A Systematic Conceptual Review- Blockchain As A Next Generation E-Government Information Infrastructure

M.Madhu Rani[1] S.Valli Sneha[2] D.Hemanand[3] M.Kavitha[4]
Assistant Professor[1] Assistant Professor[2] Assistant Professor[3] Assistant
Professor[4]
Department of IT[1] Department of IT[2] Department of CSE[3] Department of
CSE[4]
Rajalakshmi Engineering Rajalakshmi Engineering Sriram Engineering Sriram
Engineering
College[1] College[2] College[3] College[4]
Chennai, Chennai Chennai Chennai

madhurani.m@rajalakshmi.edu.in[1] vallisneha.s@rajalakshmi.edu.in[2] hemanandd.cse@sriramec.edu.in [3]
kavitham.cse@sriramec.edu.in [4]

J Paul Rajasingh[5]
paulrajasingh@yahoo.co.in[5]
Assistant Professor(Sr.G)[5]
SRM Institute of Science and Technology[5]
Ramapuram,Chennai

Abstract

The most difficult E-government systems which needs to be open, distributed, secured and privacy-preserved. To deliver better government public services to the citizens, businesses, and employees effectively, efficiently and transparently, E- government uses information and communication technologies. The objective of this paper is to discuss the application of blockchain technology towards e-government. This theoretical paper explores the impact of blockchain technology on the evolution of e-government and public sector processes. To prevent fraud, and to establish trust in the public sector the blockchain technology records the transactions on decentralized distributed ledgers provide new opportunities for governments to improve transparency. The blockchain technology improves the privacy and information in which data are encrypted and distributed across the entire network. The adoption of blockchain based applications in e-Government is still very limited and there is a lack of experimental evidence according to results showed. This article discusses how blockchain technology can contribute to the development of e-government and public services and analyzes the framework, difficulties and challenges of applying blockchain to e-government at present. Security, scalability and flexibility are the primary technological aspects that are faced as challenges in blockchain adoption.

Keywords : Blockchain technology ,Decentralized systems,, Distributed ledger ,E-government systems, Applications.

1.INTRODUCTION

The implementation of the e-government can improve the efficiency of the current Paper based system. Now a day the world is moving in the direction of the mobile connections which makes for an e-government services to be easily accessible to every citizen irrespective of location all over the country. By the use of new technologies by governments, Innovations and transformations across many aspects of the public sector can be driven. The public sector is improved by the use of information technologies (IT) that was often captured by the label of e- Government. The Knowledge epoch is how the tremendous benefit of an e-government service as we live in what is now termed as in many countries around the world to reduce costs, to improve public services, to save time and to increase effectiveness and efficiency in the public open sector, E -government has become more popular and most of the governments have introduced and implemented e-government systems. Escaping long queues in public offices as saving time the E-government users enjoy the online services without leaving the comfort of their homes, and transportation costs, and also the service providers can deliver services more effectively and efficiently without any problems. The websites and electronic identity management systems (E-IDs), voting management are some of the existing e-government systems that are centralized at duplicated servers and databases. A single point of failure from the centralized management systems can make the system a target to cyber attacks such as malware, denial of service attacks (DoS), and distributed denial of service attacks (DDoS). The central banking platforms and other use cases including business process improvement, trades, health information sharing, automotive ownership, and voting would be replaced by blockchain.

A distributed ledger, also known as blockchains are used instead of single centralized database of transaction records, it uses a peer-to-peer decentralized network to create a shared distributed digital ledger that keeps an irreversible record of each transaction. Without any single point of vulnerability, it is an open, distributed, communal, transparent system. Data integrity, data quality, transparency, fraud prevention, reducing corruption, and enhancing trust, security, and privacy are the potential benefits of Blockchain in e-government. The attention of governments in many countries was attracted due to the potential benefits to improve transparency and to eliminate corruption. By the improvement of the delivery of public services and by increasing trust in public sectors the blockchain becomes more necessary for the efficiency of government operations, also the blockchain has come up as the company's and government's support for the exchange of information and transaction that requires trust and authentication for potentially disruptive and general-purpose technology. Basically, a distributed ledger that is shared among the nodes present in a network, used to record transactions that are verified by a consensus mechanism that creates trust in the network is called the blockchain. Each transaction is validated by a network of nodes, hence after a record is verified and stored, all the changes are immediately reflected in all copies of the ledger across the network and it will be very difficult to manipulate data on the blockchain, as they are linked with the previous transaction. so, the distributed ledger ensures the traceability of transactions and provides an immutable record.

