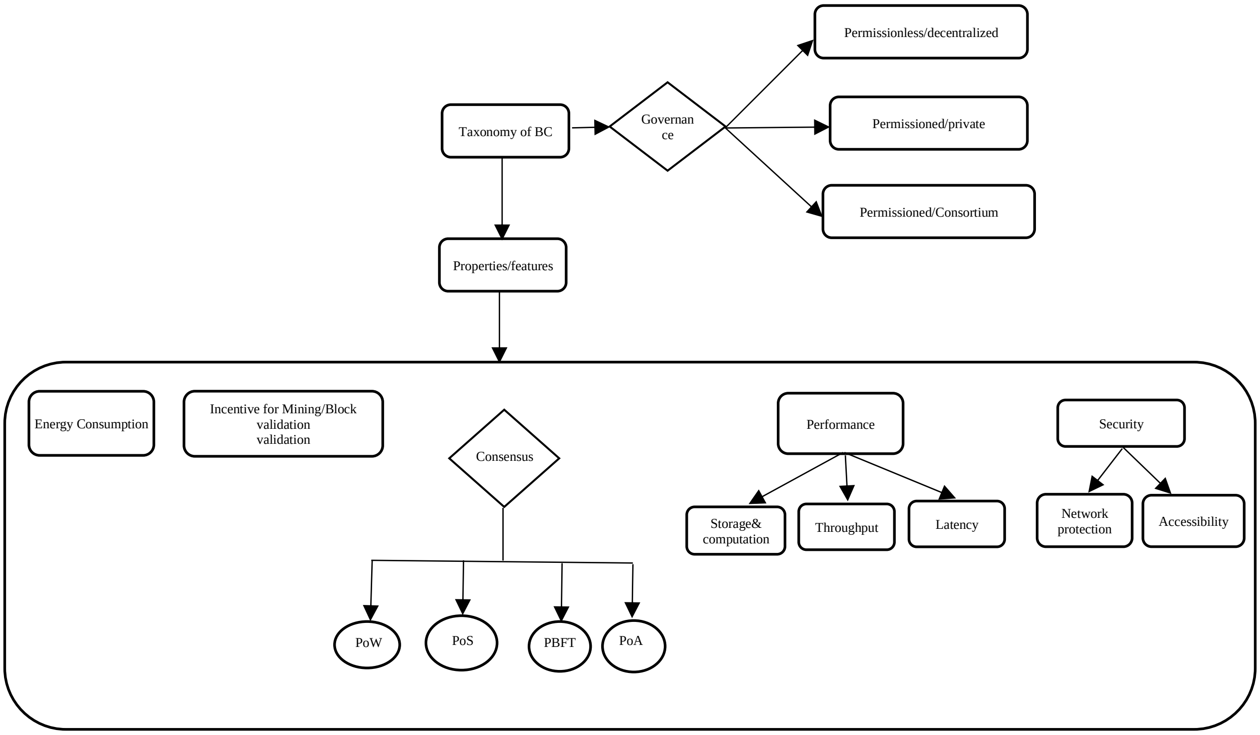

Figure 1: Taxonomy Architecture of Blockchain Technology

Consensus: In a blockchain network, a shared ledger is continuously updated with an expanding list of transactions. This procedure is governed by multiple entities or nodes, which may lack mutual trust. During the processing of a block, these nodes must carry out various tasks, including authentication and verification of transactions, block mining, network communication, and the collaborative establishment of trust within the blockchain system without the need for a central authority. There is a potential for individual nodes to be malevolent, deviate from the primary objective, or cause network connectivity to fail. To maintain a consistent and reliable service that guarantees the availability, confidentiality, integrity, and accessibility of data, it is necessary to establish a secure mechanism that enables most participant nodes to collectively agree on which information should be added to the blockchain. This technique is commonly referred to as consensus.

Performance: Network performance is the speed at which users and clients receive the desired service. From a system standpoint, transaction latency, throughput, storage, and computational capacity are key indicators of blockchain platform performance. Blockchain computation and storage uses distributed ledger technology to use cryptographic methods to store and verify transaction data in a decentralized network (Shahriar Hazari & Mahmoud, 2020). A network-wide perspective of latency is the time it takes for a transaction's effects to become available to users elsewhere on the network (Ray et al., 2020). The rate at which legitimate transactions are added to a blockchain within a predetermined time is known as transaction throughput. Benchmarking tools like Blockbench and Hyperledger Caliper can be used to measure the performance metrics of blockchain platforms. Metrics like fault tolerance, scalability, latency, and throughput may all be measured with these instruments (Monrat et al., 2020). Workloads and blockchain platforms can be integrated via a straightforward set of APIs. Permissioned governance models, whether fully or partially centralized, function noticeably better than permissionless networks, according to studies and trials on blockchain technology. The intricate consensus techniques used by decentralized, permissionless blockchain systems may be the primary cause. Permissioned blockchain systems have the potential to process transactions more quickly, but they usually don't scale up the number of miners or validators to the same extent (Danielle et al., 2024).

Security: Using private and public keys is an essential element of security and anonymity in a blockchain network. Blockchain systems employ asymmetric cryptography to protect user transactions. Each user possesses a public and private key in these systems. Public keys on the network can be shared between users without compromising user privacy. With the use of a hash function and their public key, each user has an address. Sending and receiving assets is made easier on the blockchain by the addresses, especially when it comes to virtual currencies like Bitcoin. Private keys are utilized when using digital signatures to ensure security and safeguard user identity (Giji Kiruba et al., 2023). Users on the blockchain can access their funds and virtual wallets by using private keys, which serve as a kind of authentication. Users must give a digital signature, generated when the private key is obtained, to transfer money to other users. This is accomplished through created addresses, allowing individuals to transact without disclosing their identities. A peer in the blockchain network is said to be able to maintain their anonymity. However, as recent research on the Bitcoin network has demonstrated, it is possible to correlate a member's transaction history to ascertain their genuine identity. It should be noted that blockchain networks are still susceptible to security vulnerabilities. For blockchain networks, several attack strategies have been developed, including as double-spending, Sybil assault, 51% hash control, and selfish mining.

Tradeoff Analysis of Blockchain Governance

In its fundamental essence, governance pertains to a collection of regulations that every participant or user consents to abide (Monrat et al., 2020). The primary objective is to meet the users' requirements with the existing resources while assuring the system's long-term sustainability. Therefore, effective governance has greater significance for any institution, company, or service, especially during periods of growth. Due to the centralized nature of most businesses and governing bodies, they are often governed by a leadership team (Zachariadis et al., 2019). Blockchain is a distributed network comprising numerous components and functionalities. This dynamic system should consistently aim to adjust and respond to the users' needs to offer enhanced user control and advantages. Blockchain governance encompasses the mechanisms by which the blockchain system can adjust and stay pertinent in response to evolving requirements and circumstances (Rondinelli, 2017). Blockchain governance necessitates the incorporation of two crucial attributes: upgradability and adaptability. According to several specialists, a significant factor in remaining up-to-date and competitive is a blockchain network's ability to expand and enhance itself in response to ongoing advancements.

