A Review of Blockchain Technology for E- Governance: Applications and Challenges

Conference Paper · January 2024

CITATIONS
0

READS
157

2 authors:

Sapni Ranchagoda
General Sir John Kotelawala Defence University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

R. P. S Kathriarachchi
General Sir John Kotelawala Defence University
31 PUBLICATIONS **9** CITATIONS
SEE PROFILE

A Review of Blockchain Technology for E-Governance: Applications and Challenges

***Abstract*— E-governance is the use of ICT to improve governance quality and effectiveness in the delivery of services to people, businesses, and other stakeholders. However, data privacy, confidentiality, dependability, coordination, and interoperability issues hinder e-governance from attaining its full potential. Therefore, this research focuses on how blockchain can add more transparency and strengthen security in e-governance. The paper uses a systematic review approach to collect relevant data and studies related to blockchain in e-government. This study integrates the basic blockchain elements including applications, data safety, and compatibility with other platforms. The paper also conducts a comprehensive analysis of blockchain applications in e-governance such as identity management, voting system security, transparent supply chains, and electronic document notary services. The study demonstrates these applications using empirical examples and case studies from different countries and contexts. The findings contribute to shaping the future of electronic governance by solving challenges and highlighting opportunities associated with the advent of blockchain. The research underscores the need for more investigations on how blockchain can be applied to effective governance for a responsible approach toward its adoption.**

Keywords*—*Blockchain, E-Governance, applications, challenges, decentralization, privacy, security

I. INTRODUCTION

Many governments across the world are gradually adopting ICTs for service modernization, to interact with citizens, and to strengthen good governance. An innovation is better known as e-governance, where Information Communication Technologies (ICTs) are employed in revamping public management and encouraging public participation. The electronic governance uses information technology for improved internal administrative processes, economic exchanges, and citizens' participation in democratic governance. The strategic approach towards e-governance is one of the strongest tools that governments can use to overcome some challenges such as bureaucratic incompetence, social divisions, and democratic weaknesses. E-governance is a crucial component of modern governance since it delivers faster, easier, and better public service, enhances public involvement and participation, and counteracts corruption and cheating. Though the merits of e-governance are many, the environment is also riddled with problems that require modern and flexible solutions. The paramount issue is ensuring the protection of data from intrusions, invasion of privacy, and suspicion by society. Government data that includes personal information, financial details, and official documents are very sensitive. It is therefore critical to safeguard them from intrusion, modification, and revelation. Further, e-government should be aimed at preserving the reliability, suitability, and control of vital government affairs including election, procurement, and taxation. Additionally important is the ability of government systems to be reliable, scalable, and interoperable, including databases, networks, and infrastructures for smooth government functions. These challenges need both technological and organizational approaches to address them.

A very innovative system known as 'blockchain' is based on distribution ledger technologies and is used to create and manage decentralized and unchangeable logs of transactions among several people without the necessity of any central authority or mediator. Its features position it as a good means of providing an effective, transparent, and dependable display, confirmation, and exchange of information. Blockchain in e-governance also has promising prospects for more secure storage of governmental data, trustworthy electronic voting, and transparent procurements. Blockchain has the potential to usher transformative change in the management style of governments as they will be empowered to involve the public and other stakeholders in active decision-making processes that can drive positive reforms.

This paper aims at looking into the existing blockchain technologies and how they relate to e-governance and identifying if there are any issues when using them in e-governance. The main research question of this paper is: How can blockchain generation be carried out to e-governance to enhance its safety, transparency, and efficiency?
The objectives of this paper are:

- Evaluate the literature on blockchain technology, their attributes, and their makes use of.
- Analyze and discourse the boundaries, integrations into current systems and destiny guidelines regarding blockchain and e-government.
- Providing some real-world examples and case studies to illustrate the blockchain applications in e-governance.

This paper uses a systematic review and search for relevant literature with recent data that was retrieved from multiple sources such as scholarly and search databases. The paper is structured as follows. Section II provides a literature review on e-governance and its importance, blockchain technologies, their applications in e-governance, and information security and privacy problems. Section III gives an analysis and discussion on the challenges and barriers, integration with existing systems, and future guidelines and emerging technologies in blockchain for e-governance. Section IV concludes the paper with a summary of the key findings and implications of the assessment, emphasizing the position of blockchain technologies in e-governance. Finally, Section V contains

all the citations used in this study to understand how Blockchain Technology can be applied to electronic governance.

II. LITERATURE REVIEW

A. *E-Governance and Its Importance*

E-Governance is defined as the 'use of IT by government agencies that enables reforms in the relationship between the government and its citizens, enterprises and other branches of government'[1]. As shown in Fig. 1[2], E-governance can be classified into four categories based on the direction of communication: G2C(government-to-citizen), G2B(government-to-business), G2G(government-to-government) and G2E(government-to-employee) [3].

G2C: This is the contact between the government and citizens in which the government provides various services and information to citizens via online platforms or mobile applications.

G2B: This is the relationship between the government and the businesses, in which the government provides several services and data to the businesses via online platforms or mobile applications.

G2G: This is the relationship between different tiers or branches of the government, in which the government stores and exchanges various offers and data amongst themselves via online structures or mobile packages.

G2E: This is the contact between the government and its workers, in which the government provides various offerings and data to its employees via online platforms or mobile applications.

As shown in Fig. 1, we can recognize some applications relating to each category.

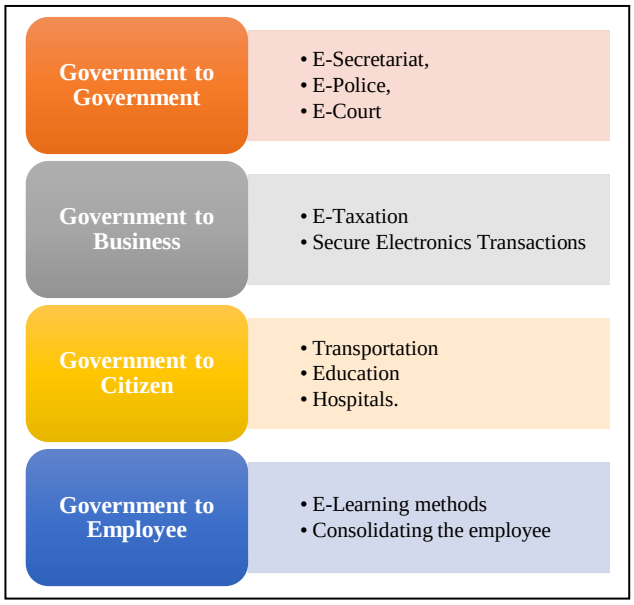

Fig. 1. Types of E-governance based on the direction of communication

There are several benefits of e-governance in modern technology including enhancing citizen services, reducing corruption, improving efficiency, and fostering innovation.

Enhancing Citizen Services: It is easy for citizens with e-governance to provide goods and services using online platforms or mobile applications[4]. E-governance will also allow public involvement in the decision-making process by letting them provide responses or engage in discussions online.

Reducing Corruption: Transparency of e-governance reduces corruption and responsibility in government operations. Monitoring is facilitated through e-governance, as well as reporting any inconsistencies or misconduct on electronic platforms or in other ways like whistleblowing systems[5].