To make the governments smarter secure, transparent, distributed, open, and inexpensive database technology the decentralized blockchain technology comes into use, the benefits provided by e-government include efficiency, improved services, better accessibility of public services, and more transparency and accountability. For the core governmental activities such as digital ID management and secure recordkeeping and document-handling the blockchain technology looks primarily suitable. The transactional data such as the ownership of land registry, birth and marriage certificates, vehicle registries, business licenses, educational certificates, student loans, social benefits and votes are some of the typical informations stored in a blockchain. The adoption of new technologies is improving the public services delivery for government organizations. The blockchain technology provides a high level of security and also the administration based blockchain offers the document management to be much simpler.

The specific aim of this paper is to discuss the outline of a decentralized e-government system using the blockchain technology, which can ensure both information security and privacy while synchronously increasing the trust of the public sectors, with the support of a theoretical and qualitative analysis of the security and privacy implications of such system.

The structure of rest of the paper is arranged as follows; Section 2 & 3 where the theoretical technological foundations concerning blockchain technology and some current applications are discussed, Section 4 explores the potential benefits of blockchain for the e-government's information and infrastructure perspective as well as presenting its implications. In Section 5 & 6, we discuss the challenges towards interesting applications of the technology and Section 7 concludes the discussions.

2.The Background -Blockchain Technology

The two researchers Stuart chemist and W. Scott Stornetta made public a system for wherever the tampering of document timestamps couldn’t be done. However, it wasn’t happening virtually untill 20 years later. The launch of Bitcoin in Jan 2009 was how the blockchain started its initial real-world application. The Bitcoin protocol is made on the blockchain. The digital currency Bitcoin is introduced in a very analysis paper Bitcoin's pseudonymous creator Satoshi Nakamoto printed it as "A new electronic money system that's absolutely peer-to-peer, with no trusty third party." Afterward, exploit blockchain in several alternative sorts of electronic cash referred to as cryptocurrencies are created and at a similar time, the blockchain is developed for various applications to implement alternative situations on the far side cryptocurrencies over the years.

A distributed ledger that is shared among participating parties in a network, used to record transactions that are verified by a consensus mechanism that creates trust in the network is the blockchain. As the name suggests, a blockchain is a series of immutable and cryptographically secured tamper-proof blocks that are chained together with complex computational algorithms. Each block records a set of transactions and its associated metadata. The consensus mechanism creates trust in the network of nodes by validating every transactions.A blockchain contains a set of blocks, the block is made up of the block header and every block contains a hash of the previous block header and the merkle tree root. A newly created block is appended to an existing chain of blocks. This chain of blocks is predominantly a *linked list* which associates one block with the other. The initial block of any such list is a *genesis block*. Genesis block is a special block that is numbered zero and is hard-coded in the blockchain application. Hence,a blockchain grows by appending new blocks to the present chain. The blockchain technology does not require an intermediary or trusted third party as it is decentralized and distributed. The blockchain participants have private keys assigned to them to digitally sign and validate the transactions they make.

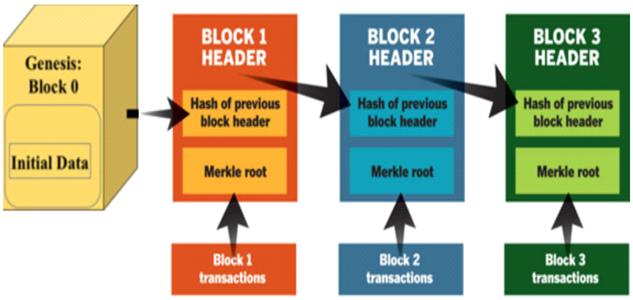


Fig.1. Blocks in Blockchain representations

The block header typically contains the timestamp, nonce, version and proof of difficulty. The timestamp indicates the time that the block was created the nonce is a random number generated by the consensus algorithm to compute the hash value of a block.

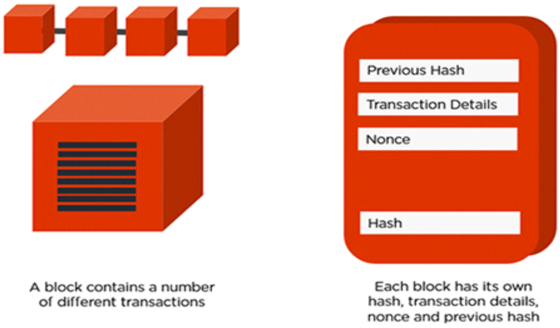

Previous Hash
Transaction Details
Nonce
Hash
A block contains a number of different transactions
Each block has its own hash, transaction details, nonce and previous hash

Fig.2. A Block

2.1 KEY ELEMENTS OF BLOCKCHAIN

Distributed ledger

The blockchain is a distributed database that does not need a central authority and it eliminates the need for third party verification. Every node in a blockchain network keeps a copy of the transaction to avoid having a centralized authority. The distributed ledger has access to all network participants. The transactions are recorded only once in this shared ledger.

Immutable Records

The shared ledger cannot be changed or tampered by any participant after the transaction is recorded.

