Preprints.org

Article

Not peer-reviewed version

Governance of Blockchain-enabled IoT Ecosystem: The Variable Geometry Approach

Ikram Ullah * and Paul Havinga

Posted Date: 9 October 2023

doi: 10.20944/preprints202310.0375.v1

Keywords: Internet of things; blockchain; governance; European Union (EU) policy; policy makers; International Organization for Standardization (ISO)

Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

Governance of Blockchain-Enabled IoT Ecosystem: The Variable Geometry Approach

Ikram Ullah [1] and Paul J. M. Havinga [1]

[1] Pervasive Systems Group, Department of Computer Science, University of Twente Enschede, 7522 NB Enschede, The Netherlands; i.ullah@utwente.nl (I.U.); p.j.m.havinga@utwente.nl (P.H.)

* Correspondence: i.ullah@utwente.nl

Abstract: The number of Internet of Things (IoT) applications is increasing at a fast-paced and so is the interest in blockchain-enabled IoT ecosystem. IoT applications make our day-to-day life more efficient, while integrating blockchain into the IoT ecosystem (blockchain-IoT) brings security, transparency, trust, and privacy to IoT applications. Perhaps, smart logistics, smart health, and smart city are some of the potential blockchain-enabled IoT application domains. One of the reasons that is hindering the mass adoption of blockchain-IoT into mainstream applications is the lack of a dedicated governance. Without proper governance and regulations, and because of the obfuscated and concealed cryptographic nature of blockchain, blockchain can be used for various illicit activities such as ransomware, money laundering, fraud and so on. Furthermore, blockchain and IoT are relatively contemporary technologies and paucity of exclusive governance can ultimately lead to lack of confidence in these technologies. Therefore, in order to fully avail from blockchain and IoT integration (blockchain-IoT) and as well as further prevail this integration, governance can play an important role. Proper regulations and standarization are required to benefit from the novel characteristics of blockchain-IoT and avoid blockchain being used for malicious purposes. In this research, we address the role of blockchain in governance mechanisms, governance for blockchain, and finally proposed a vigorous governance framework for blockchain-enabled IoT ecosystem. We also demonstrate the applications of our proposed governance framework through a smart logistics case study. We anticipate that our proposed governance framework can facilitate and encourage blockchain and IoT integration in various application domains.

Keywords: Internet of things; blockchain; governance; European Union (EU) policy; policy makers; International Organization for Standardization (ISO)

1. Introduction

In this paper, we propose a variable geometry approach based governance mechanism for blockchain-enabled IoT ecosystem. Governance mechanism is vital for blockchain-enabled IoT ecosystem in order to plan, execute, and monitor blockchain-enabled IoT infrastructure. In the following subsections, we first introduce IoT applications, we then illustrate blockchain and IoT integration, and finally we elaborate the significance of blockchain-enabled IoT governance.

1.1. IoT applications

IoT is integrated into our day to day life to provide innovative applications. Technological innovations have fundamentally changed our lifestyles by improving communications, bringing ease, enhancing our everyday life, and have intrinsically changed the industrial spectrum as shown in the Figure 1. IoT technology is still in its infancy and many new innovations are happening at a blistering fast pace in the IoT spectrum. The number of connected devices is swiftly increasing and it is estimated that by 2025 the number of connected devices could potentially reach 100 billion [10,13]. Such an increase in the number of IoT devices potentially leads to exponential growth in data [24]. The data is gathered, stored, and processed for various IoT services. IoT infrastructure consists of various sensors, actuators, RFID, Wireless Sensor Network (WSN), cloud, and Big data. Cloud computing

© 2023 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

can potentially increase IoT success with its tremendous applications such as easy implementation, cheap, efficient, and have the capabilities to store and process large sets of data. Cloud computing can be extremely handy where IoT generates large amount of data and when the sensors are distributed geographically [12]. Integration of IoT, cloud and Big data mechanisms is the cornerstone of many modern innovations [24].

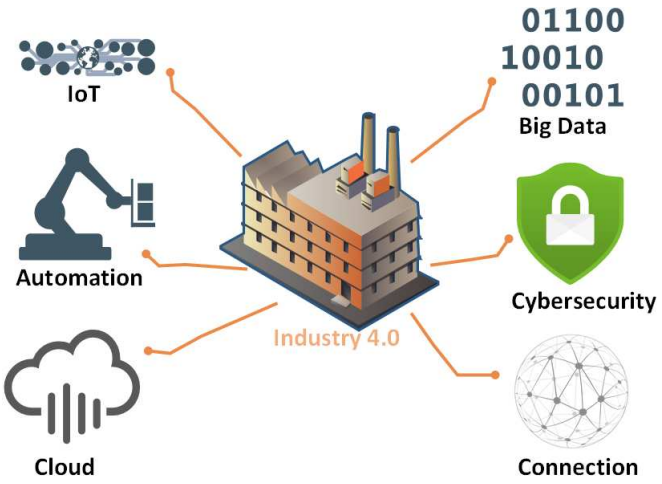

Figure 1. Industry 4.0 revolution.

Apart from the vast applications of IoT, IoT also suffers various challenges [16]. IoT solutions are still in the early stages of the development and in most of the cases the solutions are complex. The complexity arises for various reasons such as interoperability, communication, data volume, real-time data analysis, strenuous development cycle, and standards [8,24,35]. Most common issues associated with IoT are privacy, security, standards, governance, and ethics [19,24,26]. Moreover, other IoT challenges are mentioned in [27,28,34]. Besides IoT, there are many challenges associated with cloud computing such as confidentiality, trust, privacy, integrity, and unlawfully storing and processing of personal data. Committing crime is getting easier due to the recent technological evolution. Criminals have scaled up their tactics, automated their attack factors, advanced cashing out victim mechanisms (paying ransom in cryptocurrencies), and criminals have modernized their business models – for instance using different languages (German language is used by wanacry for German rail).

1.2. Blockchain and IoT inclusion

Blockchain is a distributed peer-to-peer network, where the nodes run blockchain protocols to validate transactions. Transactions are transparently stored in distributed ledgers and each node has a copy of the ledger. Blockchain allow participants of a network to achieve consensus over the shared ledger without the need of any central party or human interactions [47,48]. Artificial intelligence (AI), IoT, blockchain, and robotics, to name a few, are some of the emerging technologies and play a vital role in Industry 4.0 revolution. Blockchain is no doubt a revolutionary and innovative technology with immense applications in various sectors of life. Even thought the number of blockchain applications are numerous [46,52], some of the well-known applications, for instance, are e-voting, cryptocurrency, healthcare, automotive, supply chain, insurance policy, and procurement services [40, 43,44]. Blockchain has attracted significant interest from investors, start-ups, venture capitalists, and various industries [49]. In 2019, over $3 billion were invested in blockchain start-ups [37,41]. Apart from businesses, other parties such as government organizations, policy-makers, scholars and regulators have also started scrutinizing blockchain possibilities [46,50,51,53]. One way to overcome IoT challenges, that we mentioned earlier, is through the integration of IoT and blockchain technology. IoT can benefit from blockchain in many ways. For instance, blockchain can eradicate IoT security, transparency, trust, and privacy challenges. Furthermore, integration of novel technologies can

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

have many advantages such as innovation, improving functionalities, and serviceability. However, blockchain and IoT integration has introduced new challenges to the paradigm. One of the main challenge is the lack of dedicated governance. In this paper, we propose an efficient and befitting governance framework for blockchain-enabled IoT ecosystem.

1.3. Governance

Governance is "a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods" [70]. In the IoT context, security, privacy, and governance are inseparable - governance is required to achieve trust, security, and privacy [24,26]. Governance aims to formulate the roles, policies, and responsibilities to achieve; for instance, interoperability, liability, security, privacy, and trust. Even thought security, privacy and governance are closely related but they are not one and the same. Security mechanisms ensure data protection from malicious purposes. While privacy mechanisms illustrate how to collect, process and store users' data. Governance framework consists of policies and processes related the controls (for instance security, privacy, business practices, organizational controls) in place. Through elaborate governance mechanisms, organizations can implement policies, processes, accountabilities, roles, and execute appropriate decisions to efficiently utilize and manage corporate resources. Absolute design and implementation mechanisms rolled out by governance can only resolve users' and stakeholders' concerns [21]. The World Bank governance consists of mechanisms and institutions which "includes the process by which governments (governing body) are selected, monitored and replaced; the capacity of the government to effectively formulate and implement sound policies; and the respect of citizens and the state for the institutions that govern economic and social interactions among them" [18]. With the evolution of emerging technologies, conventional governance mechanisms which constitute people, process, and technology are evolving [1,9] into more rigorous frameworks. After the introduction of General Data Protection Regulation (GDPR) [72] in Europe, adducing governance is becoming more indispensable [35]. Governance can facilitate IoT development [12] and adoption. With the introduction of distributed ledger technologies such as blockchain technology and the already distributed nature of IoT architecture, the concept of governance is getting more important but it becomes also challenging as existing centralized governance mechanisms are not anymore applicable [7]. Technical aspects of IoT are widely discussed while adequate legal frameworks do not exist yet [17]. European commission has advised experts to investigate potential features of governance [17]. And European commission is the first international organization aiming to constitute a governance framework [19].

Figure 2 shows the main principles that an inclusive governance framework is required to encourage and ensure. These principles are democracy & ethics, confidence, collaboration, innovation, well-being, and economic prosperity. Through governance, it is intended to achieve these main factors of modern world ultimate goals. Governance policies are ought to withhold the key pillars of democracy and adequate principles of ethics. Transparency and disclosure are regarded as the core characteristics of a governance frameworks [68]. Sometimes change is hard, especially in the adaption of new technologies as there is a lack of confidence and users are concerned about their data. Generally, achieving consensus is challenging due to the competition among the stakeholders or lack of trust [59]. Confidence in new technologies is crucial as it can lead to success and ultimately large scale adoption of technology and consequently collaboration among many partners and stakeholders. In new technologies where personal data is involved, there are many consumers' concerns such as "fear of unknown" [21]. Governance can facilitate future development [12], adoption, and ratification of novel technologies. Governance is required to include efficient and protective policies related to users and stakeholders concerns. Confidence of users can be achieved through implementing mechanisms and policies to ensure confidentiality, integrity, and availability. Confidence in the novel technology can lead to mass adoption of the technology and innovations. Governance encourages collaboration among diverse partners and industries. An individual technology can be beneficial;

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

however, integration of diverse technologies can concoct finest innovations. Hence, bring efficiency to various diverse application domains. Partners can come together to build a common technological infrastructure, where each partner has dedicated knowledge, expertise, and resources and consequently generate value. Governance policies reassure the applications enhance quality of life [21] by reducing environmental impacts (recycling physical object) and enhance environmental sustainability (long lifetime of the technology).

Figure 2. An illustration of main cogitation principles of governance.

Governance can be classified into various categories. As mentioned in [59,62,63], governance frameworks are divided into three main categories: markets (individual choice), hierarchies (formal organization), and networks (consensus, blockchain). These categories are further divided into various types of frameworks as mentioned in the literature and used in practice such as IT [61], IoT [15], cloud [12], social-political [71] and so many other generic and industry specific frameworks. Like, National institute of Standards and technology (NIST) [36] elaborate standards regarding cyber security. For instance, NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) [36] describes security and privacy controls for federal information systems and organizations. General Data Protection Regulation (GDPR) [72] introduced by EU to protect citizens privacy and the citizens rights over their data. This standard is applied to European Union organizations and businesses in particular for EU residence. Fines can significant if GDPR policies are violated. Marriott was fined $123 million for 2018 data breach [73]. ISO 27000 [3] is an internationally recognized family of standards. For instance, ISO/IEC 30141 [2] is aimed to standardized IoT reference architecture to ensure IoT ecosystem is "seamless, safer, far more resilient". ISO/IEC 27001 is applicable for cyber security. Other related standards are ISO 270018 [4] and ISO 270017 [5]. ISO 27000 [3] ensures information assets security. These various standards and frameworks can be simultaneously implemented in practice. Furthermore, every country has a dedicated body for standards and compliance. For instance, in Netherlands, The Royal Netherlands Standardization Institute (NEN) [6] is responsible for standardization.

Each of these governance frameworks is designed for specific purposes and the frameworks are significantly different from each other. IoT is different from standard Internet in various ways. For instance, in implementation, maintenance, development, ethical issues, privacy, security [21], and inclusion of new technologies (blockchain). IoT characteristics and requirements go beyond the scope of Internet governance [22] and other governance frameworks so therefore a contemporary blockchain-enabled IoT governance framework is paramount. However, Internet governance [19] and other governance frameworks knowledge is crucial and can play an important role in developing comprehensive blockchain-enabled IoT governance [21]. For instance, Internet governance, which is the predecessor of IoT governance, collaboration with Internet governance bodies would be vital [21].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

Existing governance mechanisms can compliment blockchain-enabled IoT governance. Therefore, as shown in the Figure 3, other standards and governance frameworks are included in order to achieve comprehensive and wide prospect of blockchain-enabled IoT governance.

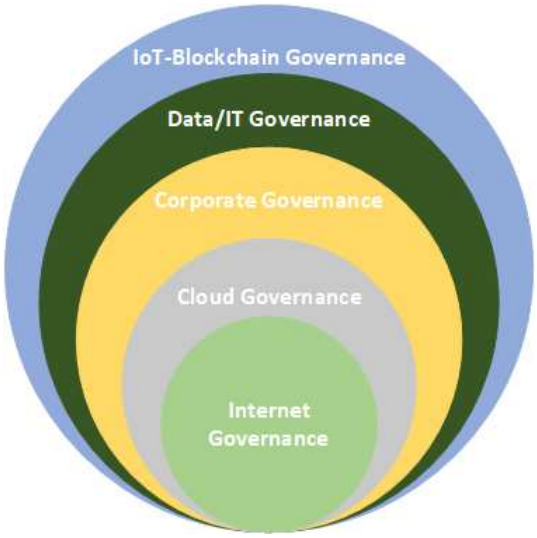

Figure 3. Some of the well known governance frameworks. Blockchain-IoT requires more comprehensive policies and roles; therefore it includes policies and roles from the other existing governance frameworks.