Improving Efficiency: Cost reduction is possible through e-governance and processes taking place in government. E-governance can also enable automation as well as collaboration and working with others in various departments or agencies.

Fostering Innovation: For instance, e-governance can open new opportunities for innovation by collaborating with the government on policy formation, co-creation of solutions by citizens, and involvement of businesses and other interests in such work. It is e-governance that can adopt new technologies like those that make possible provision of efficient, high-standard services by the governments.

E-governance is a new trend in the implementation of government objectives but poses some constraints that must be remedied like data security and privacy, trust, corruption, and cooperation.

Data Security: In e-governance, a large volume of sensitive and personal data is collected, stored, processed, and shared. This data must remain inaccessible or safe against unauthorized access, modification, or leakage. It is necessary to secure data to preserve the confidentiality, integrity, and accessibility of data. This also preserves the faith and beliefs of the users in it.

Data Privacy: Data gathering has become a part of e-governance. It is used for service delivery, policy-making, and conducting research. Personal data may include personal or identifiable information that may provide an understanding of the user's identity, tastes, and actions. Privacy is critical or paramount to maintaining the rights and dignity of users, as well as conforming with laws and ethics. It allows identifying that some e-governance activities like data mining, data sharing, and data profiling may interfere with privacy rights and expose them to risks like discrimination, surveillance, or manipulation.

Trust: E-government refers to the interface of government and its public through electronically driven platforms. To build confidence, trustworthiness, and authenticity of these interactions trust becomes very crucial in creating a good relationship between government and consumer. Several

factors such as the quality-of-service delivery, how responsive the government is, openness in processes, and the security and privacy of data may influence trust. For instance, distrust can cause users not to use or try adoption of e-governance services and negatively affect their satisfaction and loyalty.

Corruption: It comprises many actors like government agents who provide services, intermediaries, and customers. E-governance is not perfect and may be threatened by corruption, destroying its integrity, fairness, and efficiency. There are different types of corruption, including inducing, fraud, nepotism, and favoritism. Corruption eats off public interest and Social Welfare. For instance, corruption can distort resource allocation, reduce the quality of public goods and services, weaken trust in government institutions, and delay democratic development.

Therefore, suitable e-governance solutions are required to deal with such challenges and make e-governance services more reliable. Among other solutions, blockchain technology offers a viable option to solve most of these issues to enhance the quality of deliverables.

E-governance can also contribute to the achievement of various national and global goals and programs, such as the Sustainable Development Goals, the Digital India Program, and the E-government Survey from the United Nations.

The Sustainable Development Goals (SDGs): This is comprised of 17 goals and 169 targets that will lead people out of poverty and towards having peace, a clean environment, and prosperous lives throughout. E-governance has a role in supplying data, information, and services for the social, economic, and environmental aspects of development towards achieving the SDGs[6].
Digital India Program: A flagship project of the government of India, which seeks to create a vibrant digital and knowledge-based society for India by 2025. E-Governance is one of the 9 target domains of the Digital India program aimed at providing digital services, usages, and literacy for civilians and sectors[7].

E-government survey from the UN which is done biannually evaluates e-government maturity as well as the development of 193 UN members, using a composite index composed of three factors – availability of services over the internet, telecom infrastructure, and human capital capabilities. Countries can improve their standing or position on the survey by embracing and establishing the highest benchmarks and standards of e-government[8].

Therefore, e-governance is a crucial instrument for boosting the quality of governance and development outcomes at both national and societal levels and facilitating the effective provision of government services and information.

B. Blockchain Technologies

Blockchain Technology is a distributed ledger scheme that guarantees the security and integrity of transactional data through transparency and immutability[9]. A blockchain is composed of several chains of blocks, interconnected through certain hashes. Validation is done through a network of nodes that use the consensus algorithm on each block of transactions[10]. The nodes update the blockchain individually by following the consensus rules. Any person can participate in the network or access information within the chain. Fig. 2 provides a concise overview of the blockchain mechanism and its components[11].

- Nodes: Nodes refer to the computers or gadgets that participate in the chain of the blockchain that have a replica of data stored across them. This makes nodes capable of performing various roles including verifying transactions creating blocks and executing smart contracts. The nodes may also operate at different levels in the network, for instance, as a full node, light node, or super node[12].

- Transactions: The information or data that is passed from one node in a blockchain network to another is known as transactions. The transaction could refer to diverse actions or events like transferring or registering assets, sending, or receiving cash, voting, stating an opinion, and making contract provisions or enforcement among others. Cryptographic proofs are used to verify transactions against the blockchain-based ledger, which is immutable, transparent, verifiable, and tamper-proof[12].

- Blocks: A batch of transactions is contained in blocks which serve as the container units on the ledger. Hashes serve as unique identifiers obtained from the previous block's raw data and used to link blocks together. This forms a series of blocks referred to as the ledger. The shared ledgers are updated such that it ensures cohesion among different nodes of the network and this single source of truth holds information on transactions and their history[12].

- Hashes: The mathematical functions responsible for changing any input data into fixed-length outputs, referred to as hashes. Hashes have two main properties: they are one-directional, indicating that hashing can be done with ease from input data, while the backward operation of identifying the originating input data from the resulting generated hash is inappropriate. Secondly, their security depends on the properties which makes them resistant to collision. The hashes ensure that no one can modify the data because any changes made will lead to new hashes[12].

- Signatures: The cryptographic methodologies by which nodes can verify their identification and authorization in the blockchain network are referred to as signatures. Signatures are also known as "Public-key cryptography", using a pair of keys such as public and private keys respectively. Any public key used for authentication can be found anywhere

in the network. The node only knows its private key for signing the transactions or the messages that it either sends or receives. The transaction and message non-repudiation and accountability of each node's signature are ensured for all nodes in a blockchain chain using signatures[12].

- Consensus algorithms: These are the rules, or the protocol used by nodes to reach a consensus about the state of the ledger on the blockchain network. In addition to this, consensus algorithms are required to ensure a consistent and truthful ledger due to different or falsified transactions or blocks on a network. Consensus algorithms can be classified into two main types: proof-based and voting-based. Proof–based algorithms need some effort or some property of value for a node to take part in the consensus like proof–of-work and proof–of-stake. In voting-based algorithms, nodes vote or delegate their votes to other nodes that are supposed to reach a specified major or threshold like in cases of proof-of-authority and proof-of-reputation[12].

- Smart contracts: The smart contract is a program or code, which is stored in the chain and performs different functions or actions depending on the given conditions or rules. Such smart contracts can interact with others, and other transactions, in addition to external data sources; as well as enforce actions or results there. Smart contracts provide ways of automation many processes under E-governance like identification and authentication systems, votes verification, procurements, document validity, and confidential information access[12].