Smart contracts

Smart contracts are computer protocols (set of rules), that provide the facility to directly track and accomplish complex agreements between parties without human interaction. A smart contract can define conditions, such as the corporate define conditions using smart contract for bond transfers, include the terms such as travel insurance, medical insurance etc.,

Consensus Mechanisms

The consensus mechanism validates every transaction in the public ledger. The consensus algorithm guarantees the reliability of the transactions in the ledger and allows to maintain and update the ledger. Consensus algorithms needs to be dependent. There is various consensus algorithm are used in blockchain, some of them include Proof-of-Work, Proof-of-Stake, Proof-of-Authority, Delegated Proof of stake (DPoS), Practical Byzantine Fault Tolerance (PBFT)and Proof of difficulty (PoD) etc.,
Bitcoin works the PoW whilst Ethereum and Bitshare works PoS and DPoS, correspondingly.

In PoW system, to add a new block to the blockchain network computers must first solve a complex computational math problem which requires great computational power. The process of adding new blocks is mining and the computers which solves the puzzle is known as miners. The miners are rewarded in bitcoins. To solve complex math problems, the computer must run programs that cost them large amount of energy and power. The blockchain network is chosen deterministically depending on its stake for the Pos system to add a new block in the block in it. The energy required in PoW to solve the mathematical puzzle, is saved and provided by Pos, and to validate the new transactions and blocks only the wealth of a node is required. DPoS validates the blocks using panel of limited trusted delegates who will witness, real time voting and reputation system. To protect the authenticity of a transactions the functionalities of cryptographic hashing and asymmetric encryption are used to.

Hashing: A cryptographic secure hash function (e.g., SHA-256), maps at random an arbitrary-length binary input to a unique fixed-length binary output image. Also, the probability to generate the same output for any two different inputs is negligible.

Asymmetric Key: Cryptography keys consist of two keys – Private key and Public key, each node in the blockchain network generates a pair of private and public keys. The private key is associated with a digital signature function, which outputs a fixed-length signature string for any arbitrary length input message. The public key is associated with a verification function, which takes as input the same message and the acclaimed signature for that message. The verification function only returns true when the signature is generated by the signature function with the corresponding private key and the input message.

2.2 General key characteristics of Blockchain

A Decentralization- A decentralized scheme in which no central authority dictates the rules. Every node in the network can validate transitioned as it has identical copy of the ledger. This Decentralization mechanism affects the transactions in a way tolerant, data consistency, higher user control, attack resistance, transparency and it also avoids third-party intermediaries.

B. Persistency -The consensus mechanism, a cryptographic hash function and a timestamp does not allow invalid transactions functionalities of cryptographic hashing and asymmetric encryption hence it becomes impossible to edit, delete or copy transactions that are already recorded in the blockchain. These characteristics provide immutable records, data consistency and fraud protection,

C. Anonymity – cryptography public-key are used to take place interactions between two parties. These characteristics protects privacy of the user.

D. Auditability. The blockchain transactions are stored in chronological order, including the hash of the current transaction which is used to connect the next block when added and the hash of previous block, these helps to verify and track the characteristics transactions easily.

3.BLOCKCHAIN DESIGN PERSPECTIVE

A. Public Blockchain Networks

In a Public blockchain anyone can join and participate in, if all the nodes have same resources, then each node has equal probability of creating a block such as in Bitcoin. Substantial computational power required, little or no privacy for transactions and week security are some of the drawbacks included. These are important for enterprise use cases of blockchain.

B.Private Blockchain

In a Private Blockchain , only some nodes are allowed to be part of the consensus process, and the next block can be generated by only using those subset of the nodes . These systems could be utilized at a banking organization where the employees are only permitted to commit the results by creating a block whereas it only allows its customers to participate in the consensus. Depending on the Use cases, this can significantly improve the trust and confidence between participants.

C.Permissioned Blockchain

Permissioned blockchain can be organized as private blockchain and public blockchain. It restricts the participants in the network only in certain transactions. The participants need to obtain a permission to join. Businesses that usually set up a private blockchain, are generally a form of permissioned blockchain network.

D.Consortium Blockchain

Multiple organizations can share the responsibilities of maintaining a blockchain. A consortium blockchain is ideal for business when all participants are needed to be given permission and have a shared responsibility for the blockchain. Government decides the type of blockchain since every type has benefits and trade-offs. The key design decisions are data ownership, privacy, Control and access. Serious privacy problems might occur if all the information can be viewed by others in an open blockchain, e.g. health, personal or other sensitive information. The access is granted only when the conditions set by the data protection act are satisfying, and this requires encryption and access control to the distributed ledger. For example, the European General Data Protection Regulation (GDPR) requires that users should be provided the rights to be able to view their data, to change or even to remove data their data. A consortium consensus model is a closed blockchain where limited number of nodes are to be involved in the consensus mechanism and do not require a token or currency because the security is controlled by the consortium governing blockchain. For example, if a citizen wants to update their data, only the citizen and the involved public organization (often the municipality) are needed to agree to make the change.