Blockchain governance usually involves four central communities:

1. Developers: Developers are responsible for maintaining the main code underpinning the blockchain. They possess the authority to add or remove code to modify the central code but cannot put it into effect networkwide.
2. Node operators: The node operators decide whether to implement the feature recommended by the foundation on their nodes or not since they have a full copy of the blockchain ledger and run it on their computers.
3. Foundation: A foundation can be a business or a nonprofit entity that acts as the representative of larger investor and supporter communities when negotiating with code authors and node operators, as well as frequently taking on a marketing role. For instance, Ripple is a project that is run by a firm, in contrast to the foundations that Bitcoin, Ethereum, and other cryptocurrencies each have. The Foundation decides when to recommend switching to alternate solutions and when to modify the consensus mechanism.
4. Token Holders: The individuals and organizations that possess blockchain tokens are known as token holders; for instance, investors, and supporters. They have varying degrees of voting privileges on what features to adopt, set prices, etc., depending on the nature of various blockchains.

On-chain & Off-chain Models: Both public and permissioned platforms can operate transactions following either on-chain or off-chain models. On-chain transactions are defined as transactions that are confirmed and stored on a blockchain (Luminea et al., 2021). The on-chain transactions are considered valid when the blockchain has been updated to reflect the transactions on the public ledger. Once they have been validated and logged on the network, on-chain transactions cannot be altered. Hence, on-chain transactions provide transparency and security. The technique of Blockchain’s verification determines the pace of on-chain transactions. On the other hand, on-chain transactions have certain disadvantages, such as slow processing times and higher fees (Eberhardt & Tai, 2017). Onchain model is democratic; a built-in voting mechanism of the Blockchain allows for direct democracy in an on-chain model, which may be tailored to meet the requirements of a network (Kim et al., 2018). The node operators’ participation in governance is reduced to following the on-chain process defined by the foundation. The issue regarding scalability is still a major concern here. The foundation’s ability to govern the community becomes more complicated as the community of node operators grows further. The blockchain community has diverse opinions regarding the value of the on-chain model (Grover et al., 2021). Any modifications might theoretically be encoded into the Blockchain, voted on by the permitted entities, and then incorporated automatically into a code. In reality, this strategy raises some significant concerns, including:

a) All community members should behave in the group's best interests, which is not always the case in a big, diverse community.
b) On-chain model does not necessarily prevent decisions from being made by a small group of people. According to Vitalik Buterin, co-founder of Ethereum, low voter participation rates exacerbate this issue; one significant vote on the Ethereum chain attracted only 4.5 percent of the electorate (Reijers et al., 2021). As a result, it might be conceivable for a small number of people to influence an election with a very small portion of all coins.
c) In practice, achieving long-term sustainability with an experimental governance model will take more effort and time.

Off-chain transactions occur outside of the network. Off-chain transactions entail the participation of multiple individuals who mutually commit to ensuring the authenticity and completion of the transaction, either independently or with the assistance of a third party (Robinson, 2017). Off-chain transactions occur independently of the core blockchain without any impact on its functioning. This obviates blockchain miners' need to await validation, expediting the process and reducing transaction costs. Off-chain transactions do not appear on the primary blockchain, resulting in the absence of a network record for these transactions and their financial details. This can provide challenges in case of disputes among many parties. The off-chain strategy aims to achieve a balance among various stakeholders within a blockchain community, including core developers, node operators, token holders, and foundations (Dursun & Üstündağ, 2021). While the chain architecture enables the decentralized and parallel functioning of multiple off-chains, each chain exhibits a highly centralized governance structure, where decisions are predominantly decided by a limited number of individuals, frequently only two. However, off-chain systems provide significantly more concurrent operational flexibility compared to traditional on-chain systems, albeit with some degree of centralization. Table 1 presents a comparison of transactions conducted on-chain versus off-chain, as referenced by sources (Brinkmann & Heine, 2019; Singh et al., 2021; Miyachi & Mackey, 2021; Hepp et al., 2018).

Tradeoffs between On-chain and Off-chain model: The validation procedure conducted by miners causes delays in processing transactions within the on-chain framework. Nevertheless, having the transaction verified by participants and publicly recorded on the blockchain network greatly enhances security.

Table 1: Comparison of Off-Chain and On-Chain Models

Attributes	Off-Chain Models	On-Chain Models
Consensus	Off-chain Voting with a limited number of nodes concurrent in different off chains.	Multi-stage on-chain voting open to all nodes (globally serialized)
Authority	Unbalanced power of node operators (filtering proposals) and core developers (for decision making) and foundations (for negotiations).	Open to all stakeholders, On-chain ballot and risks of low participation and domination by experts or whale token holders
Fairness	Few Nodes have power and can delay or reject proposals	Many nodes share control and power in decision making
Complexity	High. Not easy to understand the reference implementation of a proposal. Parallelism, routing across off-chain channels, etc.	Moderate. Complex proposals are serialized
Performance	process transactions faster than on-chain models.	Existing models are rather slow and staged

The choice between on-chain and off-chain transactions depends on the parties involved and their priorities. If the major goals are security, immutability, and a verified transaction, then an on-chain transaction would likely be the better choice. However, if speed and low transaction costs are of utmost importance, then an off-chain transaction would be preferable. The governance model of a blockchain can be categorized as a consortium, permissioned, or permissionless, according to the specific characteristics of the blockchain taxonomy, including whether it operates off-chain or on-chain. In the subsequent part, we will discuss that.

1. Permissionless/Decentralized Blockchain Platform

Customers who utilize a bank, such as one with a centralized system, depend on its systems to update their account balances precisely after a bank transfer. A sole entity may have complete control over the system, including updating the system's operating software and modifying the backend databases. A central authority is a singular trust source in a centralized system. In contrast, individuals can establish consensus on transactions and ownership without depending on a specific intermediary in a decentralized system such as Bitcoin. This system is decentralized and highly available because every node in the Bitcoin network receives and verifies every block and transaction using the core consensus rules of Bitcoin. Additionally, each node provides the essential functionality to facilitate transactions. The Bitcoin network currently has approximately 12,835 nodes as of March 2022 (Hao et al., 2021). A system can possess both centralized and decentralized components and functionalities equally. There are two distinct types of centralized systems. Corporate monopolies, local governments, and courts are all instances of monopolistic service providers. The second category comprises alternative suppliers such as banks, cloud computing businesses, and online payment processors. Each centralized system represents a singular vulnerability or reliance for its users. However, the termination of a singular service provider affects its users in the event of many providers, who may opt to employ different providers or switch providers. Cloud parties are examples of centrally managed services typically distributed across data centers.

Ethereum and Bitcoin are instances of public permissionless blockchains that exhibit complete decentralization. Permissionless public blockchains are fully inclusive, allowing anybody to participate in the network, create new blocks, and validate transactions (Avan-Nomayo, 2021). The main application of these blockchains is facilitating bitcoin exchange. Moreover, the collective motivation of all network participants to improve the public network fosters trust throughout the entire user community. Sybil attacks need anonymous validators to offer decentralized defense against an assailant's dissemination of antagonistic anonymous nodes. Bitcoin provides a certain level of protection against this issue because of its proof-of-work system, which ensures that the aggregate processing power is more important for maintaining integrity than the number of nodes.

