A survey on blockchain for intelligent governmental applications

Ibrahim Ramadan Abdelhamid[1], Islam Tharwat Abdel Halim[2,3], Abd El-Majeed Amin Ali[1], Ibrahim Abdelmoniem Ibrahim[1]
[1]Faculty of Computers and Information, Minia University, Minia, Egypt
[2]School of Information Technology and Computer Science (ITCS), Nile University (NU), Giza, Egypt
[3]Center for Informatics Science (CIS), Nile University, Sheikh Zayed City, Egypt

Article Info

Article history:

Received Jan 27, 2023
Revised Mar 23, 2023
Accepted Mar 24, 2023

Keywords:

Cryptocurrency
Digital transformation
E-government
Encryption
Ethereum
Public sector

ABSTRACT

Blockchain technology has attracted a lot of attention lately because it is seen as an all-purpose method for conducting online transactions between unidentified parties without the need for a centralized authority. Modern developers and businesspeople think it will disrupt or even change both the government and industry. In this setting, government-focused blockchains are becoming increasingly prevalent. Several recent studies highlighted use cases in the public sector for decentralized information infrastructures. Blockchain is expected to revolutionize or at least simplify many governmental functions. However, because blockchain use has yet to be widely adopted in government or industrial settings, the question arises: what are the technical hurdles impeding blockchain adoption? To that purpose, a systematic literature assessment of 29 academic articles investigating software engineering problems in blockchain technology for government applications has been done. The papers are initially inductively analyzed in order to illustrate and identify the issues frequently highlighted in academic literature. Furthermore, a theoretical framework is discussed by relying on models used in traditional software development, which is then followed by deductive analysis to map out the blockchain use cases and future trends connected to the difficulties.

Corresponding Author:

Ibrahim Ramadan Abdelhamid
Faculty of Computers and Information, Minia University
Minia, Egypt
Email: Ibrahim.ramadan2207@gmail.com

1. INTRODUCTION

The development of information technology (IT) has made it possible for governments to provide services to citizens more directly, a practice known as "digitalized-government", which is defined as "the use of information and communication technologies, notably the internet, as a tool to accomplish better governance" [1]. The notion of digitalized government arose from the desire for governments to save costs and improve their efficacy. Nowadays, an efficient government and a competitive society are both understood to depend on successful e-governance [2]. Politicians, government agencies, private businesses, and civil society organizations are the three main stakeholder groups that are connected through e-government [3]. Traditionally, e-government initiatives have focused on one of the three aspects that connect these groups: e-service, digitalized administration, or e-democracy. Today, governments keep track of citizens and states, assist in electronic voting, facilitate economic transactions, regulate markets, combat tax evasion, and redistribute public funds like grants.

In the sphere of e-government, new technology has evolved that offers up a world of opportunities [4]. With the use of this technology, governments can interact with residents, businesspeople, and other entities in entirely new ways [5]. It merges existing technologies into a new information architecture. The fundamental promise of this technology is that it will allow for direct communication between people, which will enable administration without the need for a government administrator and personalise government services. This opens up the possibility of reconsidering society's present institutions. Blockchain is the technology that is powering this change.

Blockchain is a mechanism that enables peer-to-peer (P2P) networks to spread the registration of digital assets and associated transactions. Encryption is used in blockchain technology to make it difficult to modify earlier transactions. A "consensus mechanism," a system that enables users in the P2P network to confirm transactions and update the registry across the entire network, is used by the network to verify a transaction. The name "blockchain" refers to an immutable chain of blocks that holds the transaction data. When a transaction is validated, its data is locked into a block of data that is linked to the block that was previously validated. This technology has the potential to change how governments interact with citizens, business owners, and other stakeholders because it fundamentally varies from existing information registration and sharing infrastructures [5].

In order to maintain data integrity and prevent fraud, society has historically established a plethora of intermediaries, such as banks, to act as a centralized authority keeping track of all transactions. Digital assets can only be sent once, and blockchain systems' transaction records are immutable [6]. Because of this, this technology has the potential to have a big effect on institutions as we know them now. It may change how people connect with one another and how economies function [7]. Because it enables decreased costs and complexity, shared trustworthy processes, increased discoverability of audit trials, and guaranteed trusted recordkeeping, blockchain technology has the potential to help governments and to be the next stage in the evolution of e-government. But the amount of material on the blockchain is really limited. A thorough analysis of the utility of blockchain technology for public administration operations is inadequate, and there is a dearth of literature on the use of blockchain technology for e-government.

By and large, the public sector's adoption of blockchain technology has been limited. This could be justified because of the lack of appropriate governance, regulation, interoperability, and inefficient support for governmental blockchain-based applications. Furthermore, knowing what to regulate and how to govern is necessary for the use of blockchain in the public sector. As a result, it is crucial to look at how blockchain may affect public governance, as this is one of the biggest obstacles to the adoption of public blockchain. For instance, in this context, the European Union is looking at the potential benefits of blockchain technology for its services and operations [8]–[11]. By enabling services to be distributed at the lowest level of government and fostering a wider exchange of information between individuals and business operators, blockchain aids the EU in realising its subsidiary concept. However, due to the multi-actor complexity of blockchain technology, EU Institutions and Bodies make unstructured decisions about blockchain experimentation, which leads to a proliferation of blockchain trials that don't add much value. Additionally, different political players' motivations lead to differences in perceptions of blockchain in the EU. The decision-making processes used by international institutions and bodies need to be improved if blockchain technology is to live up to its potential.

Numerous informational gaps are the root cause of this unstructured decision-making. First, it's not apparent how blockchain technology interferes with how governments function. The second issue is that governmental blockchain applications' technological and multi-actor complexity is not well understood, which could have unintended repercussions. Thirdly, there is a paucity of knowledge regarding how blockchain technology fits into governmental operations and the socio-technical effects that government blockchain deployments can have. Finally, despite the fact that both the kind of blockchain and the consensus procedure have an impact on system performance, blockchain is commonly viewed as a one-size-fits-all solution. It is necessary to do research that explains the benefits of blockchain for governments and enables structural evaluation of how well information exchange or registration processes match with blockchain.

Therefore, in order to improve decision-making in international institutions and bodies debating the merits of experimenting with blockchain technology to improve their information-sharing or registration procedures, we invested our time and effort into conducting a thorough survey and analysis on blockchain technology for government applications and its opportunities, limitations, and issues. We start by selecting keywords like blockchain, government, and public sector and using them to look up articles and information online. Then, we examine government-related blockchain articles that have been published in renowned digital scientific libraries, such as ScienceDirect, IEEE Xplore, and Springer. Consequently, we examined as many publications as possible in order to avoid research and outcome biases. Our survey study summarizes the conclusions of several studies. The following are our survey's primary contributions: i) we provide a thorough background and understanding of blockchain technology; ii) we present rich information about ongoing projects and initiatives for blockchain-based governmental applications; and iii) we conduct an extensive analysis on different public sectors, domains, technologies, and issues for blockchain-based governmental applications; and in order to prepare for future attempts to develop blockchain technology for extensive deployments in the public and government sectors, the difficulties and research trends are compiled and presented in this paper.