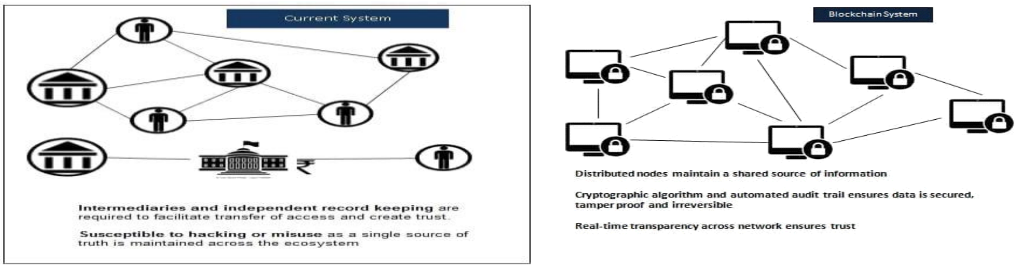
Table 1. Analysis of Performance and characteristics of various Blockchain

Principle	**Bitcoin**	**Ethereum**	**Stellar**	**IPFS**	**Blockstack**	**Hashgraph**
Consistency	Block verifications. 30-60 minutes	Block verifications. 20-60 minutes	Single block verification. Less than 1 minute	P2P mirroring. Limited primarily by network I/O. Several seconds for files less than 128KB.	Block verifications. 30-60 minutes	Consensus with probability one; Byzantine agreement, but attacker must control less than one-third
System Availability Virtual	Block verifications. 30-60	Block verifications. 20-60 minutes	Single block verification. Less than 1	Single storage request	Block verifications. 30-60 minutes	DoS resistant w/o proof-ofwork,

voting;	minutes		minute.	response. Several seconds for files less than 128KB		fast gossip
Failure Tolerance	Longest chain wins	Longest chain Wins	Last balloted block always has consensus.	Content address hash. Highly resilient against network partitioning	Longest chain wins	Strong Byzantine fault Tolerance
Latency	Block verifications. 30-60 minutes	Block verifications. 20-60 minutes	Single block verification. Less than 1 minute.	Single storage request response. Several seconds for files less than 128KB.	Block verifications. 30-60 minutes	Virtual voting; limited only by exponentially fast gossip protocol
Scalability	Block size. 7transactions per second	Block size. 7-20 transactions per second	Thousands to tens of thousands oftransactions per second	Thousands to tens of thousands of transactions per second. Scales linearly as nodes are added.	Block size. 7 transactions per second	Thousands to tens of thousands of transactions per second. Limited by bandwidth only
Auditability	Full	Full	Full	Difficult	Full	Configurable

4.METHODS -BLOCKCHAIN IMPLICATIONS FOR GOVERNMENT

Blockchain experiments are geared up globally in the public sector. By the use of new technologies by governments, innovations and transformations across many aspects of the public sector can be driven. The direct interaction between government and citizens, businesses and providing administration without the central governmental administrator can be facilitated by the distributed blockchain technology. Blockchain implements a wide range of processes for asset registry, inventory, and information exchange, both hard assets like physical property, and subtle assets like votes, patents, ideas, reputation, intention, health data, information etc. The diversity of government blockchain applications are vast in nature and include digital identity, the storing of judicial decisions, financing of school buildings and tracing money, marital status, e-voting, business licenses, passports, criminal records and even tax records. Among the categorizations of e-government some categories are: Government to Government, Government to Business, Government to Employees, Government-to-citizen etc., The democratic process, like e-voting is a type of Government-to-citizen relationship. The US Government’s use Government-Business,Government-Employee and Government-Government categories. Federal government business opportunities, FedBizOpps, provides Government to Business access. National Environmental Information Exchange Network used for communications among Utilization of e-government services is the category of Government-Government blockchain. . An example for Government to Employees relationship is the Employee Express where federal employees can control their savings and health benefits accounts online.



Intermediaries and independent record keeping are required to facilitate transfer of access and create trust.

Susceptible to hacking or misuse as a single source of truth is maintained across the ecosystem

Distributed nodes maintain a shared source of information

Cryptographic algorithm and automated audit trail ensures data is secured, tamper proof and irreversible

Real-time transparency across network ensures trust

Fig.4.Current System vs Blockchain based system

4.1 Diffusion of Innovation

The diffusion of innovation (DOI) concept discussess how an idea, product, or service is adopted through a system over time. In general, the diffusion of innovation are based on the number of users who have successfully adopted the technology and it can be by a number of factors including network effects,cost, technical complexity, technical compatibility, trialability, perceived needs of relative advantage. Adoption of e-government improve mutual trust between government, enterprises and citizens and built a next generation open-operation platform based on blockchain technology.