2. Permissioned/Private Blockchain Platform

In contrast to a public blockchain, a private blockchain is a permissioned and restrictive one that functions within a closed network (Monra et al., 2020). This type of blockchain is mostly employed within an organization where a restricted number of participants operate the network. Eris and Ripple are instances of networks that require authorization to access. This solution is most suitable for corporations and organizations that intend to utilize blockchain for internal purposes. The main differentiation between private and public blockchains is in their accessibility. Public blockchains are open and easily available to anyone, but private blockchains are limited to a specific group of nodes (Peng et al., 2021). Due to the presence of a sole organization responsible for maintaining the network, a private blockchain exhibits a higher degree of central control. Permissioned or semi-permissioned blockchains offer improved data processing speed and decreased time delays compared to public blockchain platforms. This is because permissioned blockchains restrict access to approved participants only. In a private blockchain, scalability issues are minimized because the network controls the number of nodes involved in validating transactions and creating blocks. In contrast to a public blockchain, the network does not permit individuals to join or exit and engage in the validation procedure freely. Additionally, it provides a cost-effective solution in terms of energy consumption compared to the public platform, as the consensus approach is significantly less demanding. The appropriateness of a permissioned blockchain may also be contingent upon the size of the network. However, the permit management technique has the potential to be a single point of failure, both operationally and commercially.

3. Consortium Blockchain Platform

The consortium refers to a blockchain system in which the platform is administered by multiple organizations instead of a single one (Liu et al., 2019). The platform operates on a permission-based model rather than a public one. However, it is permissioned, meaning that only nodes belonging to organizations with ledger access can participate, yet it still maintains decentralization. A sole entity exists within a private blockchain, creating the perception of a centralized business. Conversely, decisions on the consortium blockchain are genuinely determined by multiple companies. Hence, no individual entity can partake in unlawful actions within the network and evade the resulting repercussions. Each entity on the platform will take turns monitoring it. The primary objective of the consortium blockchain example was to streamline inter-business communication (Wang et al., 2019).

5 Tradeoff Analysis of Blockchain and Features

This segment discusses the tradeoffs among different properties in the taxonomy architecture with respect to the consensus approach. The consensus algorithm plays a vital role to determine the purpose and outcome of a blockchain network. A blockchain's technical properties are partly dependent on its consensus mechanism. For instance, if the network requires security over performance then the consensus approach could be significantly different than the one which focuses on performance and scalability. Based on the taxonomy architecture, the following tradeoff comparisons are considered:

a) Tradeoff Analysis of Energy Consumption & Consensus
b) Tradeoff Analysis of Security
c) Tradeoff Analysis of Performance

Tradeoff Analysis of Energy Consumption and Consensus

There are different consensus algorithms, among them, we choose to cover: Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), and Practical Byzantine Fault Tolerant (PBFT) for carrying out the tradeoff analysis.

Proof of Work (PoW) is a process where nodes with varying computational abilities compete to be chosen as the producer of a new block in each consensus round. The rival nodes must employ a brute force method to discover a valid hash to add a random integer to the block. The responsibility to initiate a new block might be assigned to the node that first identifies a valid hash (Yang et al., 2019). Participants must continuously compute the hash value by adding additional secret or nonces to the block until an appropriate hash value is achieved (Gai et al., 2019). A nonce is a binary number of fixed lengths used only once by a cryptographic procedure (Puthal et al., 2018). The mining method involves hashing a block of transactions, and the resulting hash must be lower than the difficulty level. Once the miner acquires the correct nonce and shares the block with the network, the newly created block will be added to the existing chain. Subsequently, all nodes will employ an identical nonce to authenticate the solution. The procedure is called proof-of-work because nodes must exert effort to determine the correct value. The winning node will receive the reward for successfully mining the block. To achieve a good outcome, nodes must consistently explore different nonce values, which requires a substantial amount of computational capacity. A malevolent attacker can disrupt a single block in a chain; however, as the number of legitimate blocks in the chain increases, the amount of effort required also increases. Consequently, the computational resources required to disrupt a lengthy chain are substantial, rendering Proof of Work (PoW) highly resistant to malicious attacks. The main drawback of the PoW methodology is that it necessitates miners to allocate substantial computational resources to produce a block, resulting in a slower process than alternative consensus methods. The facility can house a substantial number of miners; however, as the number of miners increases, the energy consumption also increases.

In a Proof of Stake (PoS) system, miners do not need to compete to discover a valid hash using significant computational resources (Wang et al., 2019). In contrast, it depends on a participant having a substantial interest in the system to participate in the process of creating blocks. The likelihood of a participating node being selected to construct a block is determined by its stake or wealth. The presence of a substantial stake (Aste et al., 2017) is believed to serve as a deterrent against potential hostile attacks on the network. Competition among peers is avoided as the selection of the block maker is based on the amount of stake they possess in the network. Consequently, a validator uses its stake to engage in the process of creating blocks. If the block is approved, the validator receives the fees from the transactions in the block. Therefore, PoS is a more sustainable option than PoW due to its lower resource consumption and superior performance in terms of throughput and latency (Saleh, 2021). Unlike Proof of Work (PoW), which incurs significant mining expenses and requires considerable work, Proof of Stake (PoS) can be more susceptible to malicious assaults. The Nothing-at-Stake dilemma (Kiayias et al., 2017) is a newly recognized limitation that affects this consensus technique. This difficulty has arisen due to the lack of a tangible existence, such as the need for energy consumption to provide a coordinating reference. In the event of a fork, the number of tokens on both chains remains constant. This means there is no deterrent for a validator to stake their coins on several histories. Modern PoS protocols, like Ethereum Casper, make significant efforts to penalize this unfavorable behavior of validators who stake their assets (Bach et al., 2018). The "Slashing Condition" is the mechanism used, which involves penalizing validators that produce incorrect blocks or blocks in failing branches by deducting their stake and adding it to a shared pool. This measure is implemented to deter fraudulent conduct and safeguard the integrity of the network. Slashing is a continuous procedure in Tezos and will also be implemented in Ethereum 2.0. Another limitation of this consensus approach is that the selection of the validator is determined by the amount of stakes they own (Li et al., 2017). The node with the highest wealth may be given more opportunities to validate a block and gain greater influence in the network, perhaps resulting in an unjust distribution or centralization.

An alternative approach to consensus-building on public blockchains is called Delegated Proof of Stake (DPoS). Stakeholders designate peers to perform validation and verification tasks in this method (Buterin & Griffith, 2017). These delegates are responsible for adding and approving new blocks to the blockchain after being chosen and confirmed. An effective substitute for the popular proof-of-stake (PoS) and proof-of-work (PoW) techniques is delegated proof of stake (DPoS). It makes it possible to choose delegates to participate in the mining process by voting. Block production speeds up significantly as a result (Shifferaw & Lemma, 2021). This is achieved by ensuring that a single node will create the next block and a small group of nodes will agree to avoid double-spending. Efficiency may be guaranteed by changing the network's settings, such as block size and block intervals. This consensus method's tendency toward centralization might be its main flaw. The high-stakes players can become validators by casting their votes and persuading others to do the same. However, stakeholders can dismiss dishonest witnesses if they engage in malicious behavior. One example of a platform that uses the DPoS consensus method is EOS.