As per the EU IoT task force, IoT differs from the general Internet governance and thus further research, separate rules and regulations are essential [23]. There is lack of sufficient guidance regarding IoT governance [1]. As mentioned earlier, there is no dedicated legal IoT governance framework yet [24]. Lack of a matured governance is one of the many IoT challenges [24]. Therefore, for instance CASAGRAS project recommends a dedicated governance framework for IoT on global and regional level [23]. The field of IoT governance has been the least researched and progressive since the IoT revolution in the last decade. Developing strategic IoT governance mechanisms have unparalleled effects on the overall IoT sustainability in regards to environments and finances. Copie et al. [12] discussed various use cases to highlight the importance of governance. For instance, IoT governance allow us to manage IoT processes to add or revoke a device , data aggregation from multiple sources, policies regarding roles, security & privacy, trust, and data storing [12]. One main reason behind the lack of governance mechanisms is that developing and managing an international legal framework is not so straightforward as different countries and regions have different legislations. With the integration of blockchain and IoT, the development of an adequate governance framework becomes highly desirable.

As mentioned earlier, absolute design and implementation mechanisms rolled out by governance can only resolve users' concerns [21] and encourage future innovations. Therefore, we feel the urge for a more dynamic and vibrant governance mechanism which includes roles and policies both at societal level and information level and utilizing the blockchain characterisitics (i.e immutability, traceability, decentralization) for the governance aspiration. Blockchain can demonstrate governance features that are more cost efficient, deliver greater trust [68], and allows to develop decentralized governance which is far more efficient and automated. Furthermore, the number of blockchain frameworks are increasing significantly, however, there is no concrete blockchain governance mechanism. Blockchain governance is "the means of achieving the direction, control, and coordination of stakeholders within the context of a given blockchain project to which they jointly contribute" [54]. Through deploying blockchain technology in various applications, we can achieve most of the principles mentioned in Figure 2. Since blockchain encourage collaboration and potentially presenting distinctive governance features [37].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

The rest of the paper is organized as follow. In Section 2, we discuss IoT architecture and reference model. In Section 3, a short introduction to the technical perspective of blockchain is presented. Related work is presented in Section 4. Our proposed governance framework is presented in Section 5. In Section 6, the proposed framework is evaluated.

2. IoT architectures and reference model

IoT includes large number of different types of devices, protocols, and architectures; therefore there is no unified IoT reference architecture. Since, a single reference architecture might technically not suffice thus multiple reference architectures can simultaneously exist [19]. Internationally standardized reference architecture guarantees that connected systems are "seamless, safer and far more resilient" [75]. Various layered architectures [14,74] are proposed; for instance, three-layered [76] and five-layered architecture [76,77]. The three-layered architecture is fundamental, though inadequate due to the continual innovation in the field of IoT [78] and it can not fulfill all the requirements of IoT for diverse application domains. The three-layered architecture consists of perception, network, and application layer. While the five-layered architecture consists of perception layer, network layer, middleware layer, application layer, and business layer as demonstrated in Figure 4. Six-layered is the new optimized IoT reference architecture. Blockchain technology is embedded in six-layered IoT architecture. An illustration of six-layered IoT reference architecture is shown in the Figure 4. In IoT implementation, it is important to realize IoT architecture in order to understand the roles and features of every layer of the architecture, enable compatibility, and consequently IoT deployment. Below we describe the six-layered architecture along with the security mechanisms and threats associated with each of these six layers. Even though, the impact of these threats may vary as the impact of the threats depends on the IoT application domain.

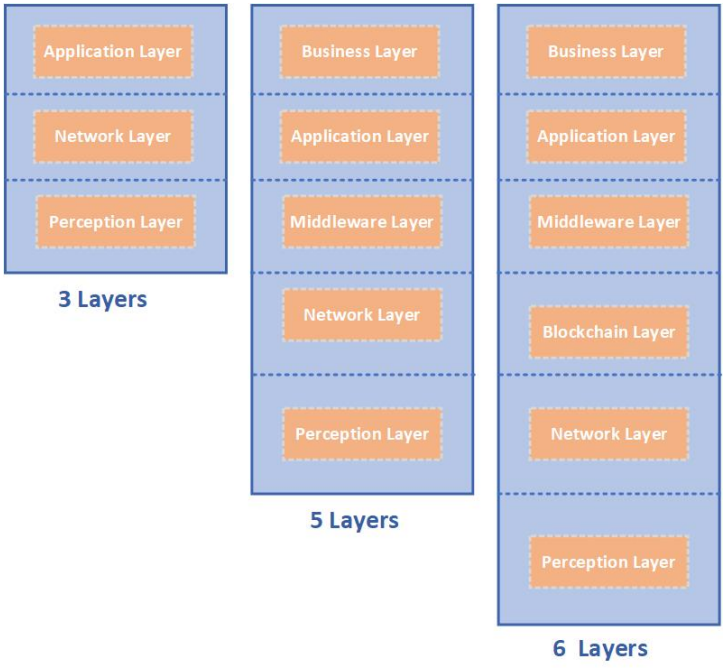

Figure 4. Six layers IoT reference architectures for blockchain-enabled IoT ecosystem.

2.1. Perception layer

It is the physical layer that mainly consists of sensors, RFID tags, and actuators. Security mechanisms required at this layer are data protection, physical security, and lightweight encryption and key management [78,82]. As most of these devices are resource constrained, simple security mechanism can be applied here; therefore, IoT devices are mostly vulnerable. Most common threats of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

perception layer are eavesdropping, node capture, replay attack, timing attack [78], sybil attack, and sniffing attack.

Roles and objectives

This layer is responsible for device identification and data collection. The data collected is forward to the network layer [76].

2.2. Network layer

This layer consists of wired and wireless communication protocols; such as ZigBee, Bluetooth, and WiFi. Frequent security threats to this layer are denial of service (DoS), man-in-the-middle, and storage attack [78]. Security mechanisms required at this layer are identity authentication, encryption, communication security, and trust mechanisms.

Roles and objectives

The role of this layer is to transmit sensor data using communication protocols to data processing entities.

2.3. Blockchain layer

Blockchain layer is a new bridging layer between network layer and middleware layer for blockchain-enabled IoT ecosystem. Blockchain is also vulnerable to various attacks such as double-spending, identity theft, illegal activities, denial of service (DoS), reply attack, and system hacking [79–81].

Roles and objectives

Blockchain characteristics such as immutability, consensus, traceability, decentralization, and automated execution of rules are utilize in this layer for transparency, security, privacy, and trust purposes.

2.4. Middleware Layer

Numerous IoT devices are deployed to attain diverse IoT services. IoT devices communicate and exchange data to deliver these services. This layer consists of ubiquitous computing, integration, data analytics, service management, and databases. Attacks possible at this layer are DoS and malwares [78]. Security mechanisms required for this layer are authentication, encryption, communication security, and trust mechanisms.

Roles and objectives

The purpose of this layer is service management and database management [14,61]. The data received from network layer is further processed to extract useful information and execute service oriented decisions.

2.5. Application layer

This layer consists of application programming interface (APIs), interfaces, and data representation. Attacks possible at this layer are cross site scripting, malicious code attack, sniffing attack, phishing attack, and sensitive data leakage [78]. Common Security mechanisms required to secure application layer are access control, authentication, key management, encryption, API protection, and trust mechanisms.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

Roles and objectives

The purpose of this layer is to provide application management for IoT applications such as smart logistics and smart agriculture.

2.6. Business layer

This layer consists of business models, business requirements, and visualizations. Attacks possible at this layer are business logic attack and zero-day attack [78]. Security mechanisms required at this layer are secure business logic programming and secure data exchange.

Roles and objectives

This layer is responsible to efficiently manage IoT system, execute business related decisions in order to attain business profits, to ensure users privacy and, plan future strategies.

3. Blockchain

Blockchain, which is a peer-to-peer network, is an alternative to centralized network architectures. Existing centralized networks depend extensively on intermediaries, and these intermediaries pose significant risks such as data tempering. Third parties or intermediaries interference can lead to various potential breaches [33,84]. Therefore, a decentralized blockchain technology, without trusted intermediaries, is required for secure and trustless networks. Blockchain is made of "blocks" which consists of transactions and these "blocks" are linked together cryptographically to form "chain". A block's data field mainly consists of block number, hash of the block data, size of block, transactions, time stamp, hash of the previous block, and a nonce. Peers verify blocks using cryptographic hashes [33]. Genesis (initial state of the chain) is the first block of the blockchain network. Other blocks are added based on the underlying consensus algorithm. Blocks are chained together by referencing a previous block's hash. Since blocks reference previous blocks, thus if a block is changed so the hash value will change and thus all the succeeding hashes will change [86]. The way blockchain works, totally depends on the application domain or requirements; there are no standardized specifications to design and employ blockchain. Blockchain developers and architectures are free to select any combination of algorithms. Figure 5 shows how blockchain works.

1. public key cryptography can be used to communicate with the blockchain. Where users are identified by their public key and private key can be used to digitally sign transactions
2. in a peer-to-peer network, a peer generates digitally signed transactions which contain the transfer of funds
3. the signed transactions are broadcast in the peer-to-peer network
4. neighbouring peers validate the transactions and spread the transactions across the entire network
5. miners form blocks of the validated transactions
6. blocks are broadcast in the network
7. the nodes verify and valid the blocks and validated blocks are added to the ledger
8. eventually, transactions are executed

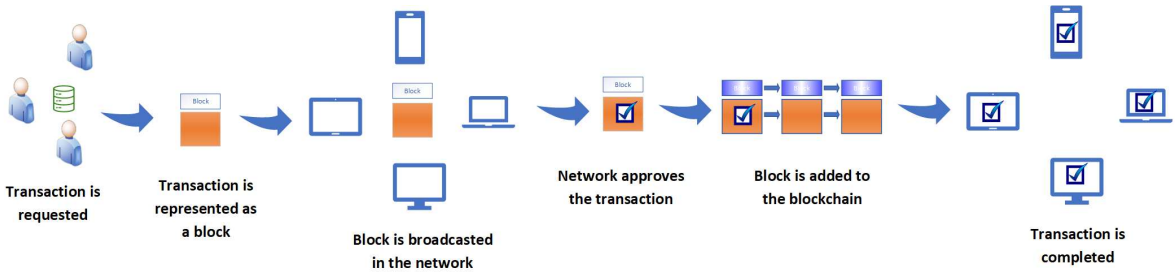

Figure 5. Blockchain working mechanism.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

Blockchain enables fast transactions since there is no centralized intermediaries. Furthermore, blockchain allows to store data in transparent, verifiable, and immutable manner in the distributed ledger. Every node in the blockchain network keeps a copy of the ledger. Various blockchain permission models are proposed. In a permissionless model, every peer in the network can participate and add a new block to the ledger without requiring permission to join the network. In a permissionless, no trust is required among the peers in order to communicate and execute transactions. In a permissionless network, peers identify other peers through their public addresses. However, malicious users might attempt to manipulate the ledgers or add erroneous blocks. In order to circumvent such malicious behaviour, blockchain uses consensus algorithms where peers are required to demonstrate certain capabilities or resources [86]. Through consensus algorithms, the nodes verify and validate the transactions. In a permissioned blockchain network, only authenticated peers are allowed to participate and add new blocks; only whitelisted peers can read and write to the ledger [86]. Since only trusted peers can execute transactions in the permissioned model, therefore consensus mechanisms are typically faster [86]. In a permisssioned blockchain network, to some extent, there is trust among the participating peers [86].

Consensus "is the process in which a majority (or in some cases all) of network validators come to an agreement on the state of a ledger. It is a set of rules and procedures that allows maintaining coherent set of facts between multiple participating nodes" [83]. In blockchain technology, consensus protocols are used to attain a common agreement on transactions or ledgers. In order to reach consensus, peers are required to agree on transactions; otherwise forks are formed. In forks, each peer have a distinct copy of the ledger. In a permissionless networks, many peers are competing to add the next block to the chain. The peer that adds the block is rewarded with transaction fees. On average, Bitcoin consensus requires 10 minutes before adding a block to the ledger [33]. Once blocks are added to the ledger it can not be modified since blockchain records are immutable. When two peers solve the block at the same time then forks are formed and peers have different ledgers. To solve this conflict, the longest chain is considered as the valid chain and peers embrace it [86]. Furthermore, technologies are regularly updated to improve performance or add new features. Updating a blockchain protocol is also called forks. There are two types of forks, soft and hard forks. Soft forks are the changes in blockchain protocols that are backward compatible. While hard fork are the changes that are not backward compatible. As mentioned earlier, forks are normally formed when multiple miners solve the block at the same time or there are conflicts in the ledger. However, there are various mechanisms to resolve such forks.

Some of the well-known consensus algorithms are proof-of-work (PoW), proof-of-stake (PoS), and practical byzantine fault tolerance (PBFT). These algorithms work significantly different from each other. Each of these algorithms retain both pros and cons. In proof-of-work (PoW) consensus mechanism, nodes solve computationally complex puzzle in order to add the next block. To solve the puzzle, miners generate hash value that should meet certain requirements. Various hashing algorithms are used in mining [39]; such as SHA-256 [29], scrypt [30], and Blake-256 [31]. Bitcoin uses PoW consensus mechanism [86]. PoW is known to be computationally the most intensive consensus mechanisms. Miners performs computationally intensive PoW operations in order to add the next block to the chain. All other nodes can easily verify that the computations performed are correct and then add the block to the chain. Miners are rewarded for their computation. In private blockchain networks, computationally intensive PoW mechanism is not necessary since there are less chances of Sybil attacks [39]. PoW can prevent blockchain network to some extent from denial of service attack [86]. PoS is another consensus mechanism where block is added to the chain based on the balance (stake) of the peer. Peers having high balance have more chance to add the next block. The advantage of PoS is that it is not computationally intensive. It can be used in permissionless blockchain networks. It is implemented in Ethereum Casper and Krypton [86]. The main disadvantage of this mechanism is that it is vulnerable to 51% attack and peers with high stakes can control the network [86]. In PBFT consensus mechanism, it is assumed that consensus can be reached as long as $n = 3f + 1$ correctly

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

working nodes are present in the network, where f represents faulty nodes and less than $1/3$ of the nodes are faulty [95]. And $2f + 1$ network nodes are required for consensus on the block. PBFT is an energy efficient consensus algorithm and suitable for private (permissioned) blockchain networks. PBFT is implemented in Hyperledger Fabric [96]. The limitation of PBFT is that it is not suitable for large scale networks. To improve the performance of PBFT, various variations are proposed. Other consensus mechanisms include delegate Proof of Stake (DPoS) [88], proof-of-Elapsed-Time (PoET) [89], lease-proof-of-stake (LPoS) [90], proof-of-capacity (PoC) [90], and proof-of-interaction (PoI) [90].