4.2 Discussion-Adoption of Blockchain Technology and Digital innovation in Public Sector

The government of Estonia implemented Keyless Signature Infrastructure (KSI) to secure all data. All Estonian citizen's health records are managed using KSI technology. The KSI technology takes up larger amount of data and creates smaller unique hash values and it allows only the authorized admins to monitor changes within databases, such as who can change the records, what changes are required, how the changes are implemented, when the records can be changed, and thus any unauthorized is impossible to tamper the records. For digitalizing the registration of land, property, vehicle, and other documents transactions, many countries and states such as Sweden, Ghana, and Georgia in USA are exploring Blockchain-based Asset registers. Sweden, Ghana and Dubai have adopted blockchain to record all real estate contracts, including lease registrations and the land registry copies are shared among all relevant parties to facilitate property purchases with each step of the sale being verified and recorded on the blockchain. Blockchain based registration system provides transparency across the system. It reduces the occurrence of fraud, and save time and cost in the registration process.

Digital voting via the Blockchain technology is gaining popularity and the Australian government unveiled that it will conduct election digitally. Voting, is a critical and authentic conceding public function. Citizens can cast their votes securely, validate their votes and even verify the election results. Digital identity management is required for identifying the voter. Digital voting via the blockchain technology reduce costs and improve efficiency of election. The educational institues are also using the using blockchain based Academic certificate recording system for eg; The Ministry for Education and Employment of Malta graduates, 100 digital diplomas by the Massachusetts Institute of Technology (MIT), The University of Melbourn store and share academic credentials using blockchain based mobile app that clearly demonstrates the use of technology to secure student records and sharing that data between agreed upon parties and the reliance of government institutions on blockchain for tamper-proof record-keeping of digital certificates. Dubai is functioning on flying taxis, self-driving vehicles, literal "Robocop's." an initiative called "Smart City" is aimed to run all government transactions on the blockchain by 2020. The Government of India launched Digital India campaign and the need for large scale adoption of exponential technologies is growing. The Digital India focusing on digital empowerment of citizens for providing digital services and implementing e-governance using technology as a transformation driver. NITI Aayog is the country's largest blockchain network - IndiaChain, offers to speed up enforcement of contracts, reduce frauds and increase transparency of transactions. Advisory committees have been set up such as Securities and Exchange Board of India (SEBI) has been established for conducting research on the blockchain platform. Development and Research in Banking Technology (IDRBT), a research Institute of the Reserve Bank of India, also exploring the applicability of blockchain in Indian Banking and Financial Services industry. The government of Andhra Pradesh is implementing blockchain in two departments; land registry and transport. The state has also situated a repository of use cases for global start-ups, through this initiative, the state prevents tampering of land records, and digitized which have been placed online. Telangana has begun to use blockchain technology for land registration while Maharashtra and Gujarat are also holding discussions to promote blockchain based start-ups and set up a Fintech Hub.

4.3 MIGRATING GOVERNMENT PROCESS TO BLOCKCHAIN

4.3.1Voting

The election frauds and the increase in the number of voters are some of the potential of the blockchain based voting system , as it was tested in the Nov 2018 midterm elections in West Virginia. Each vote would be stored as a block. The transparency in the election process can be mainted by the blockchain technology, making it impossible to tamper the votes, and it can provide instant results. A valued transaction of casting a vote is in focal point of New York, Texas, Denmark, Estonia, Ukraine, South Korea, and Australia. In India, Electronic Voting Machines (EVM's), are used to conduct elections and its vulnerability is a risk for democracy. The major issue lying here is the transparency of the process and security of the data.

A key is given to each voter as his vote. The key shall open on the Election Day which is connected with a smart contract. The votes shall be recorded as a transaction on the blockchain, it validates the transactions and seals the blocks. The data would reduce the discrepancies a its time stamped and verified constantly. A blockchain based approach is more transparent than the current ballot system as it could increase efficiency of transaction processing and prevent fraud.