The remainder of the paper is structured as shown in: the problem definition and study technique are described in section 2. A history and literature review, as well as any associated projects or initiatives, are provided in sections 3 and 4, respectively. Section 5 provides the results and discussion of this work. Finally, section 6 summarises the conclusions.

2. METHOD

We reviewed the literature, current projects, and use cases that utilize blockchain technology and are supported by governments worldwide [12]–[16]. Our goal is to discuss several representative and meaningful applications. Overall, a wide range of businesses stand to gain from the increased interest in blockchain technology. However, a lot of them are useless or impractical. Determining the trend in government use cases is the primary goal of this effort. Opinions from regulators, consumers, and developers on the deployment of government blockchain. A state might wish to keep an eye on how blockchains are used, just like with cryptocurrencies. Blockchains can be used by governments to streamline procedures. For internal business needs, a government may potentially develop its own blockchain-based application. It is critical to look into the effects of different blockchain governance architectural choices on the public sector in order to synthesis the existing conceptual approaches towards blockchain governance across domains. in particular, as shown in: i) what governance choices are necessary to build a public blockchain system?; and ii) how do contextual factors related to the public sector affect the blockchain governance options?

We followed Kitchenham and Charters' guidelines when doing the systematic literature review (SLR) [17] guidelines, in order to fulfill the study objective. To allow a full evaluation of the SLR, we cycled through the study's planning, execution, and publication processes.

2.1. Selection of primary studies

Primary research was highlighted by submitting keywords to a specific publication's or search engine's search feature. The keywords were chosen to promote the appearance of study findings that would assist in addressing the research questions. ("Document Title": blockchain) AND ("All Metadata": government) were the query phrases. We looked at platforms like IEEE Xplore, ScienceDirect, and SpringerLink. The title, keywords, or abstract were utilized in the searches, depending on the search platforms. We completed the searches and processed all papers issued up to that moment on November 7, 2022. The results of these searches were filtered using the criteria for inclusion and exclusion listed in section 2.2. We were able to compile a set of findings using the criterion, which we then put into Wohlin's snowballing process [18]. Iterations of snowballing were done both forward and backward until no further papers meeting the inclusion criteria could be discovered.

2.2. Criteria for inclusion and exclusion

By utilizing a broad definition of blockchain and government, we were able to include articles on Ethereum, cyber security, cryptocurrencies, crypto transactions, systematic literature reviews, distributed ledgers, the internet of things, and other subjects. Abstracts, article names, and keywords were evaluated for inclusion. Where necessary, the articles' main texts underwent a thorough examination. Peer-reviewed studies that detail the use of the technology being discussed, as well as those that have appeared in a journal or conference proceedings, will be considered. Studies that rely on business, finance, or other unrelated topics are disregarded. Additionally, the studies are only available in English.

2.3. Result of selection

There were 1084 records found in the initial phase (310 from Springer, 106 from Science Direct, and 668 from IEEE Xplore). The number of literary works was decreased to 148 articles maintained for further title reading after the removal of literary works like grey literature, extended abstracts, presentations, keynotes, book chapters, non-English language papers, and inaccessible publications. Only 41 more publications met the requirements for additional abstract reading after that. There were only 34 papers left to be read in their entirety after reading the abstracts. 29 of them eventually studied blockchain for government applications after snowballing, and those articles were downloaded for further inspection.

3. BACKGROUND

All blockchains use cryptography and an underlying consensus mechanism to help decentralised nodes agree on the overall order of transactions. Technically, blockchains can be classified as permissioned or permissionless. Permissionless blockchains are considered "open" and rely on algorithms for trust. Anyone can join them. On the other hand, permissioned blockchains are frequently "private" or "consortium," where everyone is known for who they are and no one needs to be believed. In some cases, it can be challenging to tell one blockchain type from another in real life. For instance, using the Ethereum private network, the permissionless cryptocurrency Ethereum can be configured to operate as a private blockchain [19]. For permissioned blockchains, anonymity has also been desired [20]. To ensure that decentralised nodes agree on the overall transactional order, all blockchains use cryptography techniques and consensus processes. The two primary forms of blockchains are permissioned and permissionless. Blockchains with no permissions are "open" and rely on algorithms to build trust. In a permissioned blockchain, all participants are known, but none of them need to be trusted. There are instances where it is difficult to distinguish between different blockchains in practise. An Ethereum private network, for instance, can be set up on Ethereum, a permissionless blockchain. [8]. It has also been attempted to anonymize permissioned blockchains [9].

Figure 1 illustrates how three layers can be separated from blockchains [10]. Layer 1: The Byzantine fault-tolerant (BFT) consensus (also known as state machine replication) is a general method for tolerating errors. BFT consensus is exemplified by conventional BFT protocols and proof of work (PoW)-based agreements. Any form must address the same issue: how to allow nodes to agree on the overall consistency (i.e., order) of transactions that clients submit as requests. The data/operations of the transactions are handled in the sequence that nodes agree upon after reaching an agreement. Spread nodes therefore act like a single centralised node. As a result, there will only be one client transaction chain. The blockchain's second layer is the smart contract. For blockchain developers, a smart contract is a mechanism to add. The way blockchain developers can include new functionality is through smart contracts. Then, by validating or enforcing transactions, smart contracts can aid in transaction execution. A software that connects consensus protocols, applications, and uses is known as a smart contract.

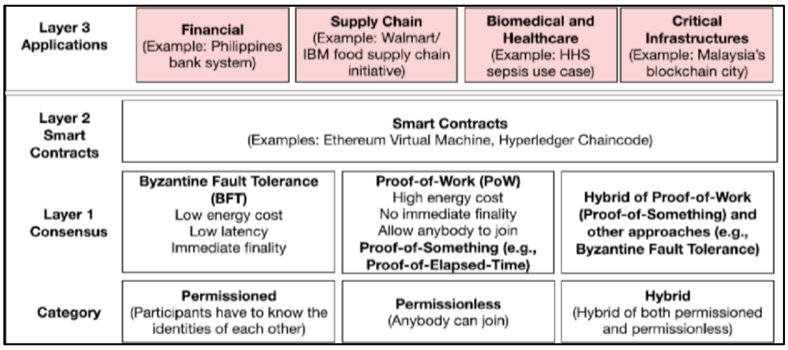
Layer 3 Applications
Financial (Example: Philippines bank system)
Supply Chain (Example: Walmart/ IBM food supply chain initiative)
Biomedical and Healthcare (Example: HHS sepsis use case)
Critical Infrastructures (Example: Malaysia's blockchain city)
Layer 2 Smart Contracts
Smart Contracts (Examples: Ethereum Virtual Machine, Hyperledger Chaincode)
Layer 1 Consensus
Byzantine Fault Tolerance (BFT) Low energy cost Low latency Immediate finality
Proof-of-Work (PoW) High energy cost No immediate finality Allow anybody to join Proof-of-Something (e.g., Proof-of-Elapsed-Time)
Hybrid of Proof-of-Work (Proof-of-Something) and other approaches (e.g., Byzantine Fault Tolerance)
Category
Permissioned (Participants have to know the identities of each other)
Permissionless (Anybody can join)
Hybrid (Hybrid of both permissioned and permissionless)