Two types of record-keeping models are popular in today's blockchain networks. The first method is called the unspent transaction output (UTXO) Model [38] and the second one is the account-based model [38]. The UTXO model is employed by Bitcoin, and Ethereum uses the account-based model [38]. Blockchain that supports the UTXO model is uniquely suited for the transfer and tracking of digital tokenized assets, whereas blockchain that supports the account-based model is aimed to run arbitrary logic and establish verifiable multi-step processes (smart contracts) [39]. Over the course of time, various applications based on blockchain are developed. Bitcoin is a standard and well known application of blockchain. The motive behind blockchain technology is not limited to cryptocurrency applications [57] but it is far beyond that. Legislators in various US states are using blockchain for different purposes such as secured records storage and smart contracts [64,66,67]. Track and trace mechanism is very important in IoT applications particularly in smart logistics. Blockchain technology can provide a trusted infrastructure to track and trace both physical objects and information [57]. Other characteristics of blockchain applications are immutability of information, transparent sharing of information and automated business processes [57]. Many different types of blockchain frameworks are being developed for various purposes [46]. Such as Bitcoin [91], Ethereum [115], Ripple [92], Hyperledger [96], BigchainDB [104], Corda [107], Quorum [93], Tezos [94], Multichain [106], Hashgraph [119], IOTA [121], and R3 [125]. Various classifications of blockchain are presented in [59,60].

3.1. The mechanics of Smart contract

Smart contract is a popular application of blockchain technology since it can be implemented easily and efficiently [33] and it has wide range of use cases. smart contract is a "a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries" [32]. Smart contract is a set of rules and policies that are executed automatically on the blockchain. These rules and policies are programmed into blockchain. Smart contract enforces immutability and automation through cryptographic mechanisms. When certain already agreed conditions are met, smart contracts execute tasks automatedly without the necessity of third party interference. Therefore, intermediaries or centralized third parties are not required to enforce contract. Any computational logic or functionality implemented on the blockchain can be regarded as smart contract, which otherwise is manually enforced in traditional contract. Peers in the blockchain network execute smart contract, all the peers in the network agree on the results and the results are recorded on the blockchain. In a permissionless blockchain network, peer pays fee for executing transaction. Smart contract can be used for various applications such as financial [86], random number generator [87], supply chain, financial, legal, intellectual property, and insurance. Smart contract has many unique characteristics; it is tamper evident and tamper resistant [86]. Which demonstrate the transparency characteristics of smart contracts. Smart contract yields many advantages since manual executions are time consuming and error prone [33] and it can save up to $4 billion costs spent in error and manual efforts [85]. Smart contracts are deterministic; for a certain input it must always generate the same output [86].

Various implementations of smart contract are introduced such as Ethereum smart contract and Hyperledger Fabric chaincode. Ethereum is considered as an extension of bitcoin as it supports wide

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

range of applications [33] such as Ethereum smart contract. As shown in the Figure 6, Ethereum Virtual Machine (EVM), which is a part of Ethereum, is a computation engine where smart contract code is executed and handles deployment of smart contract. Ethereum is a transaction-based state machine [97]. Miners or account holders initiate transaction execution in order to perform a task. When smart contract is invoked, EVM changes the Ethereum state as per the Ethereum protocol. The account that requests transaction pays transaction fees in Ether (Ethereum cryptocurrency). The miner is awarded the fees after successfully execution of the transaction. Ethereum smart contracts are written in high level programming language such as Solidity. Solidity is compiled into EVM bytecode instruction. The EVM bytecode is deployed on the Ethereum blockchain network. EVM provides large set of functionalities such as arithmetic operations, stack operations, system operations, logic operations, block operations, and environment operations [97].

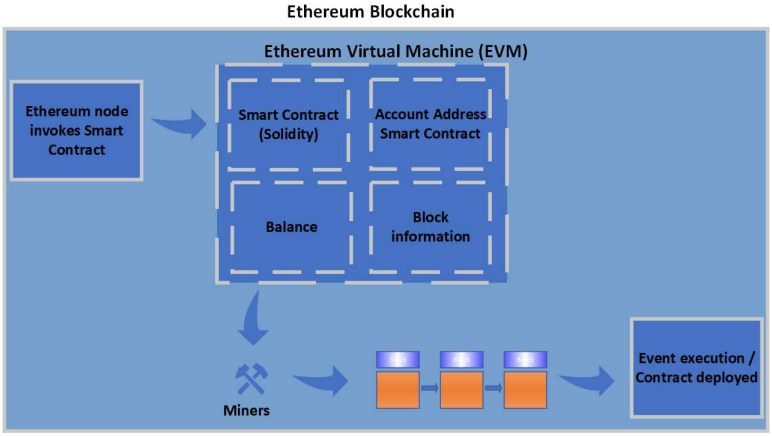

Figure 6. Ethereum Virtual Machine (EVM) working mechanism.

3.2. Role of blockchain in governance

Blockchain is not only beneficial for upholding security, privacy, and trust. But it can also be used as a governance mechanism. Contracts are inscribed to align the interests of organizations working together. Contracts are mainly enforced among multiple parties in order to collaborate and cooperate. Contracts are aim to legally enforce the rights and obligations and each party is obliged to adhere to the contract conditions. Inter-organizational collaboration is challenging due to various reasons such as mistrust among the partners [59], large number of intermediaries, and overall the processes are error prone [64]. However, inter-organizational collaboration is highly important and advantageous [59]. Technologies are adopted to improve transparency and verifiability in collaboration among partners [64]. Exchanging data among many partners collaborating is quite challenging for various reasons; such as data ownership, business secrets, and privacy consequences. Accountability, predictability, and common understanding are the three conditions required in order to collaborate [37,45]. Governance plays an important role in achieving these three requirements and therefore organizations refer to governance mechanisms [37]. The rules and regulations of the contract can be self-enforcing, manually or enforced legally (national laws). In traditional collaboration, task are executed manually and manual execution is not only error prone but also it is time consuming and conflicts can arise. Blockchain can play an important role to enforce the contract in a decentralized and transparent manner. For instance, in the smart contract scenarios, the rules of the contract are enforced automatedly through blockchain technology (protocols and code-based rules) [37]. Blockchain allows in real-time and decentralized manner to verify and validate policies and rules agreed among the partners. Furthermore, immutability, transparency, and traceability characteristics of blockchain can be used to establish intra-organization and inter-organization collaborations [37,42]. Other novel characteristics of blockchain are decentralized consensus and machine-based automation [37], which can make collaborations fast, reliable [37], and boost confidence in the fairness of the evaluation of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

data and quite easy to perform audit in case of fraud or error. Through decentralized consensus, data integrity can be achieved and it is hard to tamper with the data [37]. The consensus and smart contract characteristics of blockchain are very beneficial to automatically execute the agreed obligations among multiple parties collaboration context [64]. Thus, blockchain can potentially resolve the existing inefficiencies of multi-parties coordination [64].

4. Related Work

Various analyses and sentiments can be found in the literature regarding blockchain-IoT integration and governance. Since governance by blockchain and governance for blockchain are two different terms, in this section, we present related work concerning IoT governance, role of blockchain as governance mechanism, and governance for blockchain.

4.1. IoT Governance

Numerous governance frameworks are proposed in the literature. Copie et al. [12] presented IoT governance aspects that are closely related to cloud governance with the main focus on security, privacy, and standards. The proposed IoT governance is a multi-agent governance architecture with the defined roles for agents. The agents are vendor, deployment, proxy, audit, monitoring, aggregation, user interface, software Thing, Thing management, security management, audit management, and governance management. Salazar et al. [15] proposed a generic governance model for IoT solutions, aiming to improve the implementation and management of IoT applications. They have described development strategy, skills, roles, standards, processes, and policies to be incorporated in IoT governance. Processes and policies module includes various principles such as technical management, complexity of the IoT solution, device vendor, portfolio management, and Operational management. Ruithe et al. [24] proposed a generic data governance framework for IoT-cloud domain. The authors have identified key concerns related to IoT-cloud convergence. IoT-cloud governance roles (to monitor security), responsibilities (providing updates, patches), and policies (security, privacy, integration etc.) in relation to security and privacy are presented in the form of a framework. Kazmi et al. [35] proposed a smart governance framework in order to manage heterogeneous IoT devices and enable interoperability across various domains in Smart cities. In their proposed mechanism, IoT data and services are integrated from heterogeneous IoT networks and then monitored and governed from a central point. Centralized governance layer provides various services such as ensuring to meet business requirements and enforcing security policies. An international framework for IoT governance is proposed in [21]. In this framework, various roles and purposes that are deemed required in implementing international governance are proposed. Purpose determines the scope and definitions of terms that might be used. Several roles are discussed as potential IoT governance stakeholders such as government, private sector, and civil society. Dasgupta et al. [1] proposed a conceptual framework for data governance in IoT-enabled ecosystem. The authors have enhanced the 4I (identify, insulate, inspect, improve) framework in order to inscribe the necessity of a vigorous data governance in IoT-enabled ecosystem. They have proposed Design Science Research (DSR) mechanism to evaluate and develop the 4I framework. Moreover, several existing IoT frameworks such as Microsoft Azure [98], IBM BlueMix [99], Xively [100], IoTivity [101], and ThingSquare [102] have adopted IoT governance to some extent; for instance, governance for encryption, cloud, and device itself.

4.2. Role of blockchain as governance mechanism

Lumineau et al. [37] researched the role of blockchain as governance mechanism within an organization and across organizations. Based on their analysis, blockchain can potentially play an important role in encouraging well defined cooperation and coordination. They have argued blockchain has the capabilities of efficient governance mechanisms and is different from contractual and relational governance mechanisms and many real-world examples are mentioned to demonstrate that blockchain can facilitate coordination among various organizations. Various arguments are

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

presented by the authors to highlight applications of blockchain and ultimately how blockchain can be used as governance mechanism due its decentralization, automation, and immutability characteristics. The authors in [57] mentioned various characteristics of blockchain to motivate the role of blockchain as a governance mechanism. The characteristics mentioned are immutability, track and trace, elimination of centralized or third parties, peer-to-peer transactions, automation of processes, and transparent consensus. These characteristics can be beneficial in many applications domains such as e-voting, corporate governance, finance, and smart logistics. Elst and Lafarre [64] proposed a governance framework based on permissioned blockchain to solve various stakeholders' problems regarding third party system of shareholder engagement. These problems are mainly divided into two categories: 1) lack of transparency and trust between shareholders and 2) information problems and inequalities among shareholders. Based on their discussion, blockchain can be used by shareholders to perform voting, execute majority requirements for certain decisions, and implement access rights for shareholders without any need of intermediaries. Falco et al. [68] studied the potential impact of blockchain on corporate governance specifically on board of directors and institutional investors. A survey is conducted which included 47 corespondents from various countries. Based on their respondents interview results, blockchain can impact areas such as ownership, voting, turn out rate, market liquidity, and transparency. Qi et al.[69] discussed applications of blockchain in e-governance to enhance service quality and efficiency. Last but not least, transparency and traceability features of blockchain allow to embrace the Shareholder Right Directive (EU Directive 2017/828) regulations more effectively [68]. Furthermore, blockchain can fulfill certain provisions from Shareholder Rights Directive II [65].

4.3. Governance for Blockchain

Pelt et al. [46] proposed a conceptual blockchain governance framework. The framework consists of six dimensions and three layers. The six blockchain governance dimensions are: 1) formation & context which illustrates the purpose of the BC, 2) roles describe responsibilities and accountabilities of the participants, 3) incentive describes the motive behind the roles assigned, 4) membership illustrates the mechanism to manage the participation and membership, 5) communication illustrates the mechanism of communication between the stakeholders, and 6) decision making illustrates achieving consensus and solving conflicts. And the three layers of blockchain governance are 1) off-chain community, 2) off-chain development, and 3) on-chain protocol. Furthermore, it is discussed which governance tasks from the six dimensions can be performed off-chain community, on-chain development, and on-chain. The framework is evaluated by conducting expert interviews and use cases. In [57], a general overview and a mechanism to govern Blockchain consortia where multiple parties are involved in the project is presented. It includes discussion related to setting up the blockchain consortium in a multi-parties coordinated project, off-chain governance such as executing standard business practices and agreements among the partners, and on-chain governance in order set up blockchain and to evaluate the blockchain progression. Ziolkowski et al. [59] discussed how blockchain governance mechanisms of 15 different blockchain frameworks are governed. They have identified six core decisions in order to govern blockchain which are demand management, data authenticity, system architecture development, membership, ownership disputes, and transaction reversal. Four application domains (supply chain, land registry, cryptocurrencies, intellectual property rights management) are presented as use cases to demonstrate how these core decisions can be transformed into practice. Experts interviews are conducted to study how the key decisions are enacted in practice. In [46], three layers of blockchain governance are discussed where governance requirements can be accomplished. The three layers are Off-chain community, off-chain development, and on-chain protocol. Off-chain community illustrates executing governance tasks in the real world, Off-chain development illustrates governance decisions regarding software development in the real world, and on-chain protocol illustrates the governance tasks that are executed on the blockchain protocols. In [57], two layers of blockchain governance are discussed which are on-chain and off-chain. In on-chain

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

governance, rules are hard-coded and in off-chain, decisions are made through informal process. On-chain governance provides fairest, flexible, transparent, and decentralized type of governance [57]. However, some policies are perhaps not feasible to execute on-chain such as decision regarding protocol updates or it is computationally intensive, so therefore these tasks can be performed off-chain. Although, off-chain governance is flexible, but there are risks of error, manipulation, and transparency. An advantages of off-chain governance is that it allows to perform both formal and informal decision in more flexible processes [57]. Through effective governance for blockchain, long term sustainability of the blockchain technology can be achieved. As per EU blockchain observatory and forum, it is important to specify who is responsible for the future blockchain changes required over time and how to enforce the changes [57]. Due to the lack of absolute governance mechanism, there have been many disputes and scandals [57,58]. As mentioned in [54,56], there is lack of significance research in the direction of blockchain governance. Furthermore, as yet it is not obvious or clearly manifested how to execute critical resolutions and how to enforce decree in the blockchain [55].