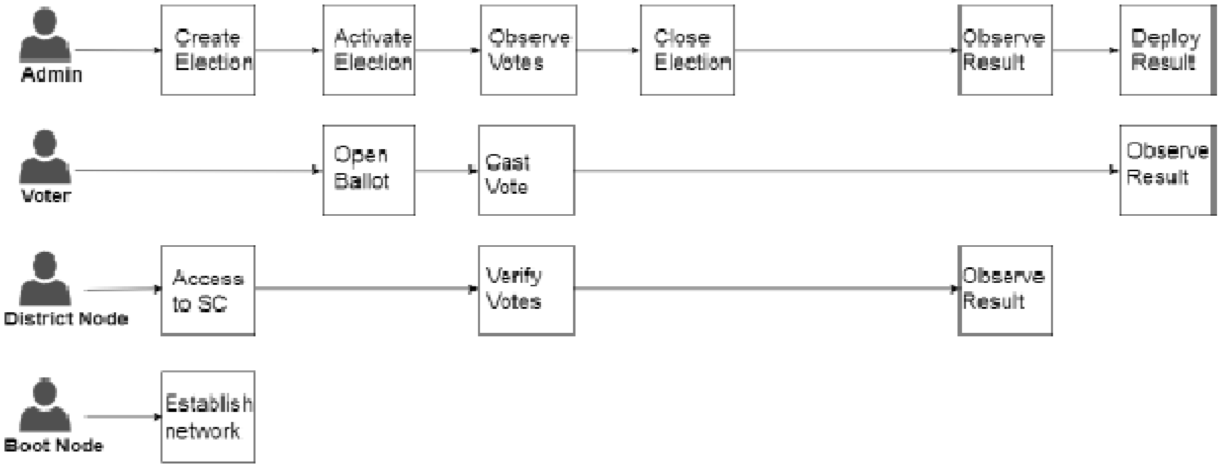


Fig.5. Blockchain based Voting system

4.3.2 Asset Registration

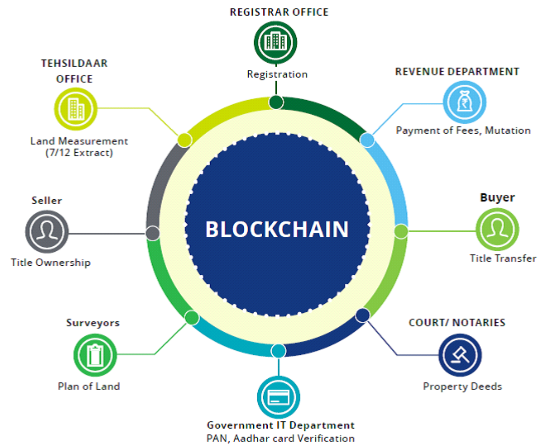
Blockchain usage in land registration is being explored across the globe the governments. Indian Government Currently registers, validates and maintains land details manually in paper-based format across various departments within the local Municipal Corporations, Registrars, Tehsildar's office, Gram Panchayats etc; which leads to high degree of latency and inaccuracy of information. Usage of Blockchain can be futuristic for the land registrations and record keeping considering its current issues. Many countries are experimenting with blockchain to digitize their land records. A blockchain securing a unique and non-corruptible record with respect to the accuracy of data, updation of records only with majority consensus and its time stamping will solve the problem. The status of that record across owners, reliable land record can be created in a secured, immutable and tamperproof manner and the changes are validated.

.

Table 2. Challenges in Land Registration Infrastructure

Intermediary	Multiple validations across departments results in high degree of intermediation, increased latency and inaccuracy of information.
Transperancy	Real-time visibility into the state of a land registry can help improve end customer experience.
Information storage	Across all the parties involved status of land registry and associated information must be consistent. However, different information is stored across different participants and thus the need for a centralized/decentralized repository
Trust	Citizens do not trust each other for title transfer and hence the government bodies are involved for authentication and verification. Also all documents are manually verified resulting in error or fraudulence.
Time sensitivity	The time to validate and verify at every level is elevated.
Manual Processing	Reporting and documentation are performed manually today which can lead to error,more time and high cost of operation.
Scalability	Land registry/transfer is a sequential process where documents are processed and verified manually in paper-based format.
Authentication	All paper-based and requires manual verification of documents at every level to ensure authenticity and reduce frauds.
Data security	Land registry data need to be open source to ensure asset transfer among citizens, however, data security must be ensured to prevent counterfeiting and theft. Data

A blockchain based Registration system brings more robust and digitization to the entire process, as it connects all stakeholders on a single platform which provides transparency, automated verification and irreversible trail of title transfer; thus everything is faster, secure and its a cheaper mode of asset registry maintenance due to the usage of blockchain. To ease the process and reduce the need for physical documentation, Maharashtra Revenue Department initiated online transformation in 73 talukas of 5 districts.