Figure 1. Overview of blockchains: categories, underlying techniques, and use cases [16]

The distributed ledger technology (DLT) known as blockchain gives users the confidence that their data has not been altered [21]. The major distinction between blockchain and DLT is that the latter uses consensus procedures and sequential information registries in a chain-like structure to generate trust, whereas the former uses a technology for maintaining a distributed database. According to theory, blockchain could make it possible to do away with middlemen in public administration like trustees and replace them with an algorithmic confidence system [22]. Blockchain governance in the public sector is conflicting and complex because of this technological aspect of the technology. In this regard, the literature presents two opposed points of view. According to the first argument, blockchain technology makes it possible to authenticate information with data openness, integrity, and traceability while also reducing transaction costs and increasing the effectiveness of public services [23]. The second perspective views blockchain as a transformative technology that makes it possible for permissionless transactions to take place in a truly decentralised manner, eliminating the need for a central authority to coordinate, mitigate, or manage public services [5] and eliminating the government's position as primus inter pares [24] in the public sector.

Blockchain as a technology, then, re-establishes the significance of legitimacy and confidence during the policy and system design process, rather than during implementation, adding a layer of complexity. Whether a blockchain is permissioned or permissionless, the rules for transactions are decided upon during the design phase. Therefore, the fact that blockchain as a technology reinstates the significance of trust and legitimacy during the policy and system design process, rather than during implementation, adds another level of complexity. What are the rules and procedures to follow in the system update once a choice has been made? Permissioned and permissionless blockchains both have transaction rules established during the design process. These are significant governance factors for blockchain-based systems. Vili Lehdonvirta refers to these inherent contradictions of blockchain governance as the "governance paradox" because once you address these governance problems, blockchain loses its value over traditional technologies and means where a trusted central party enforces the rules [25]. This is because you are already trusting some organisation or process to make the rules. The system requires authorised users to approve requests. Additionally, while blockchains can validate the legitimacy of a transaction, they cannot assess the veracity of a given input or the fairness of the transaction rules. The question of "who will be authorised to make changes in the system?" and "what are the rules/procedures to follow in the system update" are therefore important governance issues for blockchain-based systems.

Additionally, the theoretical underpinnings of what blockchain governance implies as well as the important choices connected with it appear to vary between fields. For instance, blockchain governance in the context of information and computer science frequently focuses on how decision rights, incentives, and accountabilities are set up in a blockchain network to promote positive resource use behaviour [26]. In particular, the best rules for affirmative incentives and cryptographically enforced constraints on a particular action in public permissionless blockchains are found using game-theoretical methods. From the standpoint of corporate management, blockchain governance is described as the procedures through which individuals and groups with long-standing ties negotiate how to respond to changes in an institutional setting [27]. In this literature, governance choices are usually analysed through theoretical corporate governance lenses. In the economics literature, blockchain governance is compared to community-pool resource governance and is related with polycentric systems operating concurrently at multiple levels of interaction [28]. A thorough conceptual framework of blockchain governance is required to accommodate the various theoretical approaches in the literature, according to this non-exhaustive review of theoretical approaches to blockchain governance. Additionally, researchers should think about how a particular context and research focus affect policy decisions related to blockchain governance. Therefore, the basic pillar of the framework described in this study is an independent blockchain infrastructure composed of independent nodes hosting multiple public and private applications. The proposed concept adds a governance layer "on top" of blockchains with permissions.

3.1. Authorized blockchains

Consensus and security are provided via distributed consensus methods that may be proved to be secure in permissioned blockchains. The use of expensive techniques, such as those employed in proof-of-work, is not necessary for the consensus protocols (POW). Because of this, permissioned systems are more energy-efficient than permissionless blockchains (which are discussed in more detail later), have low latency (the amount of time it takes for a client to send a transaction and receive a response), and are scalable (both in terms of the number of clients and transactions as well as the number of servers) [29]. Provably secure BFT protocols are employed by the majority of permissioned blockchains, especially those that are operated or tested by governments.

Among these BFT systems, the leader-based protocols, such as practical-BFT (PBFT) [30] and its variations [31], are frequently employed. In these protocols, the sequence of the transactions is proposed by a particular leader. The nodes then engage in a series of interactions with one another to reach consensus on the order. In the majority of leader-based protocols, before moving on to the next step, each node sends messages to every other node in the step and gathers matching messages from a select few nodes. If the current leader is perhaps flawed or malevolent, other nodes will execute a leader change protocol until a new leader is elected.

In addition to consensus procedures, blockchains use a variety of techniques to store transactions. The basic system architecture of a permissioned blockchain is shown in Figure 2. A number of nodes employ the BFT protocol to assign orders to the transactions after receiving client requests. All other nodes in the system are then sent the transactions and their order. The final step is to store and process the transactions in the order that they were received. In this architecture, the nodes that store the transactions take on the role of learners by passively absorbing the order from the consensus nodes.

Several BFT techniques have been put out in the literature [32]–[34]. A node only needs to communicate with its previous node and, if relevant, its next node in chain-based techniques, avoiding the all-to-all communication previously discussed and resulting in speed advantages. Another choice is a hybrid strategy that mixes BFT protocols, as Aliph [34]. Because there isn't a consensus process that works for everyone, Aliph employs a hybrid strategy to integrate the best aspects of many BFT methods. In Aliph, the protocol can utilise a single low-cost protocol to provide excellent performance with fewer failures. When errors occur or become more frequent, the system moves to a more expensive system to ensure system security.

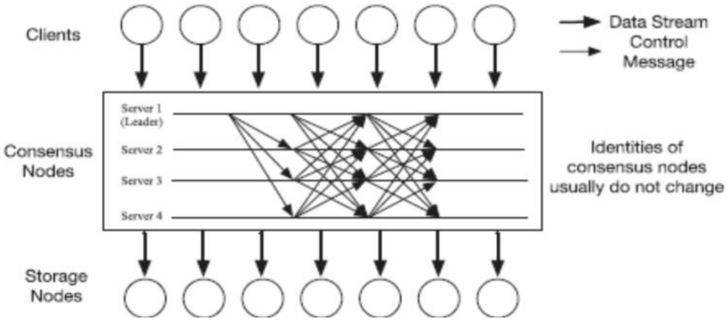

Figure 2. The normal operation for a permissioned blockchain running PBFT [16]

3.2. Unrestricted blockchains

The majority of permissionless blockchains employ the "Proof-of-Something" tactic. This is known as POW in the context of Bitcoin and is a mathematical difficulty that all nodes in the system must try to overcome (or work through) through the mining process. After a block of transactions has been mined, a node can propose it, and if it is approved, it will be paid in Bitcoin. This method's disadvantage is that it consumes a lot of energy and has a low throughput (number of transactions completed per second). Additionally, nodes create mining pools, cartel-like organisations that concentrate mining activities under the management of a single group. Mining pools make the blockchain less decentralised, less safe, and more open to assault and manipulation.