A modified variant of DPoS, Proof of Authority (PoA) puts validators' identities and reputations at stake. Identification, in this sense, refers to the consistency between the official documentation and the validators' personal identification, which facilitates the process of verifying their identity. These validators have been permitted to stake their reputation on the network after a rigorous evaluation. In the context of Proof of Authority (PoA), only nodes designated as validators have the ability to create new blocks (Yang et al., 2020). Validators are motivated to maintain the security and durability of the blockchain network because they personally stand to gain from their identity. A small group of validators (less than 25) are incentivized to secure and preserve the blockchain network while their reputation are at stake. PoA is a very energy-efficient method because the consensus process it uses does not involve mining.

Practical BFT (PBFT) is an improved version of the Byzantine fault tolerance (BFT) consensus mechanism. It enables members to have partial trust and enhances the system's ability to withstand failures that arise from the Byzantine Generals' Problem (Nguyen & Kim, 2018). The consensus mechanism is predominantly employed on the Hyperledger Fabric platform. Even in scenarios with malicious nodes in the network, PBFT enhances the probability of attaining a consensus. However, it is crucial to note that the ratio of malevolent nodes inside the network must not exceed one-third of the total number of nodes. Increased network nodes directly correlate with enhanced security. In order for a transaction to be executed, it must receive the permission of the majority, or at least 51%, of the nodes in the network. It is important to mention that the protocol does not require a unanimous agreement of 100% because a valid transaction can still be processed even if a rogue node attempts to stop it. In a permissioned network, specific nodes can intentionally reject the transaction. The PBFT consensus approach can overcome this problem. Like Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT) is characterized by its energy efficiency as it does not necessitate intricate mining procedures. PBFT exhibits scalability limitations as adding nodes or replicas to a network results in an exponential increase in the message count.

Figure 2 depicts the tradeoff analysis regarding different consensus approaches and the amount of energy consumption. While PBFT, PoA, and PoS consume less energy, POW consumes resources at a staggering rate. The consensus mechanism in PoW could provide better security to the network due to the resource-intensive consensus process an asynchronous manner of ordering the transactions, however, falls short when it comes to sustainable energy consumption.

Tradeoff Analysis of Security

Blockchain security refers to a comprehensive risk management strategy that is applied on a blockchain network. The process entails utilizing cybersecurity frameworks, assurance services, and optimal methodologies to minimize the vulnerabilities linked to attacks and fraudulent activities. Security, in this context, refers to the dependability and genuineness of information. The degree of security is directly related to the quantity of hash power that supports a blockchain network.

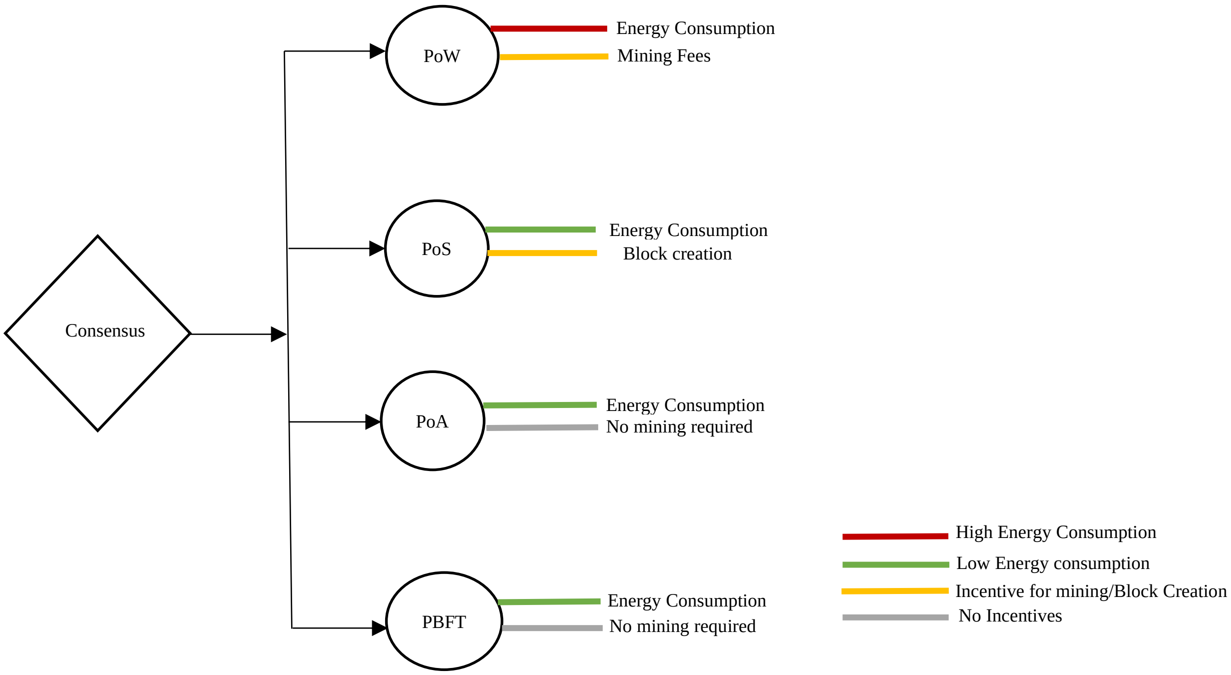

Figure 2: Tradeoff Analysis of Energy Consumption

The network's vulnerability to attacks diminishes as the number of miners and the potency of their mining equipment rise.

Double spending is when a single input is utilized for several transactions. It denotes an occurrence wherein an individual attempts to transfer an identical sum through many transactions without possessing enough balance in their wallet. The issue is specific to digital currency because knowledgeable individuals who comprehend the blockchain network and possess the required computational capabilities can readily duplicate digital information. The replication problem is not present in physical currencies as they are not easily duplicated. Moreover, the parties engaged in a transaction can promptly verify the legitimacy and previous ownership of physical currencies. Bitcoin utilizes a transaction log system called the blockchain to authenticate transactions and avoid the occurrence of double-spending.

A 51% attack is carried out to execute a double-spend, which entails spending the same unspent transaction output (UTXO) twice. To execute a 51% assault on a blockchain, it is necessary to possess most of the hash rate. A nefarious miner seeking to engage in double spending will initially execute a conventional transaction, wherein they expend their coins on a specific item or exchange them for an alternative currency. This indicates that they will adhere to conventional mining protocols with two exceptions. Initially, they will refrain from incorporating their transactions into the public chain. The term "private chain" describes this fork because it does not disclose the blocks it discovers. Possessing the majority of computer power would enable them to expedite the development of their chain compared to the public chain. The longest chain rule in Proof of Work (PoW) blockchains determines the outcome when a fork becomes publicly recognized. The legitimate chain would be the branch with the most blocks and significant computational resources expended. The attacker will disseminate the private branch to the entire network upon acquiring the items or other currencies with their coins. Every truthful miner will abandon the truthful branch and commence mining on the malicious chain. Subsequently, all miners begin mining on the malicious chain rather than the honest branch. The network disregards the transaction from the malicious node, treating it as nonexistent since the attacker failed to include it in their deceitful chain. This phenomenon has been observed in numerous minor blockchains in the past. Horizon experienced a 51% assault in early June 2018.