5. Blockchain-IoT governance

The aim of this research is to develop a decentralized, automated, and shared-value governance mechanism for blockchain-enabled IoT ecosystem and as well as utilizing novel characteristics of blockchain for the purpose of governance - to achieve governance requirements. Numerous governance requirements are proposed. These requirements are discussed in the context of smart logistics as shown in the Figure 7 as a use case. Where every partner in the consortium can transparently verify, monitor, and configure the governance module. The proposed methodology delivers an umbrella framework for agreements in multi-party collaborations and ensures to fulfill the objectives of each and every partner. We propose variable geometry based approach to form collaboration among partners and accomplish the governance requirement. In this section, we discuss variable geometry governance approach, the proposed governance requirements for blockchain-enabled IoT ecosystem, and the mechanisms to accomplish these requirements.

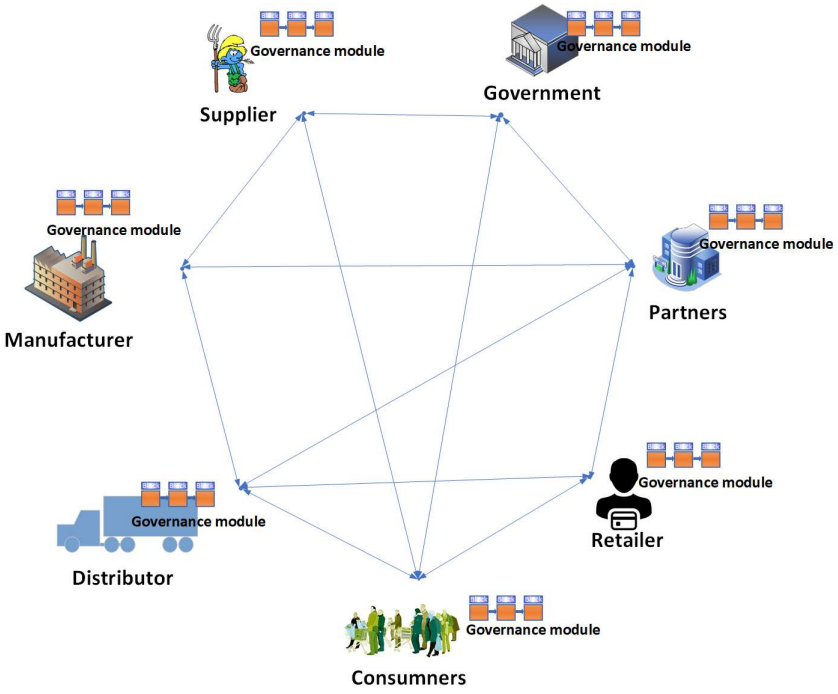

Figure 7. Distributed governance framework for blockchain-enabled smart logistics.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

5.1. Variable geometry approach

There are various organizational models to form collaboration among partners and to coordinate policies and responsibilities at organizational level. Namely:

1. Top-down approach is a centralized approach where a single entity is managing all the other entities.
2. Bottom-up approach is where multiple entities are involved in the decision-making process. Top-down and bottom-up approaches are not preferable for complex scenarios [19].
3. Variable geometry approach is a multi-level approach - combination of multiple mechanisms. It is a more broader approach thus appropriate for complex [19] and heterogeneous scenarios. Complex scenarios which includes multiple stakeholders, varying interests, and diverse application domains where certain partners can adhere to the overall obligations and certain partners can adhere to some selective obligations. Such mechanism is less restrictive and can potentially enhance cooperation among regional and international partners. It provides flexibility during the negotiation process [103]. We propose variable geometry approach to implement the governance requirements.

Financial, business or in some cases legal differences among the partners arise. These differences effect the way collaborations are formed. Such differences are undesirable and can lead to conflicts. Single agreement might not be efficient. Conflicts can be resolved by accommodating the interests of partners in the consortium. And partners having the option to opt out of conditions or policies that do not meet their financial or business interests. In variable geometry approach, partners are not required to make the same commitments as other partners. Allowing less restrictive and flexible cooperation and such model can enhance innovations and agile developments. Variable geometry demonstrate new mechanisms of overcoming negotiation challenges and potentially leads larger co-operations [103]; since it ensures flexibility in negotiation by not enforcing the complete set of obligations. Variable geometry approach [103] include strategies to address differences in the regional or multilateral agreement among the partners. Partner agreeing on certain conditions should execute efforts to fully comply with it. The partners only avail the benefit of the agreements to which they agree to adopt. Flexible model is required for complex processes of negotiations. Even though variable geometry approach is complex and difficult to design but it offers better integration of multiple entities (partners) [103]. International organization such as World Trade Organisation (WTO) and economic union such as EU have reflected on this approach to facilitate the negotiation process during multi-parties collaboration [103,105].

Variable geometry approach yields flexibility in forming private channels among the members where certain partners could agree to certain obligations but not all. Also channels can be formed between individual partners, if they are willing to have private channels independent from the other partners. The policies and conditions are decided by these individual partners themselves. Channels can be formed among subsets of partners who independently agree on subsets of policies or conditions to meet partners' specific requirements. In variable geometry approach, stakeholders or signatories can have common policies where all the stakeholders agreed upon and also some policies for individual stakeholders who request or form specific agreements. However, parties willing to join the consortium should adhere to certain specified pre-conditions to meet the integration criteria. In private channels, certain policies might not be implemented on them or certain might only be implemented for them based on their desires. Such approach takes into consideration unwillingness or non-uniformity among the partners. In such model, partners have freedom regarding signing agreements of their interests and are not necessarily required to undertake every agreement [105]. However, partners are only awarded the advantages of the agreements they are signatories of. Variable geometry approach consists of common and private agreements as discussed below.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

1. Common agreements are applied as pre-conditions to every partners to achieve the fundamental interests of every partner and collective aim of the consortium. For instance, all the partners agree on privacy and security requirements.
2. Private agreements that are agreed among partners while forming channels to provide certain services. Multiple stand-alone agreements can be signed, where every contracting party is free to join any agreement they want. For instance, certain partners can agree among themselves on a specific cost model for a service.

Blockchain technology is comprised of distinctive frameworks and thus exceptionally suitable for variable geometry approach. Enterprise blockchain has different paradigm than public blockchain [126] because enterprises are profoundly discreet about the business data and processes [126]. For instance, in public blockchain, it is expected that every transaction is public, however, in enterprise blockchain, businesses are not willing to make all transactions public for various reasons such as business secret and competition [126]. Therefore, certain blockchain frameworks allow forming private channels among partners, such as Hyperledger fabrics [96].

5.2. Proposed Governance Requirements

We demonstrate specific proposals to establish a legal framework for blockchain-enabled IoT ecosystem, which includes the following requirements. It is essential to address these requirements in blockchain-enabled IoT governance framework. These requirements lay foundation of a comprehensive governance mechanism and provide significant value to the consortium (collaboration) and services. Where viable, we further categorize these requirements into sub-categories as shown in the Figure 9. Furthermore, the proposed mechanism is highly flexible - the proposed requirements can be adopted according to the individual needs of the consortium. Table 1 summarizes which requirement to implement during off-chain or on-chain development.

Table 1. The table shows which requirement of the governance can be executed Off-chain and on-chain. For the purpose of simplicity and clarity we will follow two layers (on-chain and off-chain) governance.

Requirement	**Off-chain**	**On-chain**
Purpose	✓	✓
Ethics	✓	✓
Transparency	-	✓
Audit	✓	✓
Interoperability	✓	✓
Architecutre	✓	✓
Security	✓	✓
Privacy	-	✓
Fault tolerance	-	✓
Performance measurement	✓	-
Cost	✓	✓
Scalability	-	✓
Automation	-	✓
Sustainability	-	✓
Support	✓	✓

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

5.2.1. Purpose

At the time of consortium (collaboration) formation, the purpose behind the blockchain-IoT adoption needs to be decided. Purpose can be subdivided into three categories; problem, vision, and roles. For instance, which problem blockchain-IoT can potentially solve, will blockchain-IoT be able to effectively solve the problem and what value it will return or generate. After initial agreements on blockchain-IoT added values to the consortium, a formal organization can be formed with all the partners and agree on the initial goals of the project. A dedicated team is required to decide the intellectual property rights. Then roles which include actors and their responsibilities are decided, such as who supports what values and who contributes what. Private and public sectors have different roles and responsibilities. The role of each actor or partner need to be clearly identified and agreed upon. It is important that each partner interrelate and coordinate with all the other partners [57]. Roles might include international, national, and regional actors. Clear policies regarding participation in the blockchain network, for instance, who can execute transaction, which nodes are allowed to read the ledger (data) and identify validators (miners) [57]. The agreements are clearly compiled in order to avoid future conflicts. Avoid over-regulation of the technical environment, as it can cause inessential burdens [19] and potentially lead to limitations on technical innovation. This requirement can be decided during the off-chain development and implemented in the on-chain development. On-chain policies are required regarding user authorization, access to data, achieve and maintain transparent consent among the users. Mainly, this requirement is included in the common agreement of the variable geometry approach.

5.2.2. Ethics

As per the EU commission, there are mainly six ethical issues: social justice & (digital) divides, trust, blurring of contexts (private vs. public), non-neutrality, agency (social contract between people and objects) and autonomy (informed consent vs. obfuscation of functionality) [20], and corporate social responsibility in enterprises [19]. Therefore, it is important to rise ethical awareness among people that are part of the blockchain-IoT consortium to ensure consent and fairness and avoid instilling backdoor and exploitation of users. Especially among developers, auditors, regulators, and stakeholders. Some of the ethical constituents that are required to be included in ethical policies are personal identity, autonomy of individuals, user consent, fairness, and social justice [19]. Development of adequate policies to enforce ethical aspects in the design and development of IoT solutions [19] and blockchain technology is vital. Awareness among citizens leads to the integration of ethics in technologies to some extent. All the partners should agree upon withholding ethics. Distinctive features of blockchain can be utilized to attain ethical principles. Ethics mechanisms mentioned above ought to be decided and agreed in the off-chain and implemented and verified during the on-chain development. This requirement could be included in the common agreement of the variable geometry approach.

5.2.3. Transparency

Transparency is an integral part of ethics and it should be adopted while making governance policies [19]. Principles regarding transparency are crucial in order to gain solid adaption since blockchain-IoT technology is still in its infancy state. The framework should elaborate which data to use, how to consent users, how to process and store data, why to collect and use data, who controls the data, data deletion, and how to ensure data transparency to achieve users trust. The framework should include polices that are legitimate and fair and it should upheld democratic principles of the society. Blockchain presents all these features of transparency. Various existing technological impediments (i.e. transparent tracking, validation, recording) can be solved through blockchain. Transparency can be

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

achieved through immutability, traceability, and consensus characteristics of blockchain. The choice of consensus mechanism can affect the security and balance of the blockchain [57]. There ought to be consequence for any wrongdoing by any entity. The consequences should be straightforward for the accountability bodies to impose and apply them fairly. Transparency requirement can achieved during on-chain development. And it could be included in the common agreement.

5.2.4. Audit

Audit is a process to continuously monitor the purpose and scope of controls. Such as analyzing that controls are functioning as required and controls are applied to systems or processes are part of the scope. The purpose of audit is to eradicate any fault, risk or vulnerability in the controls. Some auditing features are mentioned below.

- *Accuracy*: Assess the controls.
- *Completeness*: Are the controls adequate or there are gaps and are controls applied thoroughly.
- *Timeliness*: Controls are executed on time.
- *Resilience*: The controls are resilient to failures, there are backups if the primary controls fail.
- *Consistency*: Primary controls and secondary controls are correctly in placed.

Audit can be performed both on-chain and off-chain. Off-chain auditing is done to monitor individual partner's contribution and commitments. In on-chain auditing, technical tools and mechanisms are put in place to monitor the performance. Automated audit mechanisms based on blockchain could be implemented in order to audit common agreements as well as private agreements (channels).

5.2.5. Interoperability

As per the Internet Engineering Task Force (IETF) definition, Internet is "a large, heterogeneous collection of interconnected systems that can be used for communication of many different types between any interested parties connected to it" [22]. Internet consists of "core Internet" which is Internet service provider (ISP) networks and "edge Internet" which comprises of private and corporate networks [22], proprietary and off the shelf software and frameworks. For collaboration and cooperation, interoperability (platform independent solutions) across various partners, architectures and domain is vital. For instance, in existing single market such as European Union has invested significantly in fostering interoperability at various levels [118] in order to have e.g. a uniform digital indentification in the Union. Policies are adopted in European Interoperability Framework (EIF) and European Interoperability Reference Architecture (EIRA) to incorporate interoperability [118]. The framework should include mechanisms for interoperability both at network and architecture level but more importantly also about data exchange nationally and internationally among the partners. Interoperability can be applied at various layers such as legal, organizational, semantic, and technical [118]. Efficient and effective interopability policies can facilitate interactions among partners [118]. Key stakeholders are involved in decisions regarding which network architecture and technological strategies to use in order to maintain interoperability. Ensure interoperability among IoT ecosystems and with systems that are outside of the blockchain network perpetuate scalability of the diverse networks. Interoperability guarantees that existing systems are adjustable with the new innovations [19]. One of the main IoT challenge is the heterogeneity of IoT devices, different IoT devices have varying compatibilities, supports different protocols and different computational capabilities which makes the interoperability very complex. One way to overcome is to embrace or incorporate existing standards and governances (IETF, ICANN, Internet, RIRs, ISOC, IEEE, IGF, W3C, cloud governance, IoT reference architecture (Industrial Internet Reference Architecture (IIRA) and Internet of Things - Architecture (IoT-A), IEEE P2413) in the framework in order to avail their advantages. At the organizational level, the framework should dictate mechanisms

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

in order to form good relations with other national and international bodies. Interoperability requirement can achieved during off-chain (organizational and legal level) and on-chain development. This requirement is included in the common and private agreements of the variable geometry approach.

5.2.6. Architecture

There are three main types of architectures: centralized, decentralized, and distributed. There are pros and cons associated with each of these architectures. For instance, in centralized architecture, it is hard to attain privacy and networks based on centralized architecture can suffer single-point-of-failure [19]. In IoT infrastructure, availability is crucial for service providers [19]. Availability can be improved or made robust with distributed architecture [19]. IoT architectures should be able to cope with large number of users and there should be no restrictions on the number of users. Also mechanisms should be placed to reduce delay in communication of information between the users and systems or devices [19]. Blockchain technology is better alternative to existing centralized technologies. So incorporating blockchain technology in IoT ecosystem could be highly beneficial. Furthermore, any blockchain framework that is not compatible with IoT architecture can potentially hinder blockchain adoption in IoT ecosystem. Architecture requirement can achieved during off-chain and on-chain development. This requirement is included in the common and private agreements (channels) where partners can form channels of their own requirements.