Contrary to BFT-based consensus, POW-based consensus lacks a constant leader and can be conceptualised as a system where the leader switches after every block of transactions. Before proposing a new transaction, a node must first solve the PoW from the prior transaction. A cryptographic nonce, a pseudorandom number, is also generated when a node proposes transaction n. As seen in Figure 3, the nonce is broadcast to all other nodes. Nodes fight to become the next leader by picking random pending transactions and creating a hash of the chosen transactions. The node that produces a hash that is less than the nonce value first is the winner. The subsequent leader is this node. Compared to BFT consensus, POW-based consensus requires less messages from nodes to reach a consensus on transactions. Tens of thousands of nodes can quickly be added to its blockchains. The issue is that the puzzle might be solved simultaneously by several nodes, which would lead to a fork in the hash chain. The POW consensus nodes will notice the fork and finally choose the longest hash chain to utilise. After a transaction has been submitted, it typically takes six blocks, each of which takes around 10 minutes, or roughly an hour in the case of Bitcoin, for the transaction to be completed. The task can be finished in less time using a variety of techniques.

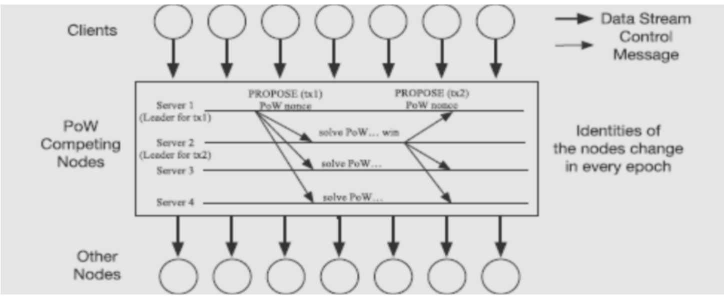

Figure 3. The message flow for PoW-based blockchains. Control messages are the messages for nodes to compete for PoW [16]

3.3. Advanced contracts

Without the need for human interaction, smart contracts are self-executing programmes that run when nodes come to an agreement. The contracts that most people are accustomed to are not the same as smart contracts. Instead, the nodes of a blockchain are configured to verify a set of conditions to see if the triggering circumstances have been satisfied. The nodes will execute a contract, which is a software that conducts tasks that have been defined by the business, if the conditions are satisfied. Users can add new features and functions to their blockchains using smart contracts without having to stop using their services. For instance, programmers might add a new set of functions to an existing smart contract. After the contract was launched on the blockchain, authorized people could use it by calling it. To make room for these new capabilities, other blockchain-based services do not need to be altered in any way. Two of the most well-known smart contract systems are the Ethereum virtual machine (written in the Solidity programming language) and Hyperledger fabric's chain code (written in a combination of Go, node.js, and Java). All blockchain transactions are part of the hash chain and hence irreversible, so a contract bug or exploitable weakness puts the system at risk. It's important to keep in mind that implementing smart contracts would probably cause the system's performance to decline, as various studies have demonstrated [35], [36].

3.4. Databases vs blockchains

Modern databases are usually created to be replicated and dispersed in order to attain high reliability. The most popular technique for replicating data across several servers or virtual machines is primary-backup replication. If one copy is misplaced, there are more copies accessible to keep the service running. This is really similar to other things. There are three key distinctions and some similarities across blockchain systems. Distributed databases are first focused on the issue of data management. On the other side, blockchains are built to guarantee data security. Second, distributed databases in blockchain technology often only manage crash failures, whereas Byzantine/arbitrary failures are accepted. Third, data integrity across many workstations is a top priority for blockchain systems. but lower data consistency requirements, such causal consistency, are often only achieved by distributed databases. In causal consistency, many nodes can simultaneously write data, which introduces the risk of data corruption. Conflicts will be settled later. Blockchain-based systems, on the other hand, provide the highest level of consistency and linearizability. A guarantee exists in distributed systems [37]. Informally, linearizability guarantees that the data is consistently consistent. Across all nodes, making distributed nodes act like centralised nodes.

4. INITIATIVE OF THE GOVERNMENT BASED ON BLOCKCHAIN

The distributed ledger technology known as blockchain guarantees consumers' data security [21]. The primary difference between blockchain and DLT is that the former is a method for establishing trust through consensus procedures and sequential data logging, whilst the latter is a system for managing a database schema. This section examines the setup, lessons learned, and attempts made by governments around the world to pilot blockchain systems. The majority of the applications examined were financial because cryptocurrencies use blockchains. Medical, building, city administration, assets, data processing, and teaching [16]. As seen in Figure 4, a number of nations around the world, including the United States, China, Switzerland, the Philippines, Japan, Brazil, South Korea, Malaysia, Georgia, Sweden, Australia, Malta, Estonia, Egypt, the United Arab Emirates, and Chile, have already started blockchain-based projects.

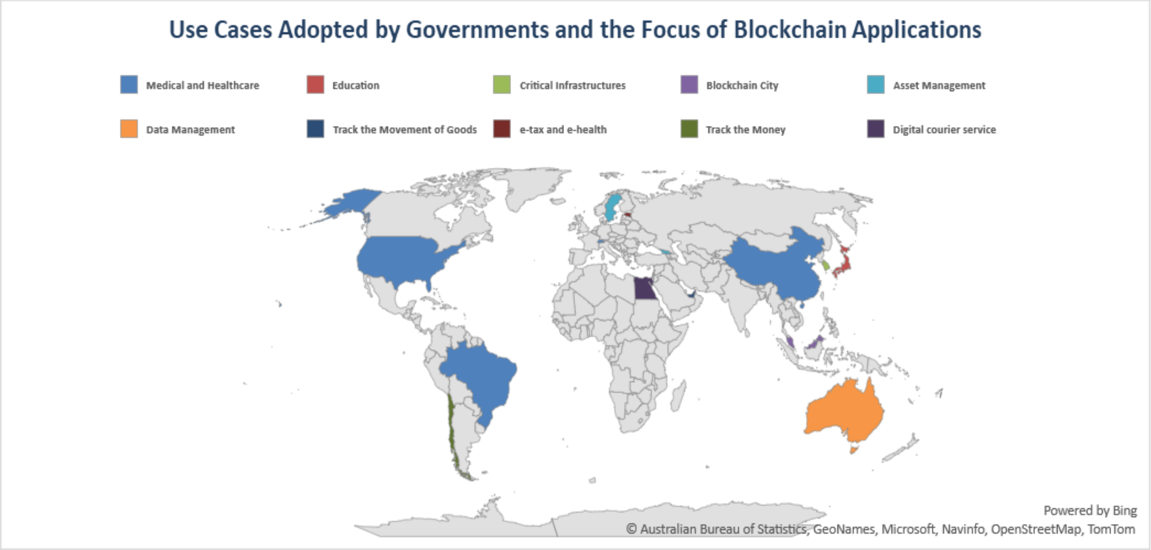
Use Cases Adopted by Governments and the Focus of Blockchain Applications
Medical and Healthcare
Education
Critical Infrastructures
Blockchain City
Asset Management
Data Management
Track the Movement of Goods
e-tax and e-health
Track the Money
Digital courier service
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Figure 4. Blockchain-based governmental use cases and applications

4.1. U.S government

Utilizing blockchain, artificial intelligence (AI), machine learning (ML), and process automation, the US Department of Health and Human Services (HHS) has created accelerate for contract billing administration.