A Sybil attack is an effort to influence a peer-to-peer network by generating many fake addresses. One entity control all of the bogus addresses at once, even if they seem to be separate individuals from the observer. Sybil attacks may be mitigated by increasing the cost of creating an identity. There must be a delicate balancing act here. Ideally, it should be low enough to allow new players to join the network and create authentic identities without being limited. If the cost of producing many identities in a short period becomes prohibitively costly, then it must be high enough. Only the mining nodes are responsible for deciding on transactions in PoW blockchains. Making a phony "mining identity" has a monetary cost, primarily the purchase of mining equipment and the use of power. Sybil attacks on PoW blockchains are complex because of the related expenses.

The study undertaken on these security vulnerabilities (Samuel et al., 2021; Gao et al., 2019; Karame et al., 2012; Sayeed & Marco-Gisbert, 2019) indicates that both permissioned and permissionless blockchain networks are susceptible to various threats. Although the likelihood of a Sybil attack is similarly minimal in permissioned and permissionless networks, they are especially susceptible to a 51% Hash power attack. On the other hand, permissioned networks based on Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) are more effective in mitigating this threat. The majority of assaults against permissionless blockchains are a result of unrestricted accessibility and the absence of a centralized entity to oversee and regulate all network operations. Permissioned blockchain platforms offer a more efficient solution to this problem by implementing a central manager who possesses knowledge of all the participants in the network and exercises control over them. Nevertheless, the main security concern is that the central manager is the sole failure point. Comparing the security dangers between permissioned and permissionless blockchains is impractical. They possess distinct offensive strategies due to varying schemes. Presently, the recently developed architectures, accompanied by novel policies, are endeavoring to enhance the system's security against a wide range of threats. Unless these security vulnerabilities are resolved, prospective users will persist in exercising prudence, impeding widespread adoption.

Tradeoff Analysis of Performance

In a Proof of Work (PoW) Blockchain, every validating computer or node retains the entire dataset on the chain and actively engages in the consensus mechanism. Public blockchain technologies, such as Bitcoin, require a consensus from most participating nodes to validate and record new records and transactions onto the ledger (Lee et al., 2018; Gemeliarana & Sari, 2018). As a result, the process of completing any transaction becomes quite sluggish. Due to the PoW algorithm, Bitcoin can typically process only seven transactions per second. Now ranked second, Ethereum has a limited capacity to process only 12–30 transactions per second. When contrasting this with Visa, which has an average capacity of processing 1,700 transactions per second, it becomes evident that blockchain technology still has a considerable distance to cover to achieve success in the future. While protocols like Proof of Work (PoW) enhance trust in the network by preventing malicious attacks, they are hindered by limited throughput and significant latency (Mott, 2020). The bottleneck arises from the resources required to solve the cryptographic puzzle necessary for publishing and attaching a block to the chain. Bitcoin exemplifies low throughput while enhancing security by mitigating risks such as double spending and 51% hash attack. Another drawback of this consensus technique is its high CPU utilization, leading to substantial energy consumption. Ethereum has a distinct approach to PoW to deter ASIC-optimized mining, which involves specialized gear like a CPU or GPU that accelerates mining but incurs significant costs and energy consumption. Nevertheless, it will be unable to eliminate the shortcomings of Bitcoin.

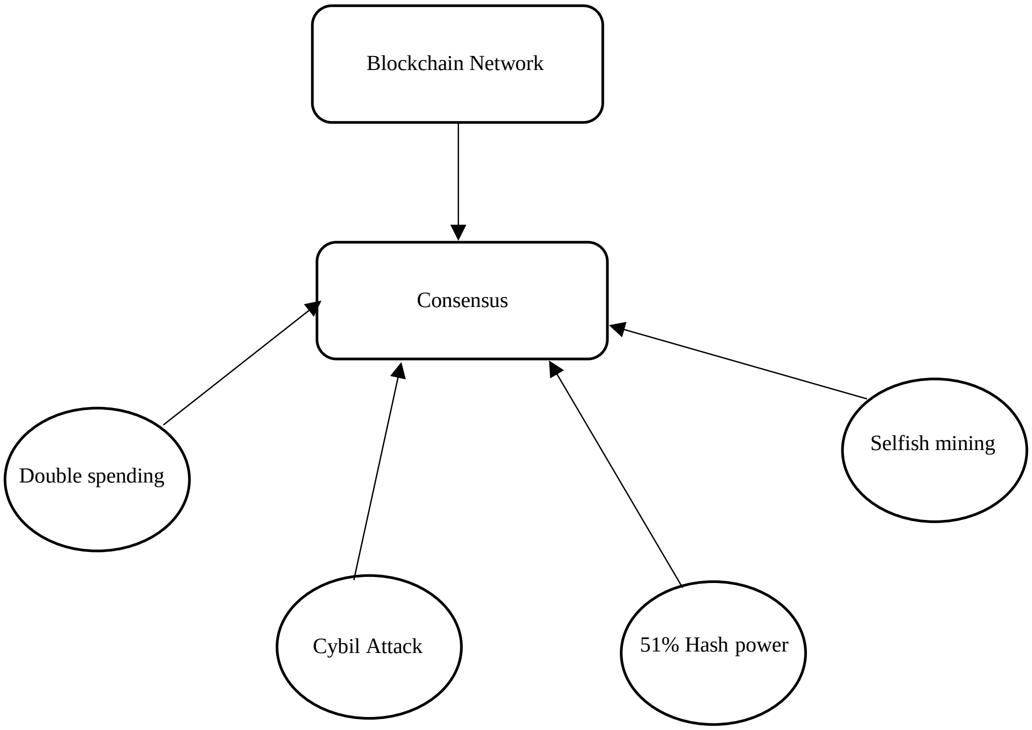

Figure 3: Tardeoff Analysis of Network Security

Additionally, the PoW protocol carries the potential for multiple branches, which might result in the double-spending issue. Hence, customers need to wait 60 minutes or until six blocks have been added to the chain to obtain confirmation before the transaction is finalized. Consequently, the duration of the transaction is lengthy, making it impractical for usage in real-world applications. The PBFT protocol can obtain consensus in the presence of malicious replicas with only a few rounds of message exchange. PBFT typically employs a solitary replica as a primary entity proposing a block. If consensus is attained by a two-thirds majority of all network peers, the block is appended to the chain. In addition, PBFT prevents forks from occurring during the consensus process in figure 3. While this strategy demonstrates energy efficiency, it does not possess long-term sustainability. The PBFT consensus algorithm has a message complexity that grows quadratically, requiring a broadcast of size n multiplied by n for a system with n copies. While this expense guarantees the achievement of consensus in the presence of malicious replicas or Byzantine failures, it also gives rise to scalability concerns. Proof of Stake (PoS) offers superior performance to Proof of Work (PoW) because of the absence of intricate computational requirements for mining in this consensus mechanism (Kędziora et al., 2020). Nevertheless, the ability to create blocks in a node is solely determined by its stakes, resulting in affluent nodes exerting greater influence over the network. DPoS and PoA exhibit superior energy efficiency and accelerated transaction processing capabilities. However, they suffer from limited scalability due to the requirement of a reduced number of validator nodes. Every widely-used platform must be capable of handling a high volume of transactions, ranging in the hundreds to thousands per second. Otherwise, the economy will experience significant disruptions for consumers and businesses, highlighting the importance of scalability and performance in this new technology.