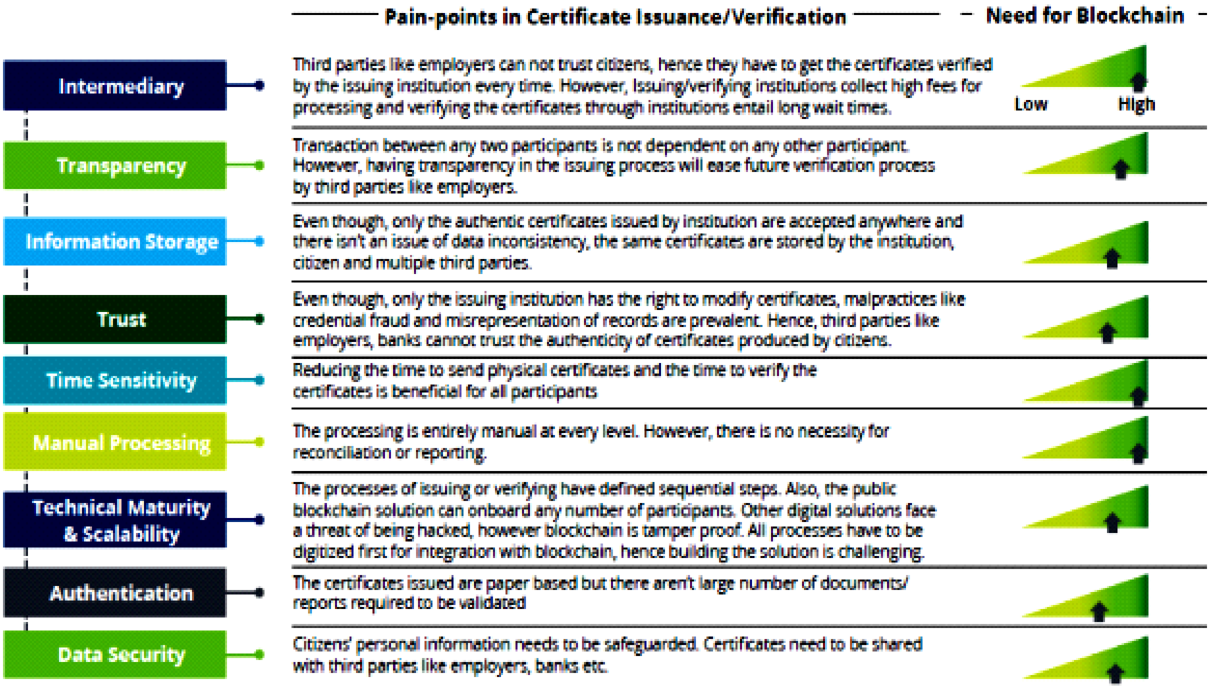


Source: Deloitte analysis

Fig.6. Blockchain based Asset Registration system

4.3.3 Digital certificates

Digital certificates, are electronic cards or digital equivalents of existing identity cards, to interact with websites, e-commerce portals, banking sites, government agencies, etc., The certificates, birth certificates and other important certificates for the retrieval of them securely and independently anywhere from the globe are stored digitally in the blockchain technology. Many institutions and organizations have realized the potential of blockchain and are embracing the technology for storing various kinds of certificates.



	Pain-points in Certificate Issuance/Verification	Need for Blockchain
Intermediary	Third parties like employers can not trust citizens, hence they have to get the certificates verified by the issuing institution every time. However, Issuing/verifying institutions collect high fees for processing and verifying the certificates through institutions entail long wait times.	Low High
Transparency	Transaction between any two participants is not dependent on any other participant. However, having transparency in the issuing process will ease future verification process by third parties like employers.	
Information Storage	Even though, only the authentic certificates issued by institution are accepted anywhere and there isn't an issue of data inconsistency, the same certificates are stored by the institution, citizen and multiple third parties.	
Trust	Even though, only the issuing institution has the right to modify certificates, malpractices like credential fraud and misrepresentation of records are prevalent. Hence, third parties like employers, banks cannot trust the authenticity of certificates produced by citizens.	
Time Sensitivity	Reducing the time to send physical certificates and the time to verify the certificates is beneficial for all participants	
Manual Processing	The processing is entirely manual at every level. However, there is no necessity for reconciliation or reporting.	
Technical Maturity & Scalability	The processes of issuing or verifying have defined sequential steps. Also, the public blockchain solution can onboard any number of participants. Other digital solutions face a threat of being hacked, however blockchain is tamper proof. All processes have to be digitized first for integration with blockchain, hence building the solution is challenging.	
Authentication	The certificates issued are paper based but there aren't large number of documents/ reports required to be validated	
Data Security	Citizens' personal information needs to be safeguarded. Certificates need to be shared with third parties like employers, banks etc.	

Fig.7.Blockchain based Digital certificates

4.3.4 Agricultural in Blockchain

Knowledge in the key areas that can contribute to the economic and environmental needs of the country are increasing due to the Leading entrepreneurial researchers in the Government of New Zealand. The Blockchain targeted at the agriculture sector are bringing digital revolutions by leveraging emerging technology such as to provide food products with solid provenance, which will enable consumers to determine where a food item is produced, its freshness, safety and quality.

4.3.5 Gross Settlement System

Current real-time gross settlement (RTGS) system replaces for future demands. Through the use of distributed ledger /blockchain the following strategic RTGS requirements are addressed and it enhances security.