Accelerate will assist HHS in managing 50 systems and 100,000 contracts totaling $25 billion. Instead of storing unstructured material, accelerate's blockchain captures a pointer to it (for example, documents). The system had an acceptable degree of risk and could be used in government applications after Accelerate became the first federal blockchain-based application to receive approval from a designated approving authority, an internal senior management official. Accelerate was expanded to include acquisition management, improving researcher access to contract information. Leadership at HHS talked about tracking sepsis data via blockchain. Up to $720 million in long-term savings at the point of purchase have been predicted by HHS. The centers for disease control and prevention (CDC) is also looking into utilising blockchain to track hepatitis A outbreaks and other public health crises. The Center for Surveillance Epidemiology and Laboratory Services of the CDC also started developing proofs of concept in 2017 for enhancing cross-state surveillance. The CDC and International Business Machines (IBM) have since worked together to develop a blockchain-based system to monitor the opioid pandemic. Ankr is also a for-profit blockchain infrastructure that is hosted in the cloud. With the help of the company's Proof of Useful Work mechanism, anyone with unused PCs or extra storage space can rent out their computing power for data mining. Ankr thinks that creating a universal basic income, which may take the place of the current welfare system, could be accomplished by paying everyone for using their computers to gather data. Additionally, the US General services administration is assessing the use of ledger systems, such as blockchain, in government operations as part of its Government IT Initiatives initiative. The organisation is investigating the application of smart contracts for patents, trademarks, IT uses, and the disbursement of foreign aid. In 2017, it held the U.S. Federal Blockchain Forum.

Furthermore, Senate Bill 1662, which acknowledges the legitimacy of blockchain-based smart contracts, was unanimously approved by the State of Tennessee in March 2018. In the bill, the state gives people employing smart contracts legal power to do so while carrying out electronic transactions, defending ownership rights, and safeguarding specific private data. Since its adoption, the law has served as a model for effective blockchain implementation for other states, the federal government, and even legal education programmes. Last but not least, one of the top US groups researching blockchain technology for use in government applications is The Illinois Blockchain Initiative. The state-funded initiative is looking into a number of distributed ledger applications to protect the data integrity of voter registration, passports, birth certificates, death certificates, and social security numbers. According to Illinois officials, using blockchain to store this important data is not only safer, but also more effective.

4.2. European governments

The Horizon programme supports blockchain projects in the European Union. A digital Luxembourg attempt to create a blockchain governance framework was initiated in 2017 by Luxembourg. The project's objectives include developing blockchain governance standards and a network of blockchain experts. In Estonia, e-government, e-healthcare, and e-identity are supported. 95% of Estonians' health data is digitalized and kept on blockchain, while 90% of Estonians file their taxes online. The way this government maintains and manages data has been completely transformed by the usage of blockchains. In Switzerland, Sweden, and Georgia, assets are managed using blockchains [15]. The adoption of blockchain for land title registry and related property transactions has streamlined the procedure in Georgia (at the intersection of Asia and Europe) [38]. A blockchain-based application for real estate transactions and land registration has been created in Sweden [39]. The Maltese government just finished the first national blockchain trial for managing academic credentials like degrees. This enhances data security, decreases red tape, and makes it simpler for students to access their credentials.

Additionally, the UK worked with GovCoin to create a blockchain for welfare payments. The programme functions as a virtual "jam-jar." The cryptocurrency is divided up into different "jars," or accounts, for things like utilities, groceries, and rent. Along with the efficiency of automatic payments, GovCoin stays away from banks, which have a tendency to keep crucial welfare funds for a long time. Elliptic further creates blockchain-based forensic investigative solutions for use by police departments, financial firms, and intelligence services. Authorities can examine cryptocurrency exchanges for linkages and unlawful transactions according to the company's technology. The programme developed by Elliptic has helped law enforcement identify instances of drug trafficking, extortion, tax evasion, and even attempted terrorism.

On the other hand, the Danish ministry of international affairs has partnered with the cryptocurrency exchange Coinify to use blockchain technology into the distribution of foreign aid. The time and money saved by not requiring a financial middleman is the biggest benefit of blockchain for Denmark. Donors and Denmark's foreign aid fund can send cryptocurrencies directly to relief organisations rather than relying on banks. Finally, the healthcare and cybersecurity systems in Estonia and the United Arab Emirates employ Guardtime. The company has created VaccineGuard, a digital network that links hospitals, vaccine makers, and distributors. The software can identify fake vaccines by using blockchain technology to speed up and ensure the safety of data sharing between parties.

4.3. Asian governments

The Philippine state endorsed an Ethereum-based solution in 2019 to deliver financial services to about 80 rural banks. The attempt is motivated by the fact that just 42% of Filipinos who are 15 or older have a bank account [40]. The blockchain city concept has been applied at Malaysia's Melaka Straits City, which was funded by China. The initiative uses blockchain to track visitors, luggage, and booking services. Additionally, the city will manage its own digital token known as the DMI coin that visitors may use to make purchases using their mobile devices. The second-most populous city in the nation, Busan, was awarded 4 billion Korean won ($3.5 million) to construct a block chain technology virtual power plant. Cloud-based power plants that mix various energy sources are necessary for optimal power output. The "city of the future" Dubai also switched its legal system to blockchain technology. The "Court of Blockchain" network uses smart contracts to improve Dubai's legal framework. Using a safe, effective, and transparent blockchain is expected to save the city some 25 million man-hours and $1.5 billion annually.

4.4. African governments

Blockchain technology has been used by African countries like Ghana to improve their commercial activities and increase the interoperability of their operational systems. Ghana's Central Bank has built a regulatory sandbox to make it easier to build and test cutting-edge blockchain-based solutions for merchant payments and remittance systems. This platform addresses the issue of platform interoperability and enhances system compatibility. Additionally, developing blockchain technology's interoperability can help with suitable standardisation across many industries and sectors. This may improve an organization's ability to quickly implement a standard industry-wide blockchain system. Additionally, the Land Layby Group, a Kenyan real estate firm with offices in Nairobi, enables people to safely purchase Ghanaian property. The Government Land registry systems are precisely replicated in the blockchain network to achieve this. As a result, prospective land buyers can use a tamper-proof digital format to effectively check, assess, and analyse the accuracy of the ownership information from the Government Land Registry systems. Based on blockchain technology, the Land Layby Group allows the online publication of land records. As a result, the issue of conflicting land titles for the same parcel of land is resolved. A similar business plan has also been developed by the Ghanaian startup BenBen.