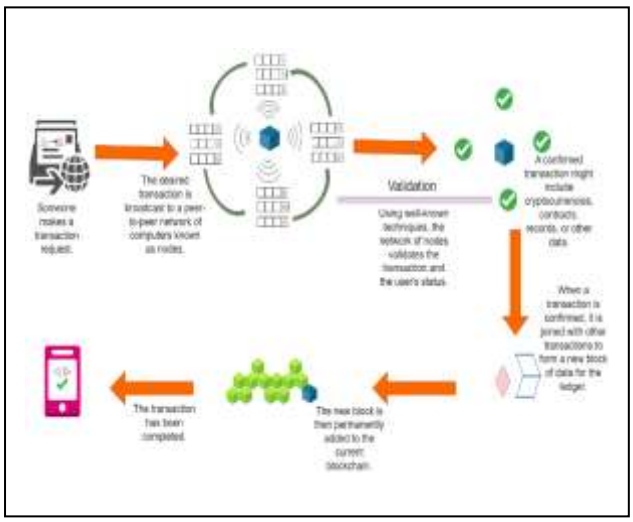

Fig. 2. How Blockchain Mechanism Works

Blockchain technology has several features that make it relevant for e-governance, such as decentralization, transparency, immutability, and security. Its distinct characteristics make it an efficient tool for consistent, clear, and effective data control and transaction processing.

Decentralization: The use of blockchain technology does not require any intermediaries or centers to confirm transactions. It is based on a distributed system of nodes that are acting as peers[13]. This capability minimizes chances associated with a single point of failure or corruption, making a backup system more endurable and robust.

Transparency: A clear visible record of transactions on blockchain can be seen by anyone with access to a particular blockchain. This enhances accountability and traceability as well in transactions allowing one to confirm the reliability and validity of information[10].

Immutability: In this case, whenever a transaction is recorded on the blockchain it can never be changed or withdrawn and newly created by breaking the chain of encryption. This characteristic makes sure that no one can manipulate or forge the data, hence the recorded history of transactions is undamaged.

Security: With cryptographic mechanisms, blockchain ensures transactions and data security within the blockchain. They include digital signature schemes, hash functions, and encryption schemes. This makes it possible for legitimate and authorized persons only to create, alter, or obtain data in these blockchain mechanisms.

As shown in Fig. 3, distributed ledger technologies can be divided into two categories based on their openness and decentralization: permissioned and permissionless blockchains. These two types of distributed ledger technologies are also compatible with four types of blockchain: public, private, consortium, and hybrid.

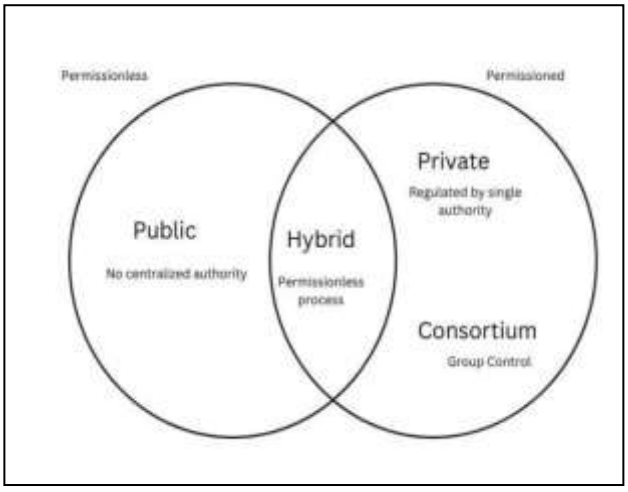

Fig. 3. Scope of Different Types of Blockchain Technologies

Public blockchain: The public Blockchain can be accessed by anybody eager to join the network or access its information. The network has a distributed architecture with no single control body or intermediary for the validation of operations. Validation of transactions is performed through a majority-based consensus algorithm, where many nodes must agree on the validity of transactions. Public blockchain includes Bitcoin and Ethereum.

Private blockchain: Only a limited number of people can enter the network, and they determine which party has the right to obtain information on the chain. This is characterized by a central authority or an intermediary regulating the network or verifying transactions. A consensus algorithm where a fixed number of nodes agreeing on the validity of transactions verifies it. Some of these private blockchains include Hyperledger Fabric and Corda.

Consortium Blockchain: Consortium blockchain is a hybrid of public and personal blockchain. They restrict a specific group of users who are allowed to connect to the network or access the data. However, there is no central authority or intermediary that oversees the networking process or validates transactions. Connections are validated by a consensus algorithm that requires a subset of nodes to agree on the validity of the connection. Only authorized users in the group can create smart contracts or applications on the blockchain. Examples of association blockchains are Quorum and R3CEV.

Hybrid Blockchain: A hybrid blockchain is an aggregate of public and personal blockchain. This records some transactions on the public blockchain and some transactions on the private blockchain. This blockchain can provide transparency and privacy for businesses. Examples of hybrid blockchains are Dragonchain and Kadena.

These details are further summarized clearly in TABLE I as follows.

TABLE I. A COMPARATIVE SUMMARY OF BLOCKCHAIN TYPES

Type	Access	Control	Validation	Examples
Public	Open to anyone	No central authority or intermediary	Consensus algorithm for most nodes	Bitcoin, Ethereum
Private	Limited to a certain group of individuals	Central authority and intermediary	Consensus algorithm using a predefined set of nodes	Hyperledger Fabric, Corda
Consortium	Limited to certain participants only	No central authority and intermediary	Consensus on a subset of nodes	Quorum, R3CEV
Hybrid	Combination of private and public blockchains	Depends on the type of transactions	Depends on the type of transactions	Dragonchain, Kadena

C. Applications of Blockchain in E-Governance

Blockchain technology has a range of e-governance applications that can enhance the security, transparency, and efficiency of government operations and create new opportunities for innovation and collaboration. This section presents some applications of blockchain technology in e-governance and provides real-world examples and case studies for each application.

a) Identity Management and Authentication

Identity Management and Authentication are important e-governance functions that enable citizens to access government services and information online. However, traditional identity and authentication systems rely on centralized or intermediary databases that store real citizens and sensitive information making these systems vulnerable to data breaches, human theft, fraud, and abuse.
Blockchain technology can provide a decentralized and self-governing identity management authentication system that empowers citizens to take control of their identity and data. Blockchain technology can enable citizens to create and verify their own digital identities using cryptographic evidence verified by a network of nodes. Citizens can use their digital identity to access government services and information without revealing personal or sensitive information. Citizens can also grant or deny access to their data to third parties based on their preferences.

As illustrated in Fig. 4[14], a blockchain-based decentralized identity verification system consists of three main entities: verifiers, issuers, and holders of identities. An identity issuer is an organization responsible for claiming characteristics that belong to an owner such as a name, birth date, home, or residence address. On top of that, there are identity holders who are a group of people that possess their identity data which they control and can provide to others if desired. An identity verifier is an organization that will confirm the identity of the holder to provide it with privileges to access a certain service or resource. Initially, the identity holder asks for a claim from the identity issuer to verify an identity. The issuer of an ID then appends its DID to signify the claim. The claim is finally signed and stored on the blockchain. The identity holder can next present the counter-signed claim to the identity verifier. The identity verifier will thereafter confirm the DID of the entity that issued the ID and the sign on the signed claim. This structure offers several advantages in comparison with conventional identity verification methodologies. It is first, decentralized (as there is no one dictator in the system). It also becomes more stable, and less vulnerable to fraud. Another feature of the system is its user-centricity in that the identity holder has control over their identity information. Lastly, the system is transparent as all the claims are kept in the blockchain and can be verified by anybody.