5.2.7. Security

Security is one of the crucial governance requirements for various reasons. Mechanisms should be developed to ensure confidentiality, integrity, and availability. The framework has to embed strategies to ensure security at every level - infrastructure (devices, networks, integration, physical). Mechanisms should be in placed for continuous security hardening. Security requirement can be further categorised into sub-requirements such as physical security, end-to-end security, security best practices, security risk assessment, real-time intrusion detection and prevention, enhanced identification and authentication, and security audit. Various security mechanisms are proposed in the literature. Almeida et al. [10] recommended four principles to be incorporated in deploying IoT applications in order to secure users data and build trust in IoT. Which are: notice and choice, data minimization, access to personal data, and accountability. IoT devices are required to adhere to reasonable security requirements; for instance, including mechanisms for encryption, authentication, and access control. Ensure that user identifications can not be traced back. Various anonymity mechanisms such as ZCash anonymity and monero aonymity [57] are proposed. Most of the security requirements can be achieved through blockchain technology. Security requirement can be mainly achieved during on-chain development. However,in case physical security is required then that can achieved through off-chain. This requirement is included in the common and private agreements of the variable geometry approach.

5.2.8. Audit

Audit is a process to continuously monitor the purpose and scope of controls. Such as analyzing that controls are functioning as required and controls are applied to systems or processes are part of the scope. The purpose of audit is to eradicate any fault, risk or vulnerability in the controls. Some auditing features are mentioned below.

- *Accuracy*: Assess the controls.
- *Completeness*: Are the controls adequate or there are gaps and are controls applied thoroughly.
- *Timeliness*: Controls are executed on time.
- *Resilience*: The controls are resilient to failures, there are backups if the primary controls fail.
- *Consistency*: Primary controls and secondary controls are correctly in placed.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

Audit can be performed both on-chain and off-chain. Off-chain auditing is done to monitor individual partner's contribution and commitments. In on-chain auditing, technical tools and mechanisms are put in place to monitor the performance. Automated audit mechanisms based on blockchain could be implemented in order to audit common agreements as well as private agreements (channels).

5.2.9. Interoperability

As per the Internet Engineering Task Force (IETF) definition, Internet is "a large, heterogeneous collection of interconnected systems that can be used for communication of many different types between any interested parties connected to it" [22]. Internet consists of "core Internet" which is Internet service provider (ISP) networks and "edge Internet" which comprises of private and corporate networks [22], proprietary and off the shelf software and frameworks. For collaboration and cooperation, interoperability (platform independent solutions) across various partners, architectures and domain is vital. For instance, in existing single market such as European Union has invested significantly in fostering interoperability at various levels [118] in order to have e.g. a uniform digital indentification in the Union. Policies are adopted in European Interoperability Framework (EIF) and European Interoperability Reference Architecture (EIRA) to incorporate interoperability [118]. The framework should include mechanisms for interoperability both at network and architecture level but more importantly also about data exchange nationally and internationally among the partners. Interoperability can be applied at various layers such as legal, organizational, semantic, and technical [118]. Efficient and effective interopability policies can facilitate interactions among partners [118]. Key stakeholders are involved in decisions regarding which network architecture and technological strategies to use in order to maintain interoperability. Ensure interoperability among IoT ecosystems and with systems that are outside of the blockchain network perpetuate scalability of the diverse networks. Interoperability guarantees that existing systems are adjustable with the new innovations [19]. One of the main IoT challenge is the heterogeneity of IoT devices, different IoT devices have varying compatibilities, supports different protocols and different computational capabilities which makes the interoperability very complex. One way to overcome is to embrace or incorporate existing standards and governances (IETF, ICANN, Internet, RIRs, ISOC, IEEE, IGF, W3C, cloud governance, IoT reference architecture (Industrial Internet Reference Architecture (IIRA) and Internet of Things - Architecture (IoT-A), IEEE P2413) in the framework in order to avail their advantages. At the organizational level, the framework should dictate mechanisms in order to form good relations with other national and international bodies. Interoperability requirement can achieved during off-chain (organizational and legal level) and on-chain development. This requirement is included in the common and private agreements of the variable geometry approach.

5.2.10. Architecture

There are three main types of architectures: centralized, decentralized, and distributed. There are pros and cons associated with each of these architectures. For instance, in centralized architecture, it is hard to attain privacy and networks based on centralized architecture can suffer single-point-of-failure [19]. In IoT infrastructure, availability is crucial for service providers [19]. Availability can be improved or made robust with distributed architecture [19]. IoT architectures should be able to cope with large number of users and there should be no restrictions on the number of users. Also mechanisms should be placed to reduce delay in communication of information between the users and systems or devices [19]. Blockchain technology is better alternative to existing centralized technologies. So incorporating blockchain technology in IoT ecosystem could be highly beneficial. Furthermore, any blockchain framework that is not compatible with IoT architecture can potentially hinder blockchain adoption in IoT ecosystem. Architecture requirement can achieved during off-chain and on-chain development.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

This requirement is included in the common and private agreements (channels) where partners can form channels of their own requirements.

5.2.11. Security

Security is one of the crucial governance requirements for various reasons. Mechanisms should be developed to ensure confidentiality, integrity, and availability. The framework has to embed strategies to ensure security at every level - infrastructure (devices, networks, integration, physical). Mechanisms should be in placed for continuous security hardening. Security requirement can be further categorised into sub-requirements such as physical security, end-to-end security, security best practices, security risk assessment, real-time intrusion detection and prevention, enhanced identification and authentication, and security audit. Various security mechanisms are proposed in the literature. Almeida et al. [10] recommended four principles to be incorporated in deploying IoT applications in order to secure users data and build trust in IoT. Which are: notice and choice, data minimization, access to personal data, and accountability. IoT devices are required to adhere to reasonable security requirements; for instance, including mechanisms for encryption, authentication, and access control. Ensure that user identifications can not be traced back. Various anonymity mechanisms such as ZCash anonymity and monero aonymity [57] are proposed. Most of the security requirements can be achieved through blockchain technology. Security requirement can be mainly achieved during on-chain development. However,in case physical security is required then that can achieved through off-chain. This requirement is included in the common and private agreements of the variable geometry approach.

5.2.12. Privacy

Various definitions and types of Personal Identifiable Information (PII) and Sensitive Personal Information (SPI) are present in the literature [108,109]. Centralized servers own by third parties mostly have the capabilities to access, monitor, and manipulate users' data. Since digital technologies are able to discriminate or can be use for the purposes of discrimination or to track users' behaviour. Therefore, ensuring privacy can increase confidence in the technology and ultimately the businesses growth. Since assuring privacy is one of the key challenges in governance frameworks, therefore, service providers should take care of human integrity, identity and privacy while providing services [19]. Individuals should have full authority and control over their data (personal, financial, commercial etc.). The framework need to formulate policies regarding securing data from unauthorized access, limit data collection, data dissemination, and determine who has authorized access to the data. Perhaps, governance framework should ensure Compliance to existing European data protection laws such as data protection directive (95/46/EC) [110], ePrivacy directive (2002/58/EC)(2009/136/EC) [111] and General Data Protection Regulation (GDPR) [72]. GDPR [72] presented 6 requirements regarding user data processing which are lawfulness, fairness and transparency, purpose limitations, data minimisation, accuracy, storage limitations, integrity, and confidentiality [122]. These laws ensure protection of users' rights, protection of users' data, transparency and accountability by proposing various privacy paradigm such privacy by default, privacy by design, and privacy as confidentiality. Where necessary, anonymize the data to avoid personal identification; for instance, patterns of energy consumption of certain households can potentially be used to track their behavior or life style. This is because privacy is not a static entity, it varies with the application domain, the way data is collected, processed and stored. Other strategies and recommendations for building strong data privacy schemes are mentioned in [112]. Cryptographic mechanisms such as homomorphic encryption, k-anonymity, data obfuscation, Zero knowledge Proof (ZKP), Secure multi-party computation (SMPC), and ring signature can be used to attain privacy and anonymity [120]. Most of these privacy requirements can be achieved through privacy-preserving solutions for blockchain technology mentioned in the literature, such as [122]. And distributed ledger technology has the technological capabilities to to minimize privacy exploitation to some extent. Users can view the type of data is collected and stored. Blockchain

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

technology can solve privacy issues using various cryptographic mechanisms and through immutable, transparent, and distributed ledger characteristics of the technology. However, different blockchain frameworks impart different level of privacy [120]. Various mechanisms are demonstrated in [120] to attain privacy in Blockchain. Privacy requirement can achieved during on-chain development and it can be included in the common and private agreements (channels).

5.2.13. Fault tolerance

Fault tolerance is important for the availability of blockchain-IoT services and it is quite closely related to security since it improves security, trust, and performance. Fault tolerance is one of the major challenges in distributed systems since networks and systems are prone to faults, errors, and failures. Faults might arise due to various reasons such as hardware, software or networks or systems failures due to malicious error. The framework should determine fault tolerance mechanisms for blockchain-IoT so that the networks and systems remain reliable in fault or error circumstances and avoid random downtime. Although fault tolerance mechanisms depend on the architecture of the network, five common fault tolerance phases are suggested which are fault detection, fault diagnosis, evidence generation, assessment, and recovery [123]. Various static and dynamic data replication schemes are discussed in the literature in order to improve systems availability [124]. Although public blockchain is based on peer-to-peer network architecture, it has inbuilt capabilities of coping with faults. For instance, even if few nodes in the network are working correctly then blockchain can function. Therefore, it is beneficial to integrate blockchain and IoT technologies. However, fault tolerance mechanisms are required especially for software level and integration failures. Enterprise blockchain frameworks allows limited and authenticated nodes to participate in the consortium, and channels are formed among the enterprises. So, failure of a node in enterprise blockchain can have adverse impact on the consensus, since each enterprise is represented by its node and failure of a node can consequently lead to failure of the blockchain [126]. Any downtime in the enterprise blockchain can be highly costly [126]. Therefore, efficient fault tolerance mechanisms are essential in order to ensure the smooth functioning of enterprise blockchain and make infrastructure resilient to failures [126]. Also, different blockchain frameworks have varying fault tolerance capabilities. Podgorelec et al. [122] discussed and compared the fault tolerance capabilities of hyperledger Fabric and Iroha, which is based on the performance of consensus mechanisms. Fault tolerance requirement can achieved during on-chain development. And it is included in the common and private agreements.

5.2.14. Performance measurement

As mentioned earlier, collaborations are formed among the partners in order to provide various services to customers. It is important to regularly evaluate and determine the framework or business performance to ensure that it is beneficial to both users and stakeholders. Business requirements are evaluated against the current status, expectations and future policies and consequently strategies are determined. Performance metrics are established in order to keep track of success in the form of customer satisfaction, return on investment (ROI), and plan future improvements accordingly. Performance measurements include various key performance indicators (KPI) to evaluate the operations of service delivery [113]. Performance metrics can be used to contemplate the framework's capabilities, effectiveness, and fruition [113]. Various criteria such as return on investment (ROI) and total cost of ownership (TCO) are used to evaluate projects' performance; however, these two are not the only metrics [113]. For instance, Grembergen & Haes [114] presented balanced scorecard approach to measure performance. In this approach, various perspectives and objectives are demonstrated. Various types of performance metrics are discussed in [113], which includes process metrics, service metrics, enterprise goals, and sample metrics. Therefore, stakeholders can use a more comprehensive cost-benefit analysis performance measurement approach that is based on quantitative and qualitative indicators [113]. Performance measurement requirement can achieved during off-chain development. And it is included in the common and private agreements (channels).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

5.2.15. Cost

To maximize profit, partners require a suitable business model along with fair pricing strategies to avoid conflicts and to ensure that the price is suitable for the blockchain-IoT ecosystem. Pricing mechanisms include rules regarding charging users or stakeholders for the services. Cost model or pricing strategy play an important role in collaboration as it is used to identify business interests of partners and also fair pricing model can potentially attract large number of users. Various pricing mechanisms and policies are discussed in the literature [116,117]. Every pricing strategy has advantages and disadvantages. However, certain cost models are good match for IoT-blockchain, for instance the models that are affordable, flexible, and predictable. Deciding cost models is always challenging since there are various partners involve and there are various types of cost models. Some of the challenges of pricing are unpredictability, fairness, and making pricing enticing to users. Because different partners or users might have different usage patterns and different services might cost differently and some users might choose only selective services. Some of the well-know pricing models are pay per use and pay per device. In pay per use model users pay for the service as per the amount of usage of the service. Such a payment model is efficient and straightforward since the user pay only for the duration or amount it requires the service. This model can be based on duration of usage, data flow or power usage. In pay per device model, users pay per device service. For instance, fixed amount per month per IoT device. Other possible strategies are storage as a Service (SaaS), Software as a Service (SaaS), monthly or yearly support costs, and up-front charges. Cost requirement can decided during off-chain and implemented in the on-chain development and it is included in the common and private agreements (channels).

5.2.16. Scalability

As mentioned earlier, blockchain for IoT enhances trust and security of IoT. However, as the number of IoT devices are increasing at a very fast pace, lack of blockchain scalability and compatibilities capabilities can be an obsticle. Transaction rate of Blockchain based technologies is significantly slower than existing digital transaction systems [127,128]. For instance, Ethereum transactions per second (TPS) is 15-20 and average transaction confirmation time is 2 minutes and Bitcoin transactions per second is 3-7 and average transaction confirmation time is 25 minutes [127]. Lack of efficient scalability mechanisms can impact real-time transaction validations and can adversely impact the large scale adoption of blockchain. Therefore, integration of blockchain and IoT requires efficient mechanisms to enhance scalability, regulations are required regarding size and duration of data storage, transaction validation time, compatibility, and interoperability. Various mechanisms are proposed in the literature to improve blockchain scalability. For instance, Hazari & Mahmoud [127] has proposed a parallel proof of work mechanism to improve blockchain scalability. Boyen et al. [129] proposed a similar parallel mining mechanism in order to execute transactions swiftly. Other mechanisms to improve the scalability can be enhancing network latency, reducing transaction queuing, compitability between private & public blockchain and between IoT and blockchain, and simplifying smart contract complexity. Scalability requirement can achieved during on-chain development and it is included in the common and private agreements (channels).