All exporters to Egypt must submit online starting on October 1, 2021. Egyptian importers must register on the Nafeza site for Egyptian customs and ask for an Acid number. For importers to complete this process, the exporter needs to be registered on the CargoX Platform. A digital courier service is called CargoX. They are taking the place of paper records. Blockchain makes it easier to find the owners of genuine digital documents. A document can only be given to a receiver by its owner. CargoX expedites, secures, and reduces the cost of shipping originals internationally [41].

4.5. Latin American governments

SurBTC, currently known as Buda.com, was the first Bitcoin exchange in Chile when it was established in 2015. Corfo provided support and funding for the venture. This judgement made it clear that Chile will accept and regulate the use of blockchain for financial transactions as SurBTC is now under the supervision of Chile's Financial Intelligence Unit, which monitors money laundering. The largest Ethereum and Stellar Lumens exchange in the area, CryptoMkt.com, is also based in Chile. The Petro, the first cryptocurrency issued by a Latin American nation's government, was also introduced in March 2018 by Venezuela. It is said that the currency, which is equal to one barrel of Orinoco crude oil, is backed by Venezuela's reported oil production. A natural resource is used to link the Petro.

The Venezuelan government wants to establish a stable currency as a possible replacement for the Bolivar, which is suffering from crippling inflation, therefore it has tied the Petro to a natural resource. Additionally, in Argentina, Nic.ar, the government, and two other non-profit organisations came together to develop Blockchain Federal Argentina, a public-private partnership of permissioned networks. Additionally, IBM has disclosed US$5.5 million in funding for Sao Paulo, Brazil's first blockchain centre, which would be based in Latin America. One of the top companies joining the Latin American blockchain market is IBM.

5. RESULTS AND DISCUSSION

As shown in Figure 5, the rise in recent years in the quantity of articles published on blockchain-related government applications is consistent with a rising appreciation of the significance of blockchain's potential for use in government. Governmental organisations have started investigating how blockchain technology might improve the public sector. The use of this technology in the public sector, however, is still in its experimental stages. Many governments have experimented with using this cutting-edge technology for a variety of jobs and services. Studies and experiments show that blockchain still needs to be developed before it can significantly impact government.

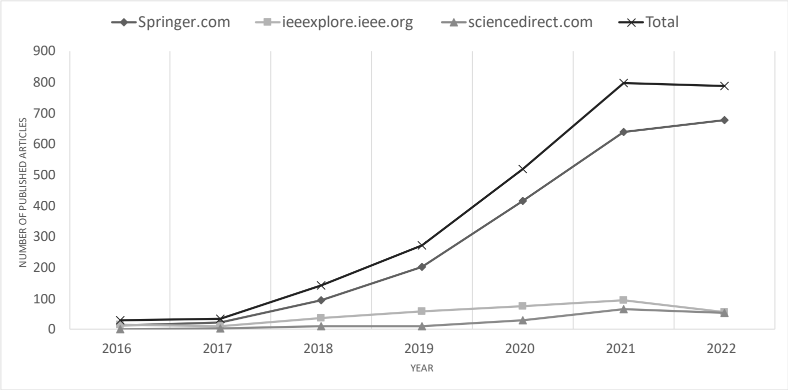

Figure 5. The growth in the number of papers published in the domain of governmental blockchain-based applications in digital scientific libraries

Governments must set out particular use cases in order to benefit from blockchain technology. Figure 6 illustrates the most frequent use cases to demonstrate how governments might apply blockchain technology to tackle real-world problems in the financial, educational, healthcare management, commercial and industrial, security and privacy, and internet of things (IoT) sectors. The majority of the time, centralised government systems are wasteful, expensive, and unsafe. To deliver more efficient and improved public services, governments all around the world have been actively exploring innovative technology. As a result, a government using blockchain technology might simplify the upkeep of trustworthy data. While limiting unauthorised data access and modification, the public sector is able to do this. The government may benefit greatly from a number of advantages of a blockchain-based system. Also, the government may find a number of elements of a blockchain-based system quite useful. Below are a few arguments for why governments ought to use blockchain technology.

Contrary to popular opinion, blockchain hasn't yet revolutionised or even disrupted the public sector. New business models, a new generation of services, or the outright disintermediation of any of the public institutions engaged in carrying out governmental duties have not yet materialised. Governments struggle to manage processes among various stakeholders, just like any large corporation. Compared to other institutions, the public wants governments to operate with greater transparency, justice, and accountability. Data management is the main impediment to success in these endeavours, especially in the digital era. The problems that governments face are, regrettably, beyond the scope of traditional centralized data management solutions. The single point of failure in the standard client-server. The usual client-server method has a single point of failure that undermines data security, and centralised government databases make it challenging to preserve openness. As a result, the majority of administrations have operations that are slow, ineffective, and opaque, ranging from property title registration to voting.

In this sense, studies of blockchain governance can be separated into two categories: governance by blockchains (such as rules and power dynamics within a network) and examinations of blockchain governance (such as how blockchains can be implemented to improve the self-governance of community-based peer production networks). According to our findings, government transactions are more effective and transparent thanks to the decentralised and distributive properties of blockchains that allow them to link a variety of loosely coupled commercial companies and government organisations. The majority of blockchain applications, however, do not clearly outperform traditional digital information storage. Additionally, despite the fact that most current implementations have not advanced past small-scale experiments, our analysis shows that blockchain applications in public sector governance have the potential to be widespread. We conclude by calling for the construction of public sector blockchain deployment indexes, given that there are not any already, and greater investigation into the reasons why governments haven't adopted blockchains more widely.

We believe that a deep understanding of the blockchain technology stack is necessary to create sustainable solutions for the public sector. When choosing a solution, information on governance processes, security, cost/duration indicators, network options (such as public, private, hybrid, or consortium), and distributed ledger technology protocols (such as Ethereum, Hyperledger, Corda, and others) must be taken into account (initial investment and annual operating costs). Furthermore,ealizing the promise of blockchain technology requires a framework for technology design and execution that starts by taking into account the areas where societal trust needs to be strengthened. Then, officials should determine which data must be recorded and kept in the blockchain (and which should not) in order to fulfil the trust's objectives, followed by a review of the blockchain designs, protocols, and other technical issues that provide the necessary capabilities. The future developments of the blockchain in applications for the government are shown in Figure 7. Blockchain technology has the potential to transform how governments run their businesses. It can be used to provide safe, open, and effective systems for controlling public information, monitoring public spending, and giving individuals access to services. Blockchain technology can be used by governments to strengthen the security of their data and lower fraud. Furthermore, blockchain-based applications might assist governments in streamlining procedures like taxation and voting. Last but not least, blockchain technology can be used to provide safe and unchangeable digital IDs, facilitating citizen access to government services.