Applicability Analysis: The taxonomy study conducted on blockchain has profoundly influenced our research regarding the analysis of blockchain's suitability (Swathi et al., 2019). This paper presents the Applicability Analysis Framework (AAF), designed to evaluate the appropriateness of adopting a blockchain technology for a certain application. The AAF is organized into six separate domains, which include eleven subdomains, and further divided into a comprehensive set of forty-five controls. This system aims to examine precise user needs to carry out a thorough evaluation using mathematical concepts. This assessment aims to ascertain the appropriateness of a solution based on blockchain technology in a certain situation. The study also includes an example of evaluating the appropriateness of a technique using AAF, facilitated by using a use-case scenario. The application analysis framework (AAF) is divided into six discrete areas to ensure a clear classification of controls: Data Storage, Transaction Attributes, Privacy and Access Control, Governance, Performance, and Market Influence. Each domain is further divided into multiple subdomains, each assigned multiple controls. The controls are shown in the format of a questionnaire (Jung, 2022).

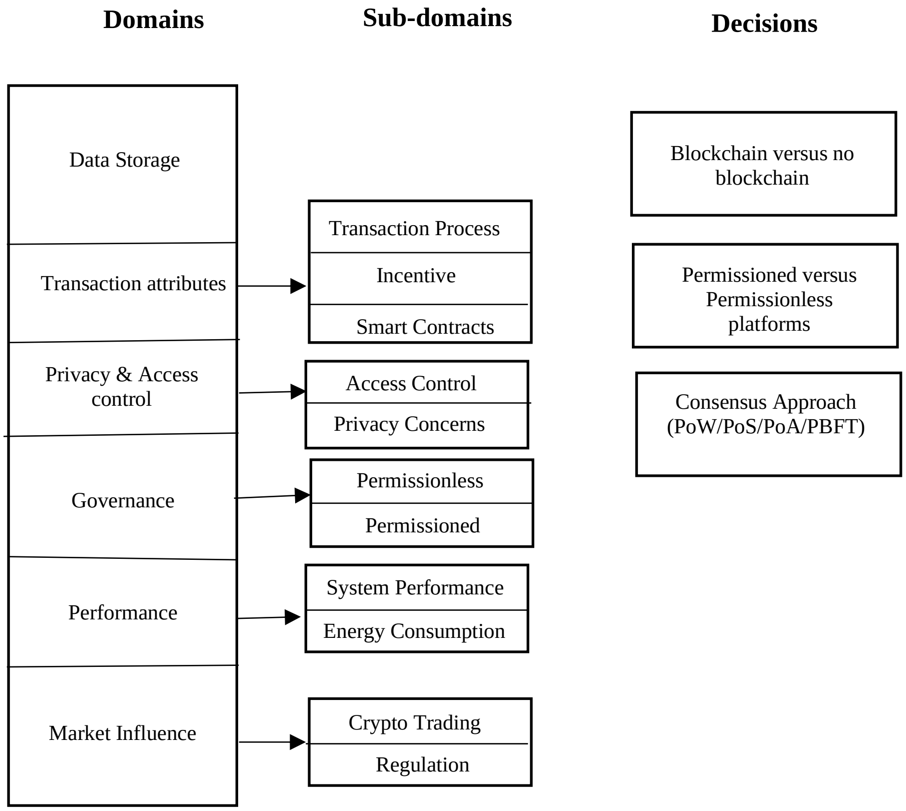

Figure 4: Overview of the Applicability Framework (Swathi et al., 2019)

The ultimate selection is achieved by combining the control states using a method of weighted accumulation. The detailed procedure will be explained in this section. Figure 4 illustrates the architectural structure of the AAF. The current version of the AAF utilizes three specific criteria to assess classes: the inclusion or exclusion of blockchain technology, the differentiation between permissioned and permissionless platforms, and the consensus mechanism implemented (such as PoW, PoS, PoA, and PBFT). Each given control can have three potential states. The states can be classified into three categories: Applicable (with a weight of 2), moderately applicable (with a weight of 1), or not applicable (with a weight of 0). It is crucial to recognize that a single control does not fully include the suitability of blockchain. Therefore, the combined responses to the several regulations dictate the level of applicability of blockchain in a certain application.

6 Conclusion

Realizing the benefits of using blockchain technology over centralized systems is a major implementation and deployment problem for businesses. The benefits of decentralization and immutability are obvious, but there has to be a greater understanding regarding the trade-offs associated with blockchain governance, performance, scalability, and interoperability. Therefore, we offer a taxonomy guideline that helps to facilitate blockchain system design considerations and offers information on the quality and performance features. In addition, the taxonomy describes the governance architecture and encapsulates the salient features of different blockchains. But we didn't consider smart contracts a key component in figuring out the blockchain's governance system. Since smart contracts are important for the future of blockchain technology, we are interested in learning more about them. In the future, this research may focus on creating a uniform framework for the blockchain governance model to assess which blockchain platforms are suitable for a certain use case. It is crucial to establish the suitability of a use-case scenario and choose the appropriate platform (permissionless, permissioned, consortium, etc.) before implementing blockchain technology globally.

Acknowledgement

This study was supported by the Swedish Energy Agency under grant 43090-2, Cloudberry Datacenters.

References

[1] Akbar, N. A., Muneer, A., ElHakim, N., & Fati, S. M. (2021). Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses. *Future Internet*, *13*(11), 285. https://doi.org/10.3390/fi13110285

[2] Ali, M., Nelson, J., Shea, R., & Freedman, M. J. (2016). Blockstack: A global naming and storage system secured by blockchains. *In USENIX Annual Technical Conference (USENIX ATC 16)*, 181-194.

[3] Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. *Computer, 50*(9), 18-28.

[4] Avan-Nomayo, O. (2021). Bitcoin network node count sets new all time high. https://cointelegraph.com/tags/bitcoin

[5] Bach, L. M., Mihaljevic, B., & Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. *In IEEE 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1545-1550.

[6] Brinkmann, M., & Heine, M. (2019). Can blockchain leverage for new public governance? A conceptual analysis on process level. *In Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*, 338-341.

[7] Buterin, V., & Griffith, V. (2017). Casper the friendly finality gadget. *arXiv preprint arXiv:1710.09437*. https://doi.org/10.48550/arXiv.1710.09437

[8] Chohan, U. W. (2022). Cryptocurrencies: A brief thematic review. https://ssrn.com/abstract=3024330

[9] Danielle, K., Satya, S., & Assaad, F. (2024). A Sustainable Circular Business Model to Improve the Performance of Small and Medium-sized Enterprises Using Blockchain Technology. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15*(2), 240-250.

[10] De Kruijff, J., & Weigand, H. (2017). Understanding the blockchain using enterprise ontology. *In Advanced Information Systems Engineering: 29th International Conference, CAiSE, Essen, Germany, Proceedings*. Springer International Publishing, *29*, 29-43.

[11] Decker, C., & Wattenhofer, R. (2013). Information propagation in the bitcoin network. *In IEEE P2P 2013 Proceedings*, 1-10.