5.2.17. Automation

Blockchain and automation are highly related. With the increase in the number of IoT devices and consequently increase in complexity; automation mechanisms are required to improve efficiency and speed but without compromising transparency and traceability. Blockchain is deployed in many application domains such as supply chain, trust building, and workflow management to achieve automation. Blockchain features of distributed architecture and automated execution of transactions without the interference of third-parties when certain conditions are met (smart contracts) are highly beneficial as these features avoid the threats associated with centralized architectures and third-party

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

interference. Efficient mechanisms for automated execution of transactions are required to improve productivity, performance, save costs, and avoid errors. Smart contract can play an important role in automation of various tasks in many diverse application domains. Scalability requirement can achieved during on-chain development and it is included in the common and private agreements (channels).

5.2.18. Sustainability

Internet is typically managed by various organizations such as Internet Engineering Task Force (IETF), Internet Research Task Force (IRTF), Internet Engineering Steering Group ((IESG) , Internet Corporation for Assigned Names and Numbers (ICANN) , Internet Architecture Board (IAB), and World Wide Web Consortium (W3C). Each of these organizations has varying responsibilities and purposes. The modern world is heavily dependent on Internet sustainability and is a critical resource for the entire mankind [22]. Therefore, international law is required for protection of this critical resource [22]. Blockchain technology has the potential capabilities of providing long term sustainable services and infrastructures such as automated compliance checks and integration with IoT [131], meeting the goals of 2015 Paris climate agreement [132], and eliminating corruption as per the United Nations Environment Programme (UNEP) 2030 goals [133]. However, blockchain is mainly dependent on heavy computational operations that requires significant power which is highly concerning for sustainability. Blockchain applications that consume high amount of energy are not environmentally sustainable [132]. The governance should consider the long term environmental and economical sustainability of the blockchain technology by reducing the energy consumption while not compromising the security. The blockchain framework should be capable to effectively evolve in order to adapt, change, and interact to environmental requirements. Sustainable blockchain mechanisms are mentioned in literature such as [134]. Sustainability requirement can achieved during on-chain development. And it is included in the common and private agreements (channels).

5.2.19. Support

Since, users are an integral part of the business, therefore, support requirement plays an important role in the success of a business. It is possible to retain and attract more customers through affable customer support mechanisms. The framework should adopt different strategies and methodologies regarding measuring and valuing customer satisfaction and achieving users' expectations. There are various types of support such as organizational support, technical support, and legal support which includes legal obligations and legal compliance. Support can be both remote, physical or in the form of documentation. Regularly evaluate if customers are satisfied with the services and then accordingly build policies and strategies. Various customer satisfaction and monitoring strategies are demonstrated in [130]. Support requirement can achieved during off-chain and on-chain development and it is included in the common and private agreements (channels).

6. Proposed governance framework use cases and evaluation

In this section, we demonstrate a smart logistics use case and then we apply our governance mechanism to the use case in order to analyze the feasibility of the proposed framework. In the smart logistics use case, we elaborate on the interests of each partner in the context of smart logistics. Then, we discuss how to achieve these interests through our proposed goverance framework. Furthermore, as shown in the Figure 10, we set up a two nodes Ethereum [115] consisting of standard voting illustration. Ethereum [115] is one of the largest public blockchain with respect to market capitalization [46] and it supports smart contract which we can use to implement the governance requirements. Solidity is used to develop the voting mechanism. The source code is available at [135]. The sole purpose of this setup is to demonstrate the feasibility of IoT (Raspberry Pi) and blockchain.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

6.1. Smart logistics use case

There are many use cases of enterprise blockchain such as financial agreements & transactions, smart contracts, records management & data sharing, smart grid, identity management & authentication, e-voting, and smart logistics [126]. Smart logistics include large number of distributed sensors, radio, and other technologies. Lets consider a smart logistics scenario in which a product such coffee from South America to Europe is being transported. There are multiple partners involved such as supplier, manufacturer, distributor, government, retailers, consumers, and other partners as shown in the Figure 8. Supplier supplies raw materials, manufacturer produces the product, and distributor distributes the product to the consumers. Supplier, manufacturer, distributor, and retailers get paid for their exertion. Governmental bodies are involve to implement the national protocols and laws for smart logistics. Other national and international partners might also be involved in the distribution as well. Collaboration among all these partners is very crucial for high quality smart logistics services. Every partner in the consortium has their own necessities and obligations. Supplier is expected to provide good quality of coffee. Consumers want to receive the product in the good order and avoid damage or loss of goods, and transparent origin of the product. Distribution can be through road, sea or air transport and the distributor ensures to avoid delay as much as possible and demonstrate transparent proof of delivery. The partners expect ethical policies regarding social justice, identity, autonomy, consent, and fairness. The consortium ensures compliance to agreements, commitments, and liabilities in case of non-compliance. To attain collaboration among diverse partners the consortium supports interoperability since the consortium might include heterogeneous devices, networks, and frameworks. Since smart logistics might consists of large number of devices, scalability and distributed architecture can be crucial. All the partners are concerned about confidentiality, integrity and availability. The overall purpose of the consortium is to provide an excellent smart logistics services and financial gain for the partners.

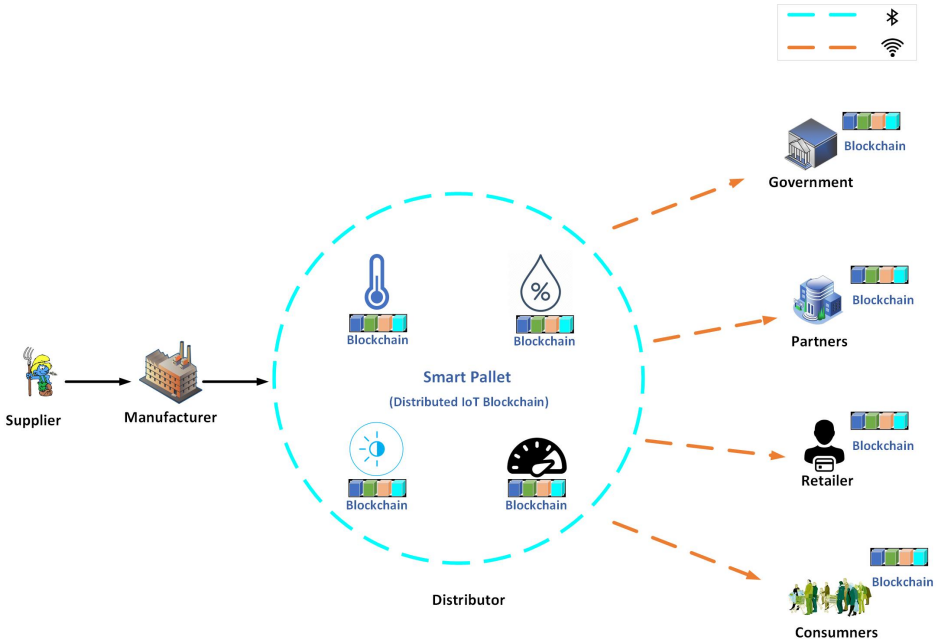

Figure 8. An illustration of ideal blockchain-enabled smart logistics scenario. We evaluate our proposed mechanism in smart logistics use case.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

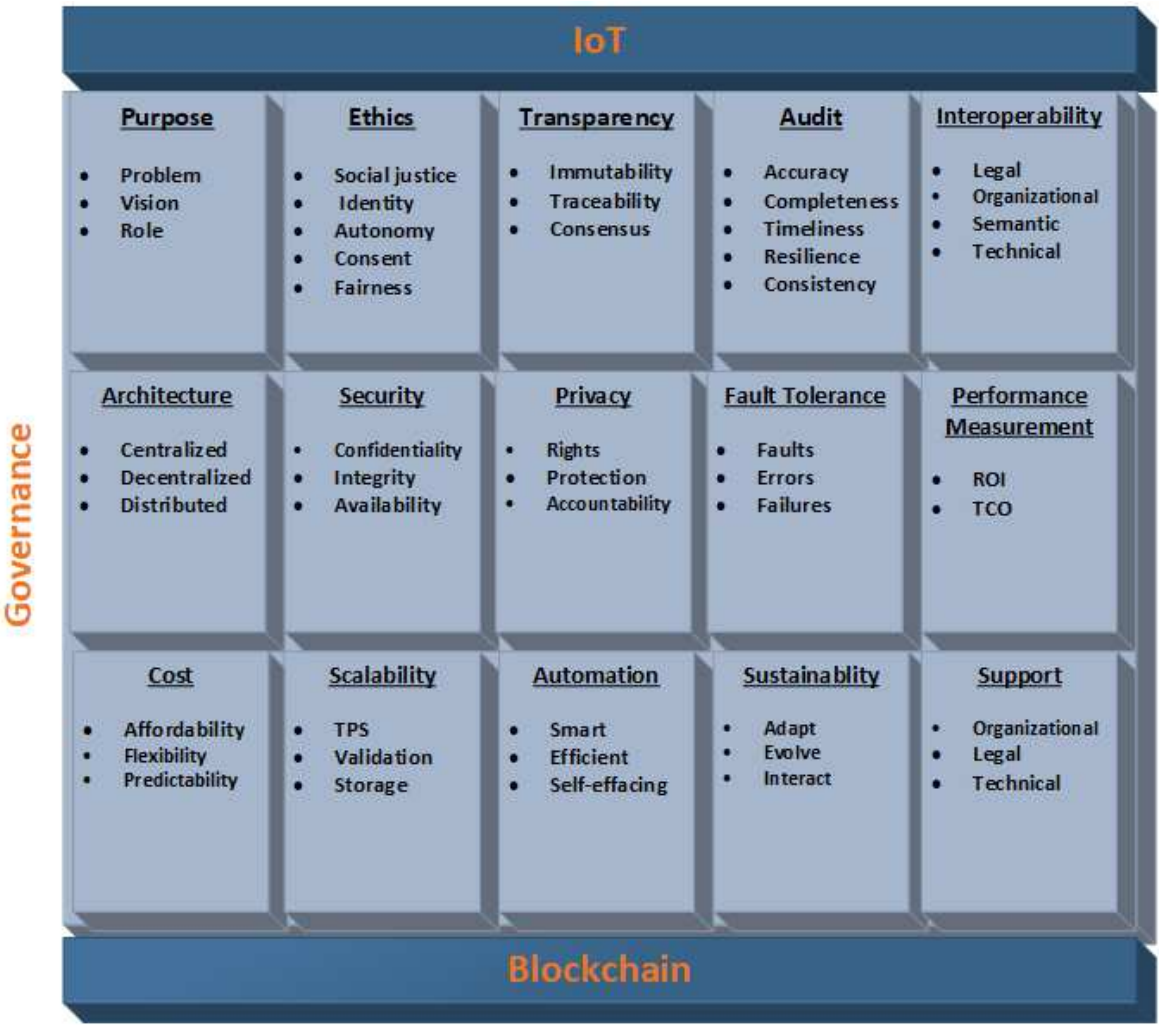

Figure 9. Framework. Governance specifies: How roles are assigned, how updates are executed,

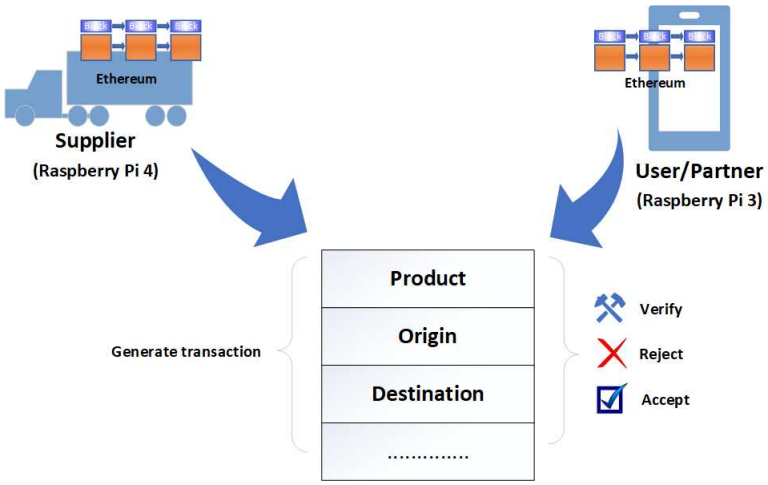

Figure 10. Transaction execution in blockchain-enabled smart logistics

6.2. Proposed governance framework evaluation

In this section we demonstrate the feasibility of the proposed framework by applying it to the smart logistics use case mentioned earlier. In order to accomplish the requirements of the smart logistics use case mentioned earlier, we proposed a blockchain based architecture for smart logistics as shown in

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

the Figure 7 and apply the proposed governance framework. For the purpose of simplicity and clarity we will follow two layers (on-chain and off-chain) governance to decide and implement the proposed framework requirements. Blockchain technology has the technical capabilities of providing innovative, transparent, and distributed smart logistics services. Based on the proposed framework, the partners initially identify the problems of smart logistics that can be solved with blockchain. Furthermore, policies are defined regarding vision of the consortium where objectives of each and every partner is guaranteed. Prior to developing smart logistics services, the concerned stakeholders are required to be consulted and perceive their concerns. And based on the vision, roles, and responsibilities are assigned to each partners. In smart logistics use case, the vision can be to provide innovative services and increase profit. Roles might include smart logistics partners, technical service providers, developers, national and international governmental bodies. Technical service providers can develop and maintain blockchain. Governamental bodies are responsible to ensure compliance to the national and international regulations. Innovative principles are included in order to promote investment and financial gains and then assign roles accordingly. Policies and frameworks are placed to ensure users' consent and the consortium functions as agreed. As per the proposed framework, developers, auditors, regulators, and stakeholders are instructed to ensure the solutions and services are developed according to ethical principles. In case of violation of users' ethical rights, the consequences should be straight for the accountability bodies to fairly impose them. During data collection and processing, implement transparent consent and users should have full control over their data. To avoid unnecessary delay, develop fast and efficient transaction mechanisms. Provide automated audit mechanisms where each partner can verify the ledger. Since, in blockchain technology each partner has copy of the ledger so through blockchain technology, it is possible to independently verify the ledger. Develop comprehensive policies to facilitate and maintain collaboration and cooperation across various partners, and to ensure interoperability among the partners at technical, legal, and as well as organizational level, which can attract more potential partners and consumers. The consortium has to implement novel security and privacy mechanisms and in order to fully avail the blockchain features, implement a distributed architecture. Distributed architecture has many applications such as security, transparency, trust, privacy, availability, and inbuilt capabilities of coping with errors and faults. Furthermore, adopt existing privacy preserving mechanisms and standards. The smart logistics consortium has to make fair and economical cost strategies that are beneficial to each and every partner. Furthermore, regularly evaluate services, users satisfaction and economical gains and then update services and strategies accordingly to attract and retain customers. So in conclusion following these requirements would transform traditional logistics into efficient and profitable smart logistics.