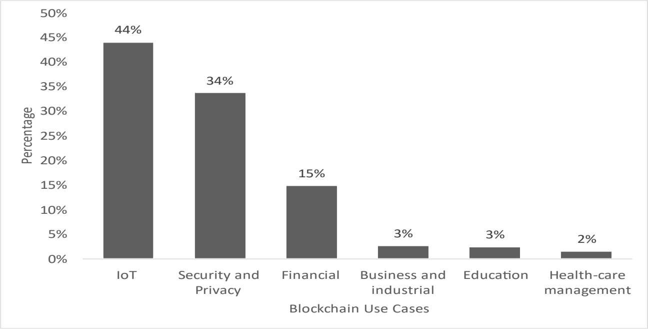

Figure 6. Blockchain-based governmental use cases

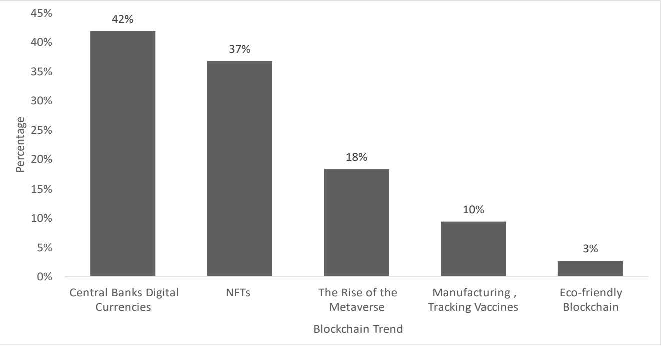

Figure 7. Future trends of blockchain in governmental applications

6. CONCLUSION

Without a question, the adoption of blockchain technology for record-keeping has the potential to increase the reliability of public bodies. Consistently validating and recording transactions, the consensus process looks for errors or attempts at counterfeiting. A continuously updated ledger is kept in several copies by independent nodes in a peer-to-peer network. It is claimed that decentralisation offers more record security and integrity than the majority of centralised systems. Additionally, blockchain technology has the potential to enable both new public service delivery and engagement models by generating data consistency across an ecosystem of organisations and players that goes beyond conventional public organisational boundaries. The once-only principle can be followed with the help of blockchain technology (OOP). In the public sector, it can aid in bridging organisational IT barriers by removing the need for endless data duplication and artificially integrating numerous back-office systems. However, a major barrier to realising blockchain's transformative potential is the incompatibility of blockchain-based solutions with current legal and organisational structures. As a result, the main objective of policy should be to advance distributed ledger technology and ecosystem maturity. In order to reduce incompatibility, technology must be adapted to legacy systems; but, to a greater extent, processes, organisations, and structures must be transformed using the disruptive power of blockchain. To provide a comprehensive conceptual framework for researching blockchain governance choices in the public sector, it is crucial to analyse diverse approaches to blockchain governance from multiple disciplines.

REFERENCES

[1] G.-R. V. Field, Muller, Lau, "The case for e-government: Excerpts from the OECD report 'The E-government imperative,'" *OECD Journal on Budgeting*, vol. 3, no. 1, pp. 62–96, 2003.

[2] M. Wimmer, C. Codagnone, and M. Janssen, "Future e-government research: 13 Research themes identified in the eGovRTD2020 project," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, Jan. 2008, pp. 223–223, doi: 10.1109/HICSS.2008.179.

[3] A. Jansen, "Assessing E-government progress–why and what," *Nokobit*, pp. 1504–1697, 2005.

[4] S. Ølnes, "Beyond Bitcoin - public sector innovation using the Bitcoin blockchain technology," *Norsk konferanse for organisasjoners bruk av IT*, vol. 23, no. 1, 2015.

[5] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?," *SSRN Electronic Journal*, 2016, doi: 10.2139/ssrn.2709713.

[6] M. Swan, "Blockchain thinking: The brain as a decentralized autonomous organization (DAC)," *Texas Bitcoin Conference*, pp. 27–35, 2015.

[7] S. Davidson, P. De Filippi, and J. Potts, "Economics of Blockchain," *SSRN Electronic Journal*, 2016, doi: 10.2139/ssrn.2744751.

[8] P. Yeoh, "Regulatory issues in blockchain technology," *Journal of Financial Regulation and Compliance*, vol. 25, no. 2, pp. 196–208, May 2017, doi: 10.1108/JFRC-08-2016-0068.

[9] T. Lyons, "Blockchain innovation in Europe," EU Blockchain Observatory and Forum, Brussels, Belgium., pp. 1-25, 2018.

[10] R. M. Garcia-Teruel, "Legal challenges and opportunities of blockchain technology in the real estate sector," *Journal of Property, Planning and Environmental Law*, vol. 12, no. 2, pp. 129–145, Jan. 2020, doi: 10.1108/JPPEL-07-2019-0039.

[11] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, Mar. 2020, pp. 342–345, doi: 10.1145/3341105.3374066.

[12] A. Datta, "Blockchain enabled digital government and public sector services: a survey," in *Public Administration and Information Technology*, vol. 36, 2021, pp. 175–195, doi: 10.1007/978-3-030-55746-1_8.

[13] D. Sarantis, C. Alexopoulos, Y. Charalabidis, Z. Lachana, and M. Loutsaris, "Blockchain in digital government: research needs identification," in *Lecture Notes in Business Information Processing*, vol. 402, 2020, pp. 188–204, doi: 10.1007/978-3-030-63396-7_13.

[14] R. M. Zein and H. Twinomurinzi, "Towards blockchain technology to support digital government," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11709 LNCS, 2019, pp. 207–220, doi: 10.1007/978-3-030-27523-5_15.

[15] D. Allessie, M. Sobolewski, and L. Vaccari, "Blockchain for digital government," JRC Science for Policy Report, vol. EUR 29677, pp. 1-88, 2019, [Online]. Available: https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049 blockchain for digital government.pdf.

[16] J. Clavin *et al.*, "Blockchains for government," *Digital Government: Research and Practice*, vol. 1, no. 3, pp. 1–21, Jul. 2020, doi: 10.1145/3427097.

[17] B.A Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Technical report, Ver. 2.3 EBSE Technical Report. EBSE, vol. 1, pp. 1–57, 2007.

[18] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *ACM International Conference Proceeding Series*, May 2014, pp. 1–10, doi: 10.1145/2601248.2601268.

[19] W. Choi and J. W.-K. Hong, "Performance evaluation of ethereum private and testnet networks using hyperledger caliper," in *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Sep. 2021, pp. 325–329, doi: 10.23919/APNOMS52696.2021.9562684.

[20] C. Cachin, D. Collins, T. Crain, and V. Gramoli, "Byzantine fault tolerant vector consensus with anonymous proposals," *arXiv:1902.10010*, 2019, doi: 10.48550/arXiv.1902.10010.

[21] R. Beck, C. Müller-Bloch, and J. L. King, "Governance in the blockchain economy: A framework and research agenda," *Journal of the Association for Information Systems*, vol. 19, no. 10, pp. 1020–1034, 2018, doi: 10.17705/1jais.00518.