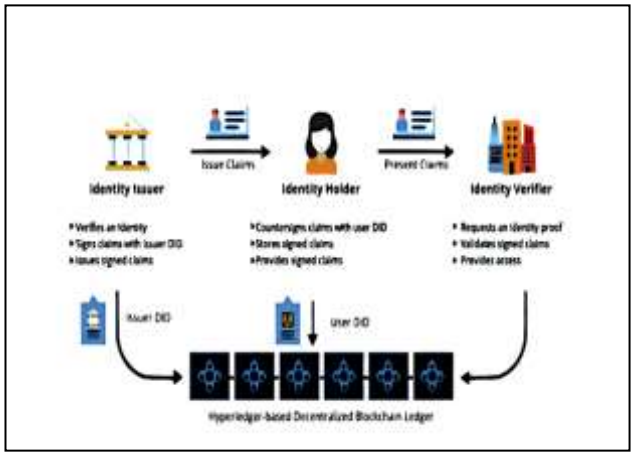

Fig. 4. Blockchain-based identity verification system

Some examples of blockchain-based identity management and authentication systems for e-governance include Estonia e-residency system,India's Aadhaar system and Canada's Verified.me network.

Estonia e-residency system: Estonia is a pioneer in e-governance and has launched a blockchain-based e-residency system that allows anyone in the world to become a digital resident of Estonia and access its online services. The e-resident system secures the digital identities and data of e-residents using blockchain technology to protect and provide them with digital signatures that can be used for validation, verification, and storage. The e-residency program enables e-residents to set up businesses in Estonia and the EU (European Union), open a bank account, pay taxes, and get other jobs[15].

India's Aadhaar system: India uses Aadhaar, a biometric-based identification system that assigns a unique 12-digit number to every resident of India. The Aadhaar system is used for various purposes, such as social welfare, banking, taxation, education, and health care. However, the Aadhaar system faces many challenges, including data security, privacy, and inclusion. To address these challenges, India is exploring how to use blockchain technology to enhance the Aadhaar system by creating a decentralized and consensus-based identity platform that can protect citizens' data and privacy. The blockchain-based platform can also enable citizens to share their data securely and selectively with service providers[16].

Canada's Verified.Me network: The Verified. Me Network of Canada is an example, being a digital identity network based on blockchain technology that empowers Canadians to establish and validate their digital identities based on their already existing bank accounts. It's a partnership between many banks, telcos, and government institutions as well as SecureKey which is a blockchain enterprise known as Verified. Me Network. The Verified.Me network is running on IBM's Hyperledger Fabric blockchain technology for creating a decentralized identity verification ecosystem that empowers users with their consent and control[17].

b) Secure voting systems

Elections are the fundamental right and duty of citizens in a democracy to elect their representatives and express their views on public issues, but traditional electoral systems face many challenges including voter fraud, vote tampering, people low attendance rates, accessibility, and transparency.
Blockchain technology can provide a secure, transparent, and accessible electoral system that can improve public confidence and participation in the democratic process. Blockchain technology can enable citizens to cast their votes online by verifying their digital identity using cryptographic evidence using a network of nodes. Irrevocable and anonymous votes are recorded on the blockchain preventing any tampering or distortion. Election results are transparent and auditable by anyone on the blockchain.

As Fig. 5 indicates, blockchain-based voting consists of several steps[18].

Voters Registration: Voters register using their identity cards and biometrics data. Voters have a voter ID and secret key that they use in voting.

Voter List Generation: The blockchain network generates and verifies the voter list. The voter's list is composed of the voter IDs and the public keys of all the registered voters.

Audit Votes: This allows voters to first audit their votes before voting. They can make sure that their IDs, voter IDs, and voting keys are in order and whether the eligibility to vote can be guaranteed.

Voter Distribution: Voters can cast a ballot over a secure channel including an application on mobile phones or a website. These are protected by a combination of the voter's cryptographic key and the general cryptographic key for the voting chain.

Casted votes are sent to the blockchain: The voters send encrypted ballots, each of which is an encrypted vote, to the public blockchain network. They verify the votes and add them to the ledger in the blockchain network.

Result: Blockchain determines election outcomes. This results in a transparent system that can be verified by anybody with the ledger copy.

Voting Machine or Voting Booth: Additionally, voters can choose their preferred nominee either through a voting machine or a blockchain-connected voting booth. Voter's identity documents and biometric data are scanned by a voting machine or voting booth which verifies a voter`s eligibility. The voter then marks his/her selection and confirms it by pushing a button on the screen. The vote is encrypted and relayed to the blockchain network.

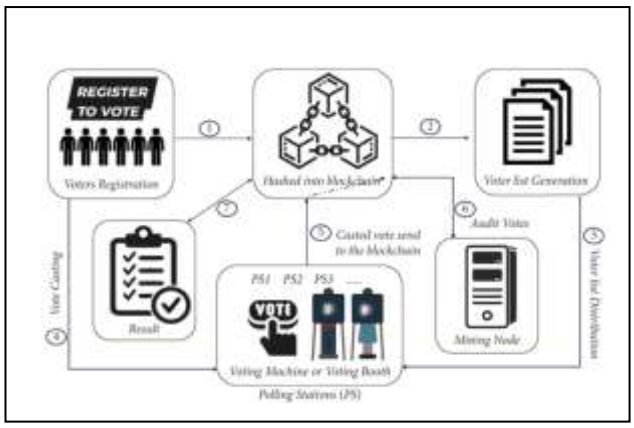

Fig. 5. End-to-end process of voting in a blockchain-based voting system

Some examples of blockchain-based voting systems for e-governance include Sierra Leone presidential election, Moscow's Active Citizen platform, and South Korea's online voting platform.

Sierra Leone Presidential Election: Sierra Leone was the first country to use blockchain technology to verify the results of its presidential election in 2018. Documents were scanned and uploaded to Agora, a blockchain platform that verifies the integrity of ballot papers using cryptographic evidence. The results of the election were visible and accessible to those present on the Agora platform[19].

Moscow's Active Citizen Platform: Moscow is a city that uses Active Citizen, a blockchain-based online voting platform that allows its citizens to participate in various public decisions, such as city planning, budgeting, and social services. Blockchain uses technology to secure citizens' votes and data and provides them with digital certificates that can be used for payments or discounts. The platform also uses smart contracts to automate the voting process and ensure equality[20].

Switzerland's E-Voting Pilot: In the case of such a country like Switzerland, which has tried e-voting using the blockchain and was among the top ten pioneer nations in this field. The city of Zug in 2018 ran a pilot project exploring if blockchain-based e-voting could be used to allow the citizens to vote on municipal issues through their smartphone. Ethereum's public blockchain platform was utilized for recording and verifying the votes using the e-voting system, which was tamper-proof.[21]

South Korea's online voting platform: The case of South Korea is even more fascinating as it contemplates the application of blockchain technology to online voting. The NEC launched an internet voting platform known as K-Voting in 2018 on a private blockchain network to guarantee privacy and openness of the elections. By 119 public institutions, using the K-Voting platform was considered for different intentions including surveys, polling, petitions, and other purposes[22].

c) Supply Chain Transparency for Government Procurement

It involves the purchase of products or services that government bodies make for their use. Government procurement is considered a substantial part of public expenditure and influences how the government provides its services. However, the buying process from governments, as in other fields, is not without problems. There are cases of grafts, scams, collusions, unproductivity, and lack of openness.