Table 2. Specifications of network devices.

Component	**Specifications (Raspberry Pi 4)**	**Specifications (Raspberry Pi 4)**
Model	Model B	Model B
Processor	Broadcom 2711, Cortex-A-72, 64-bit SoC @ 1.5 GHz	Broadcom 2711, quad-core Cortex-A72, 64-bit SoC @ 1.5GHz
Internal Working Memory (RAM)	4GB	8GB
SD card support	Micro SD card (operating system and data storage)	Micro SD card (operating system and data storage)
SD card size (capacity)	64GB	128GB
Connectivity	a) 2.4 GHz and 5 GHz IEEE 802.11.b/g/n/ac wireless LAN b) Bluetooth 5.0, BLE c) Gigabit Ethernet	a) 2.4 GHz and 5.0 GHz IEEE 802.11b/g/n/ac wireless LAN b) Bluetooth 5.0, BLE c) Gigabit Ethernet
Operating system	Raspbian	Raspbian

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

7. Conclusion

In this research, we proposed a governance framework for blockchain-enabled IoT applications that consists of various fundamental requirements. Furthermore, we demonstrated that most of these requirements can be achieved through blockchain technology thanks to the unique characteristics of blockchain technology and thus making IoT more secure and reliable. IoT generates tremendous amount of data and the growth of IoT leads to complexity in the architecture and eventually induce various security threats. Data processing methods are becoming more automated and smart to precisely learn and predict distinctive human behaviours. With the recent advancements in various industries, the products are becoming smart, efficient, and safe, however, the products are also becoming more intrusive. As per the European data protection jurisdiction, IoT that can be directly linked to a person - " wearable devices, quantified self (devices that track and record aspects of someone's life) and dobotics (devices with sensors used in home automation)" [10,11]. One of the main challenge is lack of dedicated governance mechanism. Without governance framework, any technology can potentially become dubious and intrusive. Compliance frameworks are applied in order to protect sensitive data, ensure accountability, etc. Governance includes policies, roles and implementation of the rule of law. Through governance and legal frameworks, it is possible to regulate both commercial and technical perspectives of the technology, facilitate further development, attract investors and improve collaboration and ultimately attain consumers' trust in the technology. Existing governance frameworks lack fundamental requirements of IoT and blockchain technology. There are large number of underlying governance challenges that need to be addressed. For instance, in IoT governance, the challenges are legitimacy, transparency, accountability [24] anti-competitive behaviour [17], varying organization size, heterogeneity [25], ethics, privacy, security, competitions [10], and encoding non-trivial disputes among the partners. As mentioned earlier, blockchain can be used to mitigate most of the IoT main challenges. For instance, unlike traditional logistics, smart logistic has brought much required ease in efficacy. However, smart logistic is far from being perfect and still smart logistics encounters many challenges. One potential approach to overcome smart logistics challenges is by adopting blockchain technology. Therefore, efforts are required to promote blockchain technology in IoT ecosystem. Blockchain allows transparent obligations to the agreements and transparent consensus mechanism to verify adherence to the governance. The proposed framework consists of 15 requirements of blockchain-enabled IoT ecosystem, each of these requirements is briefly studied, arguments are presented to highlight the importance of each requirement and mechanisms are mentioned regarding achieving these requirements. The mentioned requirements are aim to overcome the large number of challenges and aiming to make blockchain-IoT mainstream technology. Requirements are researched while keeping into consideration the economical, social, and environmental incentives and interests of each and every partner of the blockchain-IoT consortium. The proposed governance mechanism takes into consideration the need for a distributed ecosystem of IoT. Furthermore, variable geometry approach is proposed in implementing the requirements in order to promote flexibility in implementation of these requirements where partners are free to not opt to agreements that are not relevant to their interests. In the end, the framework is evaluated through a smart logistics use case.

8. Future Work

We discussed the requirements from a high level perspective regarding the challenges and improvements of each requirements. Future research is needed to further improve the proposed mechanism by analyzing each of these requirements more in dept and proposed absolute mechanisms to achieve these requirements and perform a survey where multiple companies could be involved to study the framework and provide recommendation regarding improving the requirements or adding new requirements.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

Author Contributions: Ikram Ullah researched, implemented, and tested the findings. Ikram Ullah together wrote the paper. Pual Havinga supervised this research.

Funding: This work has been partially supported by the EFRO, OP Oost program in the context of Countdown project.

References

1. A Conceptual Framework for Data Governance in IoT-enabled Digital IS Ecosystems. [Online]. Available: https://www.scitepress.org/Papers/2019/79243/79243.pdf
2. ISO/IEC 30141:2018(en) Internet of Things (loT) — Reference Architecture. [Online]. Available: https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:30141:ed-1:v1:en
3. Barnaby Lewis. ISO/IEC 27000 - Key international standard for information security revised. [Online] Available: https://www.iso.org/news/ref2266.html
4. ISO/IEC 27018:2019. Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. [Online] Available: https://www.iso.org/standard/76559.html
5. ISO/IEC 27017:2015. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. [Online] Available: https://www.iso.org/standard/43757.html
6. Royal Netherlands Standardization Institute. NEN Netherlands.[Online] Available: https://www.iso.org/member/2027.html
7. Ted Friedman , Saul Judah. Data Risks in the Internet of Things Demand Extensive Information Governance. 30 June 2016. [Online] Available: https://www.gartner.com/en/documents/3362117/data-risks-in-the-internet-of-things-demand-extensive-in
8. Anna Gerber, Satwik Kansal. Defining your IoT governance practices. August 7, 2017. [Online] Available : https://developer.ibm.com/technologies/iot/articles/iot-governance-01/
9. Jan Merkus. (2015). Data Governance Maturity Model. November 2015 DOI:10.13140/RG.2.2.19274.16321
10. V. A. F. Almeida, D. Doneda and M. Monteiro, "Governance Challenges for the Internet of Things," in IEEE Internet Computing, vol. 19, no. 4, pp. 56-59, July-Aug. 2015, doi: 10.1109/MIC.2015.86.
11. Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, tech. report, 16 Sept. 2014; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
12. A. Copie, T. Fortis, V. I. Munteanu and V. Negru, "From Cloud Governance to IoT Governance," 2013 27th International Conference on Advanced Information Networking and Applications Workshops, Barcelona, 2013, pp. 1229-1234, doi: 10.1109/WAINA.2013.169.
13. I. Ullah, N. Meratnia and P. J. M. Havinga, "Entropy as a Service: A Lightweight Random Number Generator for Decentralized IoT Applications," 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2020, pp. 1-6, doi: 10.1109/PerComWorkshops48775.2020.9156205.
14. Blockchain for Internet of Things: A Survey Hong-Ning Dai, Senior Member, IEEE, Zibin Zheng, Senior Member, IEEE, Yan Zhang, Senior Member, IEEE
15. G. D. Salazar Ch., C. Hervas, E. Estevez and L. Marrone, "High-Level IoT Governance Model Proposal for Digitized Ecosystems," 2019 International Conference on Information Systems and Software Technologies (ICI2ST), Quito, Ecuador, 2019, pp. 79-84, doi: 10.1109/ICI2ST.2019.00018.
16. I. Ullah, N. Meratnia and P. J. M. Havinga, "iMAC: Implicit Message Authentication Code for IoT Devices," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 2020, pp. 1-6, doi: 10.1109/WF-IoT48130.2020.9221331.
17. Rolf H. Weber, Internet of things – Governance quo vadis?, Computer Law & Security Review, Volume 29, Issue 4, 2013, Pages 341-347, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2013.05.010.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

18. Worldwide Governance Indicators. [Online] Available: accessed on 18-Jan-2021. https://datacatalog.worldbank.org/dataset/worldwide-governance-indicators
19. Château de Bossey. June 2005. Report of the Working Group on Internet Governance, June 2005, p. 4, Available online: http://www.wgig.org/docs/WGIGREPORT.pdf
20. Jeroen van den Hoven. European Commission, Internet of Things. Factsheet Ethics Version 4.0. [Online] Available: https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation
21. Anthony Furness. Internet of Things (IoT) European Research Cluster Activity Chain. International Framework for IoT Structure and Governance. (CASAGRAS2 Deliverable 4.1 – A Specification of rules and procedures for governance). 27-09-2011.
22. Harald T. Alvestrand. Internet Engineering Task Force (IETF – Mission statement – RFC3935, 2004). DOI: 10.17487/RFC3935. Available online: https://rfc-editor.org/rfc/rfc3935.txt
23. Wolfgang Kleinwachter. Final Report of the EU IOT Task Force on IOT Governance. Summary. Brussels, November 14, 2012. [Online] Available: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1748
24. M. Al-Ruithe, S. Mthunzi and E. Benkhelifa, "Data governance for security in IoT & cloud converged environments," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, 2016, pp. 1-8, doi: 10.1109/AICCSA.2016.7945737.
25. R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A Survey on Security Issues in Cloud Computing," Int. J. Innov. Technol. Explor. Eng., vol. 5, no. 6, pp. 83–87, 2011
26. R. Weber, "Governance of the Internet of Things— From Infancy to First Attempts of Implementation?," Laws, vol. 5, no. 3, p. 28, 2016. DOI:10.3390/laws5030028.
27. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Comput. Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
28. Q. Jing, A. V Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," Wirel. Networks, vol. 20, no. 8, pp. 2481–2501, 2014.
29. Announcing the Secure Hash Standard. Federal Information Processing Standards Publication 180-2 2002 [Online]. Available: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
30. C. Percival. Tarsnap—The Scrypt Key Derivation Function and Encryption Utility, accessed on Mar. 15, 2016. [Online]. Available: http://www.tarsnap.com/scrypt.html
31. J.-P. Aumasson, L. Henzen, W. Meier, and R. C. W. Phan. (Dec. 16, 2010). SHA-3 Proposal BLAKE. [Online]. Available: https://131002.net/ blake/blake.pdf
32. N. Szabo. (1994). Smart Contracts. [Online]. Available: http://szabo.best.vwh.net/smart.contracts.html
33. Michael Nofer, Peter Gomber, Oliver Hinz, Dirk Schiereck. Blockchain. Bus Inf Syst Eng 59(3):183–187 (2017). DOI 10.1007/s12599-017-0467-3
34. Z. Yan, P. Zhang, and A. V Vasilakos, "A survey on trust management for Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120–134, 2014.
35. A. Kazmi, M. Serrano and A. Lenis, "Smart Governance of Heterogeneous Internet of Things for Smart Cities," 2018 12th International Conference on Sensing Technology (ICST), Limerick, 2018, pp. 58-64, doi: 10.1109/ICSensT.2018.8603657.
36. Joint Task Force Transformation Initiative. SP 800-53 Rev. 4. April 2013 [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
37. Fabrice Lumineau, Wenqian Wang, Oliver Schilke. Blockchain Governance—A New Way of Organizing Collaborations? Organization Science. https://doi.org/10.1287/orsc.2020.1379
38. Sun, F. UTXO vs Account/Balance Model. Available online: https://medium.com/@sunflora98/utxo-vs-account-balance-model-5e6470f4e0cf (accessed on 9 August 2018)
39. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. Special section on the Plethora of research in Internet of Things (IoT). 2016 doi: 10.1109/ACCESS.2016.2566339.
40. Cole R, Stevenson M, Aitken J (2019) Blockchain technology: Implications for operations and supply chain management. Supply Chain Management 24(4):469–483. DOI:10.1108/SCM-09-2018-0309
41. CBInsights (2020) Investment to blockchain startups slips in 2019. Accessed March 25, 2020, https://www.cbinsights.com/research/ blockchain-investment-trends-2019/.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