[22] P. De Filippi, M. Mannan, and W. Reijers, "Blockchain as a confidence machine: The problem of trust challenges of governance," *Technology in Society*, vol. 62, Aug. 2020, doi: 10.1016/j.techsoc.2020.101284.

[23] R. Ziolkowski, G. Miscione, and G. Schwabe, "Decision problems in blockchain governance: old wine in new bottles or walking in someone else's shoes?," *Journal of Management Information Systems*, vol. 37, no. 2, pp. 316–348, Apr. 2020, doi: 10.1080/07421222.2020.1759974.

[24] J. Pierre, B. G. Peters, and N. Bradford, "Governance, politics and the state," *Environment and Planning C: Government and Policy*, vol. 19, no. 6, pp. 927–936, Dec. 2001, doi: 10.1068/c1906rvw.

[25] K. Werbach, *The Blockchain and the New Architecture of Trust*. The MIT Press, 2018, doi: 10.7551/mitpress/11449.001.0001.

[26] R. van Pelt, S. Jansen, D. Baars, and S. Overbeek, "Defining blockchain governance: a framework for analysis and comparison," *Information Systems Management*, vol. 38, no. 1, pp. 21–41, Jan. 2021, doi: 10.1080/10580530.2020.1720046.

[27] D. W. E. Allen, C. Berg, A. M. Lane, and J. Potts, "Cryptodemocracy and its institutional possibilities," *Review of Austrian Economics*, vol. 33, no. 3, pp. 363–374, 2020, doi: 10.1007/s11138-018-0423-6.

[28] B. E. Howell, P. H. Potgieter, and B. M. Sadowski, "Governance of blockchain and distributed ledger technology projects," *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3365519.

[29] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9591, pp. 112–125, 2016, doi: 10.1007/978-3-319-39028-4_9.

[30] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, Nov. 2002, doi: 10.1145/571637.571640.

[31] A. Bessani, J. Sousa, and E. E. P. Alchieri, "State machine replication for the masses with BFT-SMART," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Jun. 2014, pp. 355–362, doi: 10.1109/DSN.2014.43.

[32] J. Cowling, D. Myers, B. Liskov, R. Rodrigues, and L. Shrira, "HQ replication: A hybrid quorum protocol for Byzantine fault tolerance," *OSDI 2006 - 7th USENIX Symposium on Operating Systems Design and Implementation*, 2006, pp. 177–190.

[33] S. Duan, M. K. Reiter, and H. Zhang, "BEAT," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2018, pp. 2028–2041, doi: 10.1145/3243734.3243812.

[34] P. L. Aublin, R. Guerraoui, N. Knežević, V. Quéma, and M. Vukolić, "The next 700 BFT protocols," *ACM Transactions on Computer Systems*, vol. 32, no. 4, pp. 1–45, Jan. 2015, doi: 10.1145/2658994.

[35] G. G. Gueta *et al.*, “SBFT: a scalable and decentralized trust infrastructure,” *arXiv:1804.01626*, pp. 1–23, Apr. 2018, doi: 10.48550/arXiv.1804.01626.
[36] E. Androulaki, C. Cachin, C. Ferris, A. Barger, and K. Christidis, “Hyperledger Fabric: A distributed operating system for permissioned blockchains,” in *EuroSys ’18: Proceedings of the Thirteenth EuroSys Conference*, 2022, pp. 125–147, doi: 10.1145/3190508.3190538.
[37] M. P. Herlihy and J. M. Wing, “Linearizability: a correctness condition for concurrent objects,” *ACM Transactions on Programming Languages and Systems*, vol. 12, no. 3, pp. 463–492, Jul. 1990, doi: 10.1145/78969.78972.
[38] Q. Shang and A. Price, “A blockchain-based land titling project for the republic of Georgia,” *Innovations: Technology, Governance, Globalization*, vol. 12, no. (3-4):, pp. 72–78, 2018, doi: 10.1162/inov_a_00276.
[39] V. L. Lemieux, “Evaluating the use of blockchain in land transactions: an archival science perspective,” *European Property Law Journal*, vol. 6, no. 3, pp. 392–440, Dec. 2017, doi: 10.1515/eplj-2017-0019.
[40] A. Demirguc-Kunt, L. Klapper, D. Singer, S. Ansar, and J. Hess, *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*. Washington, DC: World Bank, 2018, doi: 10.1596/978-1-4648-1259-0.
[41] “CargoX,” *CargoX*, 2018. Accessed: Apr. 12, 2022. [Online.] Available: https://cargox.io/.

BIOGRAPHIES OF AUTHORS

Ibrahim Ramadan Abdelhamid is a post-graduate student at the Faculty of Computer and Information Sciences, Minia University, Egypt. He received his B.Sc. Degree in Computer Science from the Faculty of Computer and Information Sciences, Minia University, Egypt in 2009. He is a Senior Project Manager in the Ministry of Finance in Egypt (Minister's Office) with 13 years of experience in the technology, private, and public sectors, focusing mainly on IT operations and program/portfolio management. He is a Project Management Professional (PMP) certified, and he is also certified in ITIL® from AXELOS. He holds a Diploma in Management from ESLSCA University. He has worked in the private sector at ITvally, an IBM Partner. He was also selected as one of the top 10 employees in the Egyptian government in 2020. He can be contacted at email: ibrahim.ramadan2207@gmail.com.

Dr. Islam Tharwat Abdel Halim is an assistant professor at, Nile University, Egypt. He received his B.Sc., M.Sc., and Ph.D. degrees in computer engineering from the Faculty of Engineering, Ain Shams University, Egypt. He is an IEEE senior member currently serving as Chair of the Awareness and Customer Advocacy Subcommittee of the IEEE Computer Society Distinguished Visitor Program. Also, he is appointed as R8 Portifio (Chapter Vitality). He has authored many research articles in various refereed conferences and journals, including IEEE Intelligent Transportation Systems Magazine, Computer Networks (Elsevier), and Wireless Networks (Springer). His current research interests include computer security, IoT, Fog/Edge computing, and mobile and wireless networks. He can be contacted at email: ihalim@nu.edu.eg.

Abd El-Majeed Amin Ali is currently a Professor with the Computer Science Department, Minia University, Minya, Egypt. He has published over 80 research papers in prestigious international journals and conference proceedings. He has supervised over 60 Ph.D. and M.Sc. students. His research interests include information retrieval, software engineering, image processing, data security, metaheuristics, the IoT, digital image steganography, and data warehousing. He is a member of the International Journal of Information Theories and Applications (ITA). He can be contacted at email: a.ali@mu.edu.eg.

Ibrahim Abdelmoniem Ibrahim received his Ph.D. in Computer and Information Sciences at the Data Science group, School of Information Technology and Electrical Engineering, University of Queensland, Australia. Supervised by Prof. Xue Li and Dr. Xin Zhao. His research projects are focused on: artificial intelligence, big data analytics and visualization, blockchain technology, sentiment analysis, machine learning, and data mining. He can be contacted at email: i.ibrahim@minia.edu.eg.