The use of blockchain technology in a transparent and traceable supply chain system could enhance the accountability and efficiency of public procurement. Using blockchain technology, government entities will be able to register and keep a record of all transactions and movement of goods and services from their source to the point of destination on the blockchain. Transactions are verified through cryptographic proofs implemented by a network of nodes, and they are then made immutable and auditable by anyone accessing the blockchain. The blockchain might also enable 'smart contracts, which can activate and carry out the performance and satisfaction of contractual clauses.

Fig.6 shows a supply chain where RFID (Radio Frequency Identification) tags are attached to the components and barcodes are used to complete the product[23].

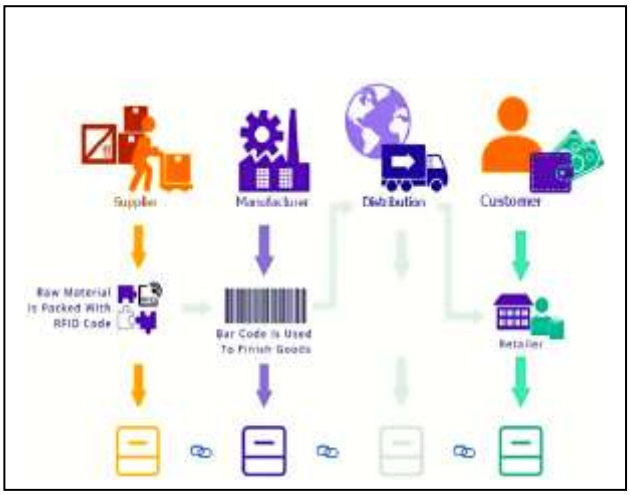

Fig. 6. Blockchain-based Supply Chain Process

Some examples of blockchain-based supply chain systems for government procurement include World Food Programme's Building Blocks project, Dubai's Blockchain Strategy, and the US Department of Defense's blockchain-based supply chain system.

World Food Programme's Building Blocks project: WFP stands for World Food Program, which feeds millions around the world. The WFP has introduced its Building Blocks project, which uses blockchain technology to enhance the effectiveness and reliability of its cash-transfer systems. The project aims at using a Blockchain system to generate Digital Identity for the beneficiaries and to document all their transaction through the Blockchain system. Also, it involves the utilization of smart contracts in cutting down operational expenses and threats as well as prompting appropriate and on-time payment procedures[24].

Dubai's Blockchain Strategy: Dubai has come up with a complete blockchain strategy aimed at turning the city into a world leader in public services by becoming the first of its kind city powered by blockchain, by the year 2020. The latter uses blockchain technology to enhance its government procurement procedures as one of the foundational blocks of this approach. This means that the strategy involves building a system of distributed ledger technology, commonly known as a blockchain platform that would include suppliers, buyers, regulators, and auditors. It could facilitate secure and smooth dealings, efficient contracts, and timely tracking of supply chains[25].

The US Department of Defense's blockchain-based supply chain system: The US DoD is a military organization that plans and implements various security issues relating to the country. In addition, it should be noted that the DoD did experimental work on a new blockchain-oriented supply chain management system which is supposed to improve the reliability of data as well as its traceability plus interoperability in connection with supplied goods and services exchange processes. Blockchain serves as a storage tool for the supply chain data and transaction exchange between the DoD and its partners and suppliers. Additionally, the system utilizes smart contracts for verifying, validating, and reconciling the supply chain outcome such as results[26].

d) Document Notarization and Digital Signatures

E-governance enables citizens to verify documents or contracts through document notarization and digital signatures online by declaring them valid and authentic. Anyway, traditional document notarization and digital signatures depend on centralized agencies or intermediate parties that issue certificates or seals that could be fake or compromised.
Blockchain Technology can deliver a distributed and confirmable document notarization and digital signature system that can eliminate the need for intermediaries or central authorities. Citizens could construct and sign official documents with digital identity, authenticated by the network of nodes through cryptographic proofs using blockchain technology. These documents exist in an immutable record on the blockchain and have timing stamps to confirm their integrity. Anyone with access to the blockchain can access the documents for verification.

As can be seen in Fig. 7, blockchain technology can be used to ensure clarity and security in government procurement processes. It represents how an administrator can upload a subscribed document and check it against the hash of the original document to authenticate its validity[27].

Some examples of blockchain-based document notarization and digital signature systems for e-governance include Estonia's KSI Blockchain, Chile's National Energy Commission, and South Korea's blockchain-based document notarization system.

Estonia's KSI Blockchain: Estonia leads the way in electronic governance through the adoption of the KSI blockchain designed for securing its digital infrastructures. The KSI Blockchain stores digital fingerprints or hashes of data, docs, or transactions in the form of electronic hash signatures created using blockchain technology. The hashes create proof of the existence, and integrity of data or documents in question, but do not disclose their content or identity. Many uses of the KSI Blockchain include securing such data including health records, tax records, court records, land registries, and e-residency certificates[28].

Chile's National Energy Commission: Energy data in Chile is currently being notarized using a blockchain-based system of record. The National Energy Commission (CNE) records its energy data on the blockchain utilizing blockchain technology. This data consists of such as installed capacity, average market prices, marginal cost, and hydrocarbon prices. On the blockchain, the truthfulness is confirmed through cryptographic proofs, while immutability and transparency of data are assured. The purpose of this system is to enhance secure, reliable, and approachable energy Information[29].

South Korea's blockchain-based document notarization system: South Korea is one of the developed countries with advanced electronic governance and digitization. As an example of this, South Korea has created a blockchain-based document notarization system to cut down on the costs associated with its document notarization as well as the errors and delays. Blockchain technology is used in the system to record and timestamp the documents which can only be verified by many nodes in the network. Digital signatures provide authenticity of all the records stored on the immutable and auditable blockchain generated by the system with public key cryptography[30].

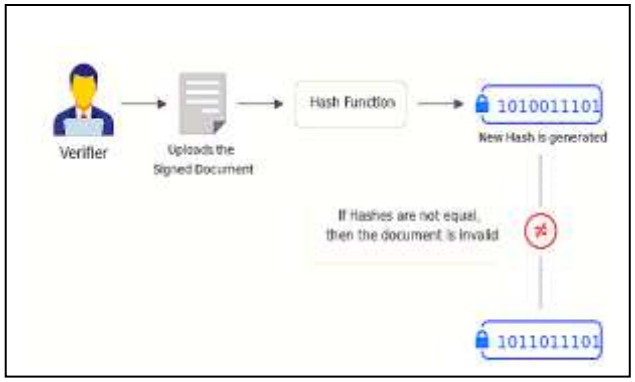

Fig. 7. Blockchain-based Document Authenticity and Validation Process

D. Data Security and Privacy

Information security has become a critical element of effective E-Governance since it entails safeguarding any data or transactions' secrecy, consistency, and availability within the e-governance system frameworks and platforms. Securing confidentiality of citizen's data and private information may help to build confidence among the citizens and relevant stakeholders in the e-governance initiatives; besides, such kind of actions will allow preventing or reducing possible consequences of cyber threats like cyberattacks, data leaks, identity fraud, The blockchain technology could significantly improve data security in e-governance since it possesses several capabilities and functionalities, including data encryption, immutability and access control that protects personal information rights.