42. Kim H, Laskowski M (2017) A perspective on blockchain smart contracts: Reducing uncertainty and complexity in value exchange. Poellabauer C, Abdelzaher T, Shen H, eds. Proc. 26th Internat. Conf. Computer Communication Networks 2017 (Institute of Electrical and Electronics Engineers, MA), 1–6
43. IBM (2018a) AIG, IBM, Standard Chartered deliver first multinational insurance policy powered by blockchain. Accessed March 25, 2020, https://www-03.ibm.com/press/us/en/pressrelease/52607.wss.
44. Nayak N, Nguyen DT (2018) Blockchain, AI and robotics: How future tech will simplify federal procurement. Accessed March 25, 2020, https://www.federaltimes.com/acquisition/2018/03/23/blockchain-ai-and-robotics-how-future-tech-will-simplify-federal-procurement/.
45. Okhuysen GA, Bechky BA (2009) Coordination in organizations: An integrative perspective. Acad. Management Ann. 3(1):463–502. DOI: 10.5465/19416520903047533
46. Rowan van Pelt, Slinger Jansen, Djuri Baars & Sietse Overbeek (2021) Defining Blockchain Governance: A Framework for Analysis and Comparison, Information Systems Management, 38:1, 21-41, DOI: 10.1080/10580530.2020.1720046
47. Atzori, M. (2016). Blockchain technology and decentralized governance: Is the state still necessary? University College of London. doi:10.2139/ssrn.2709713
48. Tasca, P., & Tessone, C. (2018). Taxonomy of blockchain technologies. Principles of identification and classification (Unpublished manuscript). Retrieved from https://papers.ssrn.com/abstract=2977811
49. Zhao, L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 2 (28), 1–7. doi:10.1186/s40854-016-0049-2
50. Hacker, P. (2017). Corporate governance for complex cryptocurrencies? A framework for stability and decision making in blockchain-based organizations. In P. Hacker, I. Lianos, G. Dimitropoulos, & S. Eich (Eds.), Regulating blockchain: Techno-social and legal challenges (pp. 40–166). Oxford, UK: Oxford University Press.
51. Rennock, M., Cohn, A., & Butcher, J. (2018). Blockchain technology and regulatory investigations (Tech. Rep.). Steptoe Johnson LLP. Retrieved from https://www.steptoe.com/images/content/1/7/v2/171967/LIT-FebMar18-Feature-Blockchain.pdf
52. Swan, M. (2015). Blockchain: Blueprint for a new economy. Sebastopol, CA: O'Reilly. ISBN-13: 978-1491920497
53. Beck, R., Müller-Bloch, C., & Leslie King, J. (2018). Governance in the blockchain economy: A framework and research agenda. Journal of the Association for Information Systems, 19(10), 1020–1034. doi:10.17705/1jais
54. van Deventer, O., Brewster, C., & Everts, M. (2017). Governance and business models of blockchain technologies and networks (Tech. Rep. No. 776936). TNO. Retrieved from https://repository.tudelft.nl/view/tno/uuid:a593f6d3-6c67-4fb1-908b-4ac7662b9b7f
55. Ziolkowski, R., Parangi, G., Miscione, G., & Schwabe, G. (2019, Januari). Examining gentle rivalry: Decisionmaking in blockchain systems. In T. Bui (Ed.), HICSS 2019. Proceedings of the 52nd Annual Hawaii international conference on system science (pp. 1–10). AISeL.
56. Finck, M. (2019). Blockchain governance. In Blockchain regulation and governance in Europe (pp. 182–209). Elcograf, GB: Cambridge University Press.
57. Governance of and with Blockchain. a thematic report prepared by the European Union Blockchain observatory & forum. Available at : https://www.eublockchainforum.eu/sites/default/files/reports/report_governance_v1.0_0.pdf
58. Justin Sun Bought Steemit. Steem Moved to Limit His Power, CoinDesk, 24 February 2020, and Inside the Crypto World's Biggest Scandal, Wired Magazine, 19 June 2018.
59. Ziolkowski, Rafael; Parangi, Geetha; Miscione, Gianluca; Schwabe, Gerhard (2019). Examining Gentle Rivalry: Decision-Making in Blockchain Systems. In: 52nd Hawaii International Conference on System Sciences (HICSS 2019), Maui, Hawaii, 8 January 2019 - 13 January 2019.
60. G. W. Peters and E. Panayi, "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," arXiv:1511.05740 [cs], Nov. 2015.
61. F. Fukuyama, "What Is Governance?," Governance, vol. 26, no. 3, pp. 347–368, Jul. 2013. https://doi.org/10.1111/gove.12035

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

62. O. E. Williamson, "Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 1496220, 1975.
63. W. W. Powell, "NEITHER MARKET NOR HIERARCHY," Research in Organizational Behavior, vol. 12, pp. 295–336, 1990.
64. Van der Elst, Christoph & Lafarre, Anne. (2019). Blockchain and Smart Contracting for the Shareholder Community. European Business Organization Law Review. 20. 10.1007/s40804-019-00136-0.
65. Directive (EU) 2017/828 of the European Parliament and of the Council of 17 May 2017 amending Directive 2007/36/EC as regards the encouragement of long-term shareholder engagement [2017] OJ L132/60.
66. Arizona Revised Statutes Title 44 - Trade and Commerce § 44-7061 Signatures and records secured through blockchain technology; smart contracts; ownership of information; definitions (2017). [Online] Available: https://law.justia.com/codes/arizona/2017/title-44/section-44-7061/
67. Blockchain enabling - Vermont Laws. 12 V.S.A. § 1913 (2017). [Online] Available: https://legislature.vermont.gov/statutes/section /12/081/01913.
68. Esposito De Falco, Salvatore & Cucari, Nicola & Canuti, Emanuele & Modena, Stefano. (2019). Corporate governance and blockchain: Some preliminary results by a survey. 10.22495/cpr19p3.
69. Qi, Renming & Feng, Chen & Liu, Zheng & Mrad, Nezih. (2017). Blockchain-Powered Internet of Things, E-Governance and E-Democracy. 10.1007/978-981-10-4035-1_17.
70. K. PHANSE. Data governance using SAP MDM - part 1., (2008). [Online] Available: https://archive.sap.com/kmuuid2/60022998-5d17-2b10-dbaa-8e3ab357fa55/Data%20Governance%20using%20SAP%20Mast\er%20Data%20Management%20-%20Part%201.pdf
71. Jan Kooiman (1999) Social-Political Governance, Public Management: An International Journal of Research and Theory, 1:1, 67-92, DOI: 10.1080/14719037800000005
72. General Data Protection Regulation (GDPR). 2018 [Online] Available: https://gdpr-info.eu/
73. Kate O'Flaherty. Marriott Faces $123 Million Fine For 2018 Mega-Breach. 2019. [Online] Available: https://www.forbes.com/sites /kateoflahertyuk/2019/07/09/mar riott-faces-gdpr-fine-of-123-million/
74. ISO/IEC 30141:2018(en) Internet of Things (IoT) — Reference Architecture. [Online] Available: https://www.iso.org/obp/ui/#iso :std:iso-iec:30141:ed-1:v1:en
75. Clare Naden. Reference framework for the Internet of things. 2018. [Online] Available: https://www.iso.org/news/ref2340.html
76. Zhu, Liehuang & Gai, Keke & Li, Meng. (2019). Blockchain Technology in Internet of Things. 10.1007/978-3-030-21766-2.
77. Nallapaneni Manoj Kumar, Pradeep Kumar Mallick, The Internet of Things: Insights into the building blocks, component interactions, and architecture layers, Procedia Computer Science, Volume 132, 2018, Pages 109-117, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.05.170.
78. Burhan, Muhammad & Rehman, Rana Asif & Kim, Byung-Seo & Khan, Bilal. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors. 18. 10.3390/s18092796.
79. Jennifer J. Xu Xu Financial Innovation (2016) 2:25. Are blockchains immune to all malicious attacks? DOI 10.1186/S40854-016-0046-5
80. Ullah I, de Roode G, Meratnia N, Havinga P. Threat Modeling—How to Visualize Attacks on IOTA? Sensors. 2021; 21(5):1834. https://doi.org/10.3390/s21051834
81. M. A. Brady, I. Ullah and P. J. M. Havinga, "DOSing Distributed Ledger Technology: IOTA," 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), 2021, pp. 55-61, doi: 10.1109/CSP51677.2021.9357600.
82. Atlam, Hany & Wills, Gary. (2019). IoT Security, Privacy, Safety and Ethics. DOI: 10.1007/978-3-030-18732-3_8. Digital Twin Technologies and Smart Cities (pp.1-27)Publisher: Springer Nature Switzerland

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

83. Tim Swanson (2015) Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. [Online] Available: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf
84. Zyskind G, Nathan O, Pentland A (2015) Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), IEEE 180–184
85. Blostein, Alexander and I. Groer. "Profiles in Innovation: Blockchain: Putting Theory into Practice." (2016).
86. Yaga, Dylan and Mell, Peter and Roby, Nik and Scarfone, Karen. Blockchain technology overview. National Institute of Standards and Technology. 2018. http://dx.doi.org/10.6028/NIST.IR.8202
87. Mell, P., Kelsey, J., and Shook, J., "Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness." October 7, 2017. https://doi.org/10.1007/978-3-319-69084-1_31
88. Skh Saad, S. M., & Raja Mohd Radzi, R. Z. (2020). Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (POS) and Delegated Proof of Stake (DPOS). International Journal of Innovative Computing, 10(2). https://doi.org/10.11113/ijic.v10n2.272
89. Chen L., Xu L., Shah N., Gao Z., Lu Y., Shi W. (2017) On Security Analysis of Proof-of-Elapsed-Time (PoET). In: Spirakis P., Tsigas P. (eds) Stabilization, Safety, and Security of Distributed Systems. SSS 2017. Lecture Notes in Computer Science, vol 10616. Springer, Cham. https://doi.org/10.1007/978-3-319-69084-1_19
90. Changqiang Zhang, Cangshuai Wu, and Xinyi Wang. 2020. Overview of Blockchain Consensus Mechanism. In Proceedings of the 2020 2nd International Conference on Big Data Engineering (BDE 2020). Association for Computing Machinery, New York, NY, USA, 7–12. DOI:https://doi.org/10.1145/3404512.3404522
91. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260
92. XRP: The Best Digital Asset for Global Payments. [Online] Available: https://ripple.com/xrp/
93. Quorum Whitepaper v0.1.pdf. [Online] Available: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf
94. Tezos. [Online] Available: https://www.tezos.com/
95. H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi and A. Rindos, "Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)," 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 2017, pp. 253-255, doi: 10.1109/SRDS.2017.36.
96. Hyperledger. [Online] Available: https://www.hyperledger.org/
97. The Ethereum Virtual Machine. [Online] Available: https://fullstacks.org/materials/ethereumbook/14_evm.html
98. Azure IoT. [Online] Available: https://azure.microsoft.com/en-us/overview/iot/
99. Watson IoT Platform. [Online] Available: https://www.ibm.com/cloud/watson-iot-platform
100. Xively. [Online] Available: https://xively.com/
101. IoTivity. [Online] Available: https://iotivity.org/
102. Thingsquare. [Online] Available: https://www.thingsquare.com/
103. Lloyd, Peter. (2008). The Variable Geometry Approach to International Economic Integration. Seventh APEF Conference, Iran, 3-5 November 2008. University of Melbourne
104. Bigchaindb. [Online] Available: https://www.bigchaindb.com
105. Cornford, A. (2004), "Variable Geometry for the WTO: Concept and precedents", UNCTAD Discussion Papers No. 171, May 2004.
106. Multichain. [Online] Available: https://www.multichain.com
107. Corda. [Online] Available: https://www.corda.net
108. What is personal data? [Online] Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
109. What personal data is considered sensitive? [Online] Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform\/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
110. Directive 95/46/EC of the European Parliament and of the Council. (1995). [Online] Available: https://eur-lex.europa.eu/eli/dir /1995/46/oj
111. Directive 2009/136/EC of the European Parliament and of the Council. (2009). [Online] Available: https://eur-lex.europa.eu/eli/dir/2009/136/oj

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

112. Why data privacy is much more than compliance. Build trust to help grow your business. [Online] Available: https://www.ibm.com /security/digital-assets/data-privacy-matters/
113. Sunil Bakshi. Performance Measurement Metrics for IT Governance.1 November 2016 https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/performance-measurement-metrics-for-it-governance
114. Wim Van Grembergen and Steven De Haes. Measuring and Improving IT Governance Through the Balanced Scorecard. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.469. 7541&rep=rep1&type=pdf
115. Ethereum. [Online] Available: https://ethereum.org/
116. Sridhar Balasubramanian, Shantanu Bhattacharya, Vish V. Krishnan (2015) Pricing Information Goods: A Strategic Analysis of the Selling and Pay-per-Use Mechanisms. Marketing Science 34(2):218-234. https://doi.org/10.1287/mksc.2014.0894
117. Fishburn, P., Odlyzko, A. Competitive pricing of information goods: Subscription pricing versus pay-per-use. Economic Theory 13, 447–470 (1999). https://doi.org/10.1007/s001990050264
118. Maria A. Wimmer, Rositsa Boneva, and Debora di Giacomo. 2018. Interoperability governance: a definition and insights from case studies in Europe. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (dg.o '18). Association for Computing Machinery, New York, NY, USA, Article 14, 1–11. DOI:https://doi.org/10.1145/3209281.3209306
119. Hashgraph. [Online] Available: https://www.hedera.com/
120. de Haro-Olmo, F.; Varela-Vaca, Á.; Álvarez-Bermejo, J. Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. Sensors 2020, 20(24), 7171; https://doi.org/10.3390/s20247171. https://www.mdpi.com/1424-8220/20/24/7171
121. IOTA. [Online] Available: https://www.iota.org/
122. J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno and A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges," in IEEE Access, vol. 7, pp. 164908-164940, 2019, doi: 10.1109/ACCESS.2019.2950872.
123. Sumit Jain. Fault tolerance in distributed systems. Distributed systems (CSE-510). Lecture notes. 2014
124. Storm C. (2012) Fault Tolerance in Distributed Computing. In: Specification and Analytical Evaluation of Heterogeneous Dynamic Quorum-Based Data Replication Schemes. Vieweg+Teubner Verlag. https://doi.org/10.1007/978-3-8348-2381-6_2
125. R3. [Online] Available: https://www.r3.com/
126. Clifford H. Farrach, Logan Pettinato. The role of fault tolerance for blockchain. The beacon group technology practice. [Online] Available: https://static1.squarespace.com/static/59b80e154c0dbfd18f2fe92 d/t/5bae720ff4e1fc4c51de81c5/1538159124018/The+Role+of+ Fault+Tolerance+for+Blockchain.pdf
127. S. S. Hazari and Q. H. Mahmoud, "A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0916-0921, doi: 10.1109/CCWC.2019.8666535
128. "How Visa Protects Your Data". Fast Company, 2018. Available: https://www.fastcompany.com/1784751/how-visa-protects-your-data. Accessed 3 Nov 2018.
129. Boyen, Xavier, Christopher Carr, and Thomas Haines. "Blockchain-Free Cryptocurrencies. A Rational Framework for Truly Decentralised Fast Transactions." IACR Cryptology ePrint Archive 2016 (2016): 871.
130. Pau Giro Manzano. Customer Satisfaction Measurement: strategies, methodologies and factors influencing customer satisfaction measures. June 2021. Universitat Oberta de Catalunya (UOC). http://hdl.handle.net/10609/131866
131. Joel.Paula@oecd.org; Timothy.Bishop@oecd.org Blockchain Technologies as a Digital Enabler for Sustainable Infrastructure. Available at: https://www.oecd.org/finance/Blockchain-technologies-as-a-digital-enabler-for-sustainable-infrastructure-key-findings.pdf
132. Leonardo, Rana & Giungato, Pasquale & Tarabella, Angela & Tricase, Caterina. (2019). Blockchain Applications and Sustainability Issues. www.amfiteatrueconomic.ro. 21. 861. 10.24818/EA/2019/S13/861.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 October 2023 doi:10.20944/preprints202310.0375.v1

133. Christophe Schinckus. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. Energy Research & Social Science, Volume 69, 2020, 101614, ISSN 2214-6296, https://doi.org/10.1016/j.erss.2020.101614.
134. A. Shoker, "Sustainable blockchain through proof of exercise," 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), 2017, pp. 1-9, doi: 10.1109/NCA.2017.8171383.
135. Solidity by Example. Voting. [Online] Available: https://docs.soliditylang.org/en/v0.4.11/solidity-by-example.html

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.