[12] Del Castillo, M. (2017). Chain is now working on six 'Citi-Sized' blockchain networks. https://www.coindesk.com/markets/

[13] Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., & Hierons, R. (2018). Smart contracts vulnerabilities: a call for blockchain software engineering? *In IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 19-25.

[14] Dursun, T., & Üstündağ, B. B. (2021). A novel framework for policy based on-chain governance of blockchain networks. *Information Processing & Management*, *58*(4), 102556. https://doi.org/10.1016/j.ipm.2021.102556

[15] Eberhardt, J., & Tai, S. (2017). On or off the blockchain? Insights on off-chaining computation and data. In *Service-Oriented and Cloud Computing: 6th IFIP WG 2.14 European Conference, ESOCC 2017, Oslo, Norway, Proceedings*. Springer International Publishing, *6*, 3-15.

[16] Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7), 95-102.

[17] Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). {Bitcoin-NG}: A scalable blockchain protocol. *In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, 45-59.

[18] Fill, H. G., & Härer, F. (2018). Knowledge blockchains: Applying blockchain technologies to enterprise modeling. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 4045-4054.

[19] Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, *51*, 102029. https://doi.org/10.1016/j.ijinfomgt.2019.10.014

[20] Gai, K., Wu, Y., Zhu, L., Qiu, M., & Shen, M. (2019). Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Transactions on Industrial Informatics*, *15*(6), 3548-3558.

[21] Gao, S., Yu, T., Zhu, J., & Cai, W. (2019). T-PBFT: An Eigen Trust-based practical Byzantine fault tolerance consensus algorithm. *China Communications*, *16*(12), 111-123.

[22] Garriga, M., Dalla Palma, S., Arias, M., De Renzis, A., Pareschi, R., & Andrew Tamburri, D. (2021). Blockchain and cryptocurrencies: A classification and comparison of architecture drivers. *Concurrency and Computation: Practice and Experience*, *33*(8), e5992. https://doi.org/10.1002/cpe.5992

[23] Gemeliarana, I. G. A. K., & Sari, R. F. (2018). Evaluation of proof of work (POW) blockchains security network on selfish mining. *In IEEE International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 126-130.

[24] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. *In Proceedings of the ACM SIGSAC conference on computer and communications security*, 3-16.

[25] Giji Kiruba, D., Benita, J., & Rajesh, D. (2023). A Proficient Obtrusion Recognition Clustered Mechanism for Malicious Sensor Nodes in a Mobile Wireless Sensor Network. *Indian Journal of Information Sources and Services*, *13*(2), 53–63.

[26] Glaser, F., & Bezzenberger, L. (2015). Beyond cryptocurrencies-a taxonomy of decentralized consensus systems. *In 23rd European Conference on Information Systems (ECIS), Münster, Germany*.

[27] Grover, B. A., Chaudhary, B., Rajput, N. K., & Dukiya, O. (2021). Blockchain and governance: Theory, applications and challenges. *Blockchain for Business: How It Works and Creates Value*, 113-139.

[28] Hao, J., Huang, C., Tang, W., Zhang, Y., & Yuan, S. (2021). Smart contract-based access control through off-chain signature and on-chain evaluation. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *69*(4), 2221-2225.

[29] Hepp, T., Sharinghousen, M., Ehret, P., Schoenhals, A., & Gipp, B. (2018). On-chain vs. off-chain storage for supply-and blockchain integration. *it-Information Technology*, *60*(5-6), 283-291.

[30] Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. *Journal of Medical Systems*, *43*, 1-35.

[31] Ismail, L., Hameed, H., AlShamsi, M., AlHammadi, M., & AlDhanhani, N. (2019). Towards a blockchain deployment at uae university: Performance evaluation and blockchain taxonomy. *In Proceedings of the International Conference on Blockchain Technology*, 30-38.

[32] Jung, S.W. (2022). Universal Redactable Blockchain. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *13*(4), 81-93.

[33] Kalinin, O., Gonchar, V., Abliazova, N., Filipishyna, L., Onofriichuk, O., & Maltsev, M. (2024). Enhancing Economic Security through Digital Transformation in Investment Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability. *Natural and Engineering Sciences*, *9*(1), 26-45.

[34] Karame, G. O., Androulaki, E., & Capkun, S. (2012). Double-spending fast payments in bitcoin. *In Proceedings of the ACM Conference on Computer and Communications Security*, 906-917.

[35] Kędziora, M., Kozłowski, P., Szczepanik, M., & Jóźwiak, P. (2020). Analysis of blockchain selfish mining attacks. *In Information Systems Architecture and Technology: Proceedings of 40th Anniversary International Conference on Information Systems Architecture and Technology–ISAT 2019: Part I*, Springer International Publishing, 231-240.

[36] Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. *In Annual International Cryptology Conference*, Cham: Springer International Publishing, 357-388.

[37] Kim, S., Kwon, Y., & Cho, S. (2018). A survey of scalability solutions on blockchain. *In IEEE International Conference on Information and Communication Technology Convergence (ICTC)*, 1204-1207.

[38] Klein, S., & Prinz, W. (2018). A use case identification framework and use case canvas for identifying and exploring relevant blockchain opportunities. *Proceedings of 1st ERCIM Blockchain Workshop*. https://doi.org/10.18420/blockchain2018_02.

[39] Kumar, A., Joshi, P., Bala, A., Sudhakar Patil, P., Jang Bahadur Saini, D. K., & Joshi, K. (2023). Smart Transaction through an ATM Machine using Face Recognition. *Indian Journal of Information Sources and Services*, *13*(2), 7-13.

[40] Labazova, O., Dehling, T., & Sunyaev, A. (2019). From hype to reality: A taxonomy of blockchain applications. *In Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019)*. https://ssrn.com/abstract=3250648

[41] Lai, R., & Chuen, D. L. K. (2018). Blockchain–from public to private. *In Handbook of Blockchain, Digital Finance, and Inclusion.* Academic Press, *2*, 145-177.

[42] Lee, H., Shin, M., Kim, K. S., Kang, Y., & Kim, J. (2018). Recipient-oriented transaction for preventing double spending attacks in private blockchain. *In 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 1-2.

[43] Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing proof-of-stake blockchain protocols. *In Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, Proceedings*, Springer International Publishing, 297-315.

[44] Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in Auditing*, *13*(2), A19-A29.

[45] Liu, Y., Lu, Q., Xu, X., Zhu, L., & Yao, H. (2018). Applying design patterns in smart contracts: A case study on a blockchain-based traceability application. *In Blockchain–ICBC 2018: First International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA*, *Proceedings*, Springer International Publishing, *1*, 92-106.

[46] Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain governance—A new way of organizing collaborations? *Organization Science*, *32*(2), 500-521.

[47] Mas'ud, M. Z., Hassan, A., Shah, W. M., Abdul-Latip, S. F., Ahmad, R., Ariffin, A., & Yunos, Z. (2021). A review of digital forensics framework for blockchain in cryptocurrency technology. *In IEEE 3rd International Cyber Resilience Conference (CRC)*, 1-6.

[48] Mattila, J. (2016). *The blockchain phenomenon–the disruptive potential of distributed consensus architectures*. ETLA working papers.

[49] Maull, R., Godsiff, P., Mulligan, C., Brown, A., & Kewell, B. (2017). Distributed ledger technology: Applications and implications. *Strategic Change*, *26*(5), 481-489.