Encryption involves changing and encoding the data in an illegible format, which only authorized entities can access and decrypt. It also includes data encryption that secures the data integrity and confidentiality of data and transactions besides preventing fraud and tampering. The blockchain network and platform utilizes several types of encryption mechanisms including symmetrical, asymmetrical, and functional cryptography. As an illustration, symmetric encryption utilizes one key called the secret key for encryption and decryption purposes. The asymmetric method applies to any type of data or transaction that makes use of two keys known as a public key and a private key. With homomorphic encryption algorithms, one could perform calculations on ciphertexts and encrypted transactions[31].

The feature of immutability refers to the fact that no one can change, delete, or amend any transaction information and data stored in the blockchain after recording and verification. This immutability also ensures that all the information presented in the system is legitimate and trustworthy while also preserving an incorruptible record that cannot be altered even at its source of creation. Using tools like hashing, digital signatures, and consensus algorithms, blockchain technology ensures the integrity and maintains the permanent record of the data and transactions contained in it. For instance, it is possible to implement hash functions to get specific and immutable identifiers called hashes that are responsible for verifying the uniqueness of data as well as the integrity of the transactions. The use of digital signatures provides a way in which to attach electronic signatures, built on the foundations of public-key cryptography, to the data and transactions to verify that it has come from a genuine source and is authentic. Consensus algorithms can be used to reach an agreement among various parties to agree to the state of the chain, the transactions, and the data involved in transactions[32].

Control of access is a system that ensures only those with approved identification and roles are allowed to interact, transact, or gain access to information in the blockchain network. The access control also makes the data and transactions available and usable, while protecting the privacy and preferences of the data owners and users. Several ways including public-key cryptography, and zero-knowledge proofs have also been implemented and enforced to access control on the blockchain. For example, public-key cryptography employs two different keys, which are a public one and a private one for encryption, and decryption, authenticating ZKP can prove the validity and correctness of the data and transactions without disclosing more sensitive information. Through multi-signature schemes, several participants may be required to agree to and approve predetermined transaction rules and transactions related to sensitive data.

Safety of data protection and privacy is an essential aspect as far as protecting classified state data like private person details, expenditure statistics, and legal documentation saved and processed in e-government systems is preferred. The sensitive government data could consist of highly important and secret material that might affect and impact the national or public concerns of the people and determine the policies that are applicable in a certain context. Thus, the secure and safe keeping of sensitive government data and prevention and control of cyberattacks, data breaches, and identity frauds to the integrity of the sensitive government data and consequently the trust and confidence placed in the e-governance services and functions by the citizens and stakeholders The security of the sensitive government data and respect for the rights and interests of the data owners and users include data encryption, immutability, and access control features enabled by blockchain technology.

Some examples of blockchain-based data protection systems for e-governance include European Union's DECODE Project and South Korea's ICONLOOP project.

European Union's DECODE Project: As part of its project on "DECODE", the European Union plans to educate people on how they can control their data, allowing them to choose who can access it. This project is based on blockchain solutions that will enable citizens to store their data in the form of blocks and give access rights over it to a third party through smart contracts. It employs zero-knowledge proofs for citizens to demonstrate their

attributes or credentials, but not expose their details or information about themselves[33].

South Korea's ICONLOOP project: The ICONLOOP project provides for secure and private COVID-19 contact tracing in South Korea. This project is powered by blockchain technology to develop a platform for providing citizens with digital certificates, documenting their COVID-19 tests, where this documentation is stored on the blockchain. The system employs a mobile phone app through which people can get themselves tested, obtain a QR code for the test result, and keep their identity secret while sharing the same with someone else. The system also employs zero-knowledge proof to guarantee that only the required information is revealed[34].

III. Analysis and Discussion

A. Challenges and Limitations

On the issues of security, transparency, efficiency, and innovation in e-government, blockchain technology proves to be valuable. However, blockchain Technology is associated with some issues and shortcomings that must be resolved for the broader use of e-governance. Some of those challenges and boundaries can be described as scalability, energy consumption, regulatory issues, interoperability, and adoption barriers.

Scalability: Scalability means that the system can support a greater number of transactions and users. The performance and functionality of the system should not be affected by this increase in workload. In addition, the decentralized and distributed nature makes every node store and process every transaction which has resulted in the scalability issue facing blockchain. The negative aspect of this system is that it results in high computing costs, low transaction speeds, and long waiting times when processing transactions. Various fixes have been suggested for improving scalability such as sharding, sidechains, state channels, and layer two protocols.

Energy consumption: The amount of energy that is consumed by a system to carry out its operation. Proof of Work, an implementation used in blockchain technology to verify transactions using complex mathematical calculations or proofs, is instead energy-consuming because nodes need it. These include huge environmental effects, massive expenses on operations as well as heavy resource consumption. Numerous solutions exist to decrease energy consumption in blockchain technology like proof-of-stake, proof-of-authority, proof-of-reputation, and proof-of-burn.

Regulatory issues: Legal and ethical considerations involve the questions concerning how the use of certain systems and technologies is acceptable in a particular context or field of application. Since blockchain is disrupting and innovative, it poses regulatory problems to contemporary laws, values, and organizations' governance. Among the issues are data protection, identity verification, jurisdiction, taxation, compliance, liability, and enforcement. Various approaches have been proposed to tackle the problem of regulating blockchain technology including self-regulation, co-regulation, standardization, certifications, or even enacting legislation.

Interoperability: Interoperability is the capability of different systems or technologies to exchange communication and information without encountering any barrier or constraint. However, different types, architectures, protocols, and standards, as well as multiple kinds of platforms of different blockchains make it difficult for blockchain technology to achieve interoperability. Such limitations render blockchain, as well as other systems or technology of e-governance, incompatible or not integrable with one another concerning other blockchains. There are several solution strategies for enhancing the interoperability of blockchain technology including cross-chain communication, atomic swaps, bridges, relays, and oracles.

Adoption barriers: The term refers to elements that inhibit or discourage the usage, adoption, or reception by the intended user or stakeholder of an innovation or technology. The adoption of blockchain technology is hindered by its complexity and ‘newness’ that needs technical expertise, skills, and even awareness to comprehend and utilize it. In particular, the e-government experience has encountered social and cultural hurdles involving the unwillingness of stakeholders such as citizens or staff to adopt new attitudes and behaviors regarding an upcoming system or technical innovation within e-governance. There are many suggested solutions for the barriers to adopting blockchain technology including education, training, awareness, incentivization, feedback, and active engagement.

TABLE II provides a concise overview of the strategies for addressing above mentioned blockchain challenges.

TABLE II. Strategies for Overcoming Blockchain Limitations

Challenge	**Solutions**
Scalability	Sharding, sidechains, state channels, and layer 2 protocols
Energy consumption	Proof-of-stake, proof-of-authority, proof-of-reputation, and proof-of-burn
Regulatory issues	Self-regulation, co-regulation, standardization, certification, and legislation
Interoperability	Cross-chain communication, atomic swaps, bridges, relays, and oracles
Adoption barriers	Education, training, awareness, incentives, feedback, and participation

B. Integration with Existing Systems

Blockchain technology could store the data in a secure, transparent, and decentralized way and verify it without any intermediate parties or central authority. However, blockchain technology can't fully substitute or replace existing e-governance systems. Instead of that, it could support these features adding more and more in number. So, it is necessary to merge blockchain technology with today's e-governance smoothly.

Integrating blockchain technology with existing e-governance systems involves several steps, as depicted in Fig. 8.

Identifying the use cases and requirements: The initial stage requires determining the e-governance use cases and needs that can benefit from blockchain technology. The use case and requirements for these systems should align with the goals and objectives of e-governance, addressing the existing system's limitations.

Choosing the type and architecture of blockchain: Thereafter, it wants to choose a suitable type and form of blockchain for the proposed use cases and needs. There are types of blockchain that involve three levels of access such as public, private, and consortium. Different protocols, standards, platforms, and frameworks may form the basis of the blockchain architecture providing distinct features or functionality.

Designing and developing the blockchain solution: In this case, a blockchain solution would be designed and developed with the capabilities of implementing the specified use cases and requirements. The blockchain solution needs elements like nodes, transactions, blocks, and consensus algorithms among others to interface with other systems such as smart contracts.

Testing and deploying the blockchain solution: In the fourth step, a test and deployment of the blockchain-based solution takes place by setting it up as a pilot project to examine how well it performs, works, and functions. Testing and deploying the system should involve taking part the stakeholders such as government agencies, service providers, citizens, and experts on whom feedback and improvement suggestions could be provided.

Monitoring and maintaining the blockchain solution: This involves monitoring and maintaining the whole blockchain solution to assure reliability, safety, and scalability of it. Therefore, the updates should include upgrading the software, hardware, as well as network components of the blockchain solution in response to the evolving needs of electronic governance.

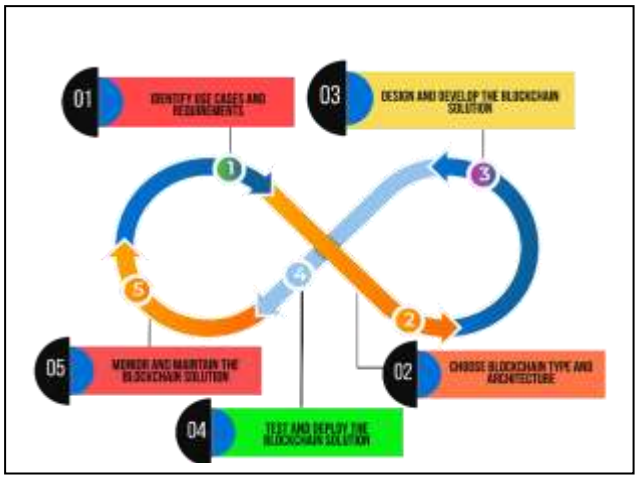

Fig. 8. Steps involved in integrating blockchain technology with existing e-governance systems

C. Future Directions and Emerging Technologies

E-Governance using blockchain technology can potentially revolutionize and redefine government-citizen interactions in the next generation, with new levels of efficiency, security, transparency, and innovation. However, blockchain technology continues to be dynamic in terms of concepts, technology, applications, and challenges. So, it is necessary to focus on the future paths and developing technologies in blockchain for e-governance.

Some of the future directions and emerging technologies in blockchain for e-governance include Decentralized Autonomous Organizations, Digital Identity Solutions, Novel Applications, and Interdisciplinary Collaborations.

Decentralized Autonomous Organizations (DAOs): These include rules coded into smart contracts as they reside on a blockchain, and form organizations known as Decentralized Autonomous Organizations (DAO). They can function autonomously and without any need for a human hierarchy. In this case, DAOs allow for novel governance models that may allow the public to take part in decision-making via tokens and/or ballots. DAOs can offer new types of service delivery, which result in cost decreases, reduced exposure or riskiness, and increased effectiveness[35].

Digital Identity Solutions: These are systems through which a user can build, and they can also control their own Digital Identity, which is verified through a network of nodes using cryptographic proofs. Identity solutions for the digital world can improve the safety and level of privacy of users' data, so as a result, they will be able to use different services online with no disclosure of their personal and sensitive information. Using ZKP(Zero-Knowledge-Proof), digital identity solutions may allow people to demonstrate their attributes or credentials without revealing their identity, or any other personal data.

Novel Applications: E-governance based on blockchain is a system of new applications for the creation of new services and improvement of existing ones. New areas like

healthcare, education, taxes, social services, environment may be covered by novel e-governance applications that apply to diverse sectors or domains. Other emerging technologies like AI, IoT, and Cloud computing can be used to improve their functionalities in novel application setups and functionalities.

Interdisciplinary Collaborations: Partnership is another characteristic of interdisciplinary collaboration, and it involves working together among individuals representing diverse disciplines on e-governance projects using technology in blockchain to address complex issues or generate new ideas. These interdisciplinary collaborations may bring on board different parties like government agencies involved, service providers, citizens' participation, researchers' contribution, and others who have knowledge, expertise, resources, and views aimed at achieving a shared goal. Such interdisciplinary collaborations may also promote learning, delivery of creative ideas, integration of diverse cultures, and cooperation among participating individuals.

IV. Conclusion

Blockchain technologies are new and radical inventions, which can radically transform ICT services. It presents a risk-free method of data storage that is open, uncensored and does not require any intermediaries or central agencies. E-governance is another area that makes use of blockchain technology such as identity management, voting systems, procurement, the document verifying, and protecting data among others. Such applications will improve the security, openness, and effectiveness of e-governance service provisioning as well as unveil opportunities for innovation and convergence. Nonetheless, blockchain has some constraints and challenges including scalability, energy consumption, regulation difficulties, Interoperability, and barriers limiting their adoption. Before this tool becomes widely accepted in e-government, several challenges and limitations must be resolved. It is possible to easily integrate blockchain technology with other e-governance systems in place. E-governance services are poised to move into a completely new security, transparency, efficiency, and initiative age with blockchain technology. Nevertheless, blockchain still has under development concepts, new technologies, applications, and problems that emerge with time. Thus, it becomes important to look forward to the future directions and evolving technologies of blockchain in e-governance.

V. References

[1] "Significance of e-Governance - Meaning, Importance & Evolution!," Testbook. Accessed: Nov. 20, 2023. [Online]. Available: https://testbook.com/ias-preparation/significance-of-e-governance

[2] "E-Governance: Meaning, Objectives, Features, and 4 Types."

[3] G. Ntulo, "E – GOVERNMENT: ITS ROLE, IMPORTANCE AND CHALLENGES".

[4] D. F. Malanga, "E-GOVERNMENT ADOPTION, IMPLEMENTATION, BENEFITS AND CHALLENGES: THE MALAWIAN EXPERIENCE".

[5] M. Alshehri and S. Drew, "Implementation of e-Government: Advantages and Challenges," *Conf. Proc.*.