[50] Meijer, D., & Ubacht, J. (2018). The governance of blockchain systems from an institutional perspective, a matter of trust or control? *In Proceedings of the 19th annual international conference on digital government research: governance in the data age*, 1-9.

[51] Meunier, S. (2018). Blockchain 101: What is blockchain and how does this revolutionary technology work? *In Transforming Climate Finance and Green Investment with Blockchains, Academic Press,* 23-34.

[52] Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing & Management*, *58*(3), 102535. https://doi.org/10.1016/j.ipm.2021.102535

[53] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, *7,* 117134-117151.

[54] Monrat, A. A., Schelén, O., & Andersson, K. (2020). Blockchain mobility solution for charging transactions of electrical vehicles. *In IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC),* 348-253.

[55] Monrat, A. A., Schelén, O., & Andersson, K. (2020). Performance evaluation of permissioned blockchain platforms. *In IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 1-8.

[56] Monrat, A. A., Schelén, O., & Andersson, K. (2022). Applicability Analysis of Blockchain Technology. *In IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 1-8.

[57] Mott, G. (2020). A storm on the horizon? "Twister" and the implications of the blockchain and peer-to-peer social networks for online violent extremism. *In Islamic State's Online Activity and Responses*, Routledge, 206-227.

[58] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access*, *7,* 85727-85745.

[59] Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems*, *14*(1), 101–128.

[60] Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2021). Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*, *7*(3), 295-307.

[61] Podvalny, S., Zolotukhina, I., Sotnikova, O., & Prokshits, E. (2021). Enhancing the investment attractiveness and effectiveness of the special economic zone. *Archives for Technical Sciences*, *1*(24), 1-8.

[62] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine*, *7*(4), 6-14.

[63] Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2020). Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. *IEEE Systems Journal*, *15*(1), 85-94.

[64] Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., & Orgad, L. (2021). Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi*, *40*, 821-831.

[65] Robinson, R. A. (2017). The new digital wild west: regulating the explosion of initial coin offerings. *Tennessee Law Review, 85*, 897. https://ssrn.com/abstract=3087541

[66] Rodrigo, M. N. N., Perera, S., Senaratne, S., & Jin, X. (2020). Potential application of blockchain technology for embodied carbon estimating in construction supply chains. *Buildings*, *10*(8), 140. https://doi.org/10.3390/buildings10080140

[67] Rondinelli, D. A. (2017). Decentralization and development. *In International Development governance*, 391-404.

[68] Saleh, F. (2021). blockchain without waste: proof-of-stake. *The Review of Financial Studies, 34*(3), 1156-1190.

[69] Samuel, C. N., Glock, S., Verdier, F., & Guitton-Ouhamou, P. (2021). Choice of ethereum clients for private blockchain: Assessment from proof of authority perspective. *In IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1-5.

[70] Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences*, *9*(9), 1788. https://doi.org/10.3390/app9091788

[71] Shahriar Hazari, S., & Mahmoud, Q. H. (2020). Improving transaction speed and scalability of blockchain systems via parallel proof of work. *Future Internet*, *12*(8), 125. https://doi.org/10.3390/fi12080125

[72] Shifferaw, Y., & Lemma, S. (2021). Limitations of proof of stake algorithm in blockchain: A review. *Zede Journal*, *39*(1), 81-95.

[73] Signorini, M., Pontecorvi, M., Kanoun, W., & Di Pietro, R. (2020). BAD: A blockchain anomaly detection solution. *IEEE Access*, *8*, 173481-173490.

[74] Singh, S. K., Jenamani, M., Dasgupta, D., & Das, S. (2021). A conceptual model for Indian public distribution system using consortium blockchain with on-chain and off-chain trusted data. *Information Technology for Development*, *27*(3), 499-523.

[75] Sreenivasu, M., Kumar, U. V., & Dhulipudi, R. (2022). Design and Development of Intrusion Detection System for Wireless Sensor Network. *Journal of VLSI Circuits and Systems, 4*(2), 1-4.

[76] Swathi, P., Modi, C., & Patel, D. (2019). Preventing sybil attack in blockchain using distributed behavior monitoring of miners. *In IEEE 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1-6.

[77] Tasca, P., & Tessone, C. J. (2017). Taxonomy of blockchain technologies. Principles of identification and classification. https://doi.org/10.48550/arXiv.1708.04872

[78] Udayakumar, R., Chowdary, P. B. K., Devi, T., & Sugumar, R. (2023). Integrated SVM-FFNN for Fraud Detection in Banking Financial Transactions. *Journal of Internet Services and Information Security*, *13*(3), 12-25.

[79] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access, 7*, 22328-22370.

[80] Wang, Y., Xiao, M., Miao, Y., Liu, W., & Huang, Q. (2019). Signature Scheme from Trapdoor Functions. *Journal of Internet Services and Information Security*, *9*(2), 31-41.

[81] Weking, J., Mandalenakis, M., Hein, A., Hermes, S., Böhm, M., & Krcmar, H. (2020). The impact of blockchain technology on business models–a taxonomy and archetypal patterns. *Electronic Markets*, *30*, 285-305.

[82] Wieninger, S., Schuh, G., & Fischer, V. (2019). Development of a blockchain taxonomy. *In IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, 1-9.

[83] Wüst, K., & Gervais, A. (2018). Do you need a blockchain? *In IEEE Crypto Valley Conference on Blockchain Technology (CVCBT)*, 45-54.

[84] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., & Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. *In IEEE International Conference on Software Architecture (ICSA)*, 243-252.

[85] Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, *7*, 118541-118555.

[86] Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., & Chen, S. (2020). Public and private blockchain in construction business process and information integration. *Automation in Construction*, *118*, 103276. https://doi.org/10.1016/j.autcon.2020.103276

[87] Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J., & Ko, K. (2017). Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. *IEEE Access*, *6*, 1513-1524.

[88] Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, *29*(2), 105-117.

[89] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352-375.

Authors Biography

Ahmed Afif Monrat is PhD student at Lulea University of Technology (LTU), Skelleftea, Sweden. His research area for PhD is mainly focused on sustainable Blockchain Technology. He has M.Sc. degree in Computer Science and Technology from Erasmus Mundus Master scholarship program PERCCOM (Pervasive Computing & Communications for sustainable development). His research interests include Expert system, Artificial Intelligence, Machine Learning, Distributed computing and cloud computing technologies.

Olov Schelén is a Professor at Luleå University of Technology and CEO at Xarepo AB. His research interests include mobile and distributed systems, software orchestration, computer networking, artificial intelligence and blockchain. He has a PhD in computer networking from Luleå University of Technology and thereafter he has more than 20 years of experience from industry and academia.

Karl Andersson has a M.Sc. degree in Computer Science and Technology from Royal Institute of Technology, Stockholm, Sweden and a Ph.D. degree in Mobile Systems from at Lulea University of Technology, Sweden. After being a postdoctoral research fellow at the Internet Real-time Laboratory at Columbia University, New York, USA and a JSPS Fellow with National Institute of Information and Communications Technology, Tokyo, Japan, he is now Professor of Pervasive and Mobile Computing at Lulea University of Technology, Sweden. His research interests include Mobile Computing, the Internet of Things, Cloud Technologies, and Information Security.