[6] "E-Governance and its Significance -[UPSC Notes]." Accessed: Nov. 20, 2023. [Online]. Available: https://byjus.com/free-ias-prep/significance-of-e-governance/

[7] "Digital India Mission, 9 Pillars, Vision, Impact, Advantages." Accessed: Nov. 20, 2023. [Online]. Available: https://www.studyiq.com/articles/digital-india-mission/

[8] "United Nations E-Government Survey", doi: 10.18356/237d52b2-en.

[9] W. Li, M. He, and S. Haiquan, "An Overview of Blockchain Technology: Applications, Challenges and Future Trends," in *2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Beijing, China: IEEE, Jun. 2021, pp. 31–39. doi: 10.1109/ICEIEC51955.2021.9463842.

[10] S. Leible, S. Schlager, M. Schubotz, and B. Gipp, "A Review on Blockchain Technology and Blockchain Projects Fostering Open Science," *Front. Blockchain*, vol. 2, p. 16, Nov. 2019, doi: 10.3389/fbloc.2019.00016.

[11] "Blockchain across Oracle." Accessed: Nov. 11, 2023. [Online]. Available: https://subscription.packtpub.com/book/data/9781788474290/1/ch01lvl1sec13/how-does-a-blockchain-work

[12] "1. Fundamental Concepts of Blockchain - Hands-On Smart Contract Development with Hyperledger Fabric V2 [Book]." Accessed: Nov. 20, 2023. [Online]. Available: https://www.oreilly.com/library/view/hands-on-smart-contract/9781492086116/ch01.html

[13] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," in *2018 International Conference on Information Networking (ICOIN)*, Chiang Mai, Thailand: IEEE, Jan. 2018, pp. 473–475. doi: 10.1109/ICOIN.2018.8343163.

[14] M. Kumar, "Advancing Identity Management with Blockchain Technology," Oodles Blockchain. Accessed: Nov. 22, 2023. [Online]. Available: https://blockchain.oodles.io/blog/blockchain-identity-management-platform-development/

[15] C. Sullivan and E. Burger, "E-residency and blockchain," *Comput. Law Secur. Rev.*, vol. 33, no. 4, pp. 470–481, Aug. 2017, doi: 10.1016/j.clsr.2017.03.016.

[16] C. V. Priscilla and T. Devasena, "Aadhaar Identity System using Blockchain Technology," *Int. J. Comput. Appl.*, vol. 174, no. 26, pp. 27–32, Mar. 2021, doi: 10.5120/ijca2021921188.

[17] B. News, "Blockchain Adopted by Canadian Banks to Verify Client Identities - BNN Bloomberg," BNN. Accessed: Nov. 20, 2023. [Online]. Available: https://www.bnnbloomberg.ca/blockchain-adopted-by-canadian-banks-to-verify-client-identities-1.1251951

[18] C. Anwar Ul Hassan *et al.*, "A Liquid Democracy Enabled Blockchain-Based Electronic Voting System,"

Sci. Program., vol. 2022, pp. 1–10, Jan. 2022, doi: 10.1155/2022/1383007.
[19] "The world's first blockchain-powered elections have just happened in Sierra Leone," World Economic Forum. Accessed: Nov. 20, 2023. [Online]. Available: https://www.weforum.org/agenda/2018/03/the-world-s-first-blockchain-powered-elections-just-happened-in-sierra-leone/
[20] S. Das, "Moscow to Use Blockchain Tech in 'Active Citizen' Project," CCN.com. Accessed: Nov. 20, 2023. [Online]. Available: https://www.ccn.com/moscow-to-use-blockchain-in-active-citizen-project/
[21] N. Braun, "E-Voting: Switzerland's Projects and their Legal Framework – in a European Context".
[22] "South Korea Tests Blockchain-Based Voting, will Integrate into Online Voting if Successful - Asia Blockchain Review - Gateway to Blockchain in Asia." Accessed: Nov. 20, 2023. [Online]. Available: https://www.asiablockchainreview.com/south-korea-tests-blockchain-based-voting-will-integrate-into-online-voting-if-successful/
[23] S. Johar, N. Ahmad, W. Asher, H. Cruickshank, and A. Durrani, "Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey," *Appl. Sci.*, vol. 11, no. 14, p. 6252, Jul. 2021, doi: 10.3390/app11146252.
[24] J. Field, "World Food Program's 'Building Blocks' project wants to harness blockchain tech for humanitarian cooperation," CoinGeek. Accessed: Nov. 20, 2023. [Online]. Available: https://coingeek.com/world-food-program-building-blocks-project-wants-to-harness-blockchain-tech-for-humanitarian-cooperation/
[25] S. Khan, M. Shael, M. Majdalawieh, N. Nizamuddin, and M. Nicho, "Blockchain for Governments: The Case of the Dubai Government," *Sustainability*, vol. 14, no. 11, p. 6576, May 2022, doi: 10.3390/su14116576.
[26] S. B. Rahayu, N. J. Rmn, N. D. Kamarudin, and A. M. Azahari, "MILITARY BLOCKCHAIN FOR SUPPLY CHAIN MANAGEMENT," vol. 13, no. 1, 2019.
[27] "Blockchain Document Signing Platform: Offering Security to Confidential Documents – AnayMalpani." Accessed: Nov. 22, 2023. [Online]. Available: https://anaymalpani.wordpress.com/2019/09/01/blockchain-document-signing-platform-offering-security-to-confidential-documents/
[28] A. Karm, "Estonia – the Digital Republic Secured by Blockchain".
[29] "Chile's National Energy Commission Launches Ethereum-Based Pilot For Energy Data," Cointelegraph. Accessed: Nov. 20, 2023. [Online]. Available: https://cointelegraph.com/news/chiles-national-energy-commission-launches-ethereum-based-pilot-for-energy-data
[30] "South Korea's digital identity blockchain prepares to add new credentials, go international | Biometric Update." Accessed: Nov. 20, 2023. [Online]. Available: https://www.biometricupdate.com/202212/south-koreas-digital-identity-blockchain-prepares-to-add-new-credentials-go-international
[31] N. Elisa, L. Yang, F. Chao, and Y. Cao, "A framework of blockchain-based secure and privacy-preserving E-government system," *Wirel. Netw.*, vol. 29, no. 3, pp. 1005–1015, Apr. 2023, doi: 10.1007/s11276-018-1883-0.
[32] V. Wylde *et al.*, "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Comput. Sci.*, vol. 3, no. 2, p. 127, Mar. 2022, doi: 10.1007/s42979-022-01020-4.
[33] "Decentralised Citizens Owned Data Ecosystem | DECODE Project | Fact Sheet | H2020," CORDIS | European Commission. Accessed: Nov. 20, 2023. [Online]. Available: https://cordis.europa.eu/project/id/732546
[34] "Iconloop secures gov backing to test blockchain driver's license project," Cointelegraph. Accessed: Nov. 20, 2023. [Online]. Available: https://cointelegraph.com/news/iconloop-secures-gov-backing-to-test-blockchain-driver-s-license-project
[35] S. Hassan and P. De Filippi, "Decentralized Autonomous Organization," *Internet Policy Rev.*, vol. 10, no. 2, Apr. 2021, doi: 10.14763/2021.2.1556.