- changing structure of the current financial system,
- users want more resilient and simpler pathways for their payments,
- remain highly resilient to the increasingly dissimilar range of threats to continuity of service,
- support the future evolution of regulatory and monetary policy tools.

4.3.6 Blockchain-as-a-Service for Public Sector

Digital Marketplace is a distributed ledger or blockchain service provider that are working to provide Blockchain-as-a-service to collaborate government with credits on the Government Digital Services'. Digital Marketplace is where the Government's official platform for public agencies to access cloud and digital services.This initiative will all be able to take advantage of Credits'platform to build applications and services on a Blockchain in central and state government, health, education, emergency services, defence, etc. Digital Marketplace based on Blockchain provides some flexibility in accessing the service public agencies. Public sector organizations can buy services without needing to run a full tender or competition procurement process based on the framework agreements signed with suppliers of services on the Digital Market. Blockchain-based systems can address the existing challenges that access to Credit's Blockchain platforms–as-a-service will allow the public agencies to establish provenance, authentication service participants, reconciliation of transactions service in addition to seamless and secure interoperability with legacy.

4.3.7 Identity management

A definite need for better online identity management is a secure identity.Identity management is the ability to verify your identity during online financial transactions for instance, in the sharing economy. Development of digital identity standards is proving to be a highly complex process. The SSL certificate (the little green lock) for secure transactions on the web is used currently on the internet for an E-Commerce, Netki is the startup that creates an SSL standard for the blockchain.

4.3.8 AML and KYC in Blockchain

Anti-money laundering (AML) and know your customer (KYC) practices , a strong potential for being adapted to the blockchain. A labor-intensive multi-step process for each new customer must be performed in the current financial institutions. The cross-institution reduces the cost of KYC through client verification and also increase monitoring and analysis effectiveness. AML/KYC has the solution Startup Polycoin that involves analyzing transactions, these transactions are forwarded on to acquiescence officers identified as being apprehensive. Tradle is another startup which is developing an application called Trust in Motion (TiM) considered as an "Instagram for KYC" that allows customers to take a snapshot of key documents such as passport, utility bill, etc., after the verification of the consensus this data is cryptographically stored on the blockchain .

5. Challenges of Blockchain adoption

In spite of the plentiful benefits and application areas of blockchain technologies in government, this literature also presents various challenges that need to be addressed. In this section we identify the challenges crossed in adopting blockchain technology for e-Government systems. Scalability, usability, interoperability, computational efficiency and storage size are some of the challenges that are highlighted in the selected articles. The scalability is the first and major issue related to its adoption and to improve scalability issues by providing techniques in consensus protocols that significantly reduce transaction time and computer power requirements. Though transaction networks are capable of processing thousands of transactions per second without any failure, when it comes to Bitcoin roughly, 3 to 7 transactions per second, and Ethereum takes 15 to 20 transactions. Making the Blockchain unviable for large-scale applications there is a remarkable slowdown in processing the transactions. The Security challenges is another issue which is a trade-off between security and performance. The adoption of blockchain should be beneficial in to public services and must be identified carefully and should be advanced than the cost of developing and running the system. Another issue that needs to be addressed is Interoperability, as this is one of the many reasons why organizations are still not adopting this technology. Most of the blockchains work in silos, hence do not communicate with other peer networks as they are incapable of sending and receiving information from another blockchain-based system. The most important challenges from an organizational point of view is the need for new governance models. The issues of acceptability are identified as the most important challenges. The blockchain platform requires the cooperation of multiple institutions and stakeholders hence a new governance model is required. The implications, trust, and auditing of blockchain applications are the other challenges that needs to be considered. The lack of standardization arises issues such as increased costs, interoperability and difficult mechanisms, making mass adoption an impossible task. Blockchain technology is acting as a barrier for the entry of new developers and investors as it does not follow a standard version. Well apart from the challenges mentioned the other challenging factors for large scale implementations are cost, security, and privacy.

Table 3: Challenges of blockchain adoption

Aspects	Challenges
Technological	Security Scalability Usability Interoperability/Compatibility Reliability Flexibility Cost effectiveness Computation efficiency General application platform Storage size Immaturity Design variables
Organisational	Organisational readiness Acceptability Business model/ Organizational transformation Risk of error for complex New governance model Implications Trust Auditing
Environmental	Laws and regulations support Support infrastructure Accessibility

6. Security And Privacy Analysis

The confidentiality, integrity and availability of the services must be a guarantee provided by every e-government system. Confidentiality is achieved when information is not disclosed to unauthorized users by, by protecting information from any form of modification; integrity is achieved, whilst availability means information is available when needed and is free from DoS or DDoS or other similar service disruption. This section provides a theoretical qualitative analysis on the security and privacy performance of the blockchain based e-government system.

The public key cryptography that protects against adversarial attempts to alteration and/or unauthorized access records, stores and secures the proposed system, whilst network users are assigned with private keys for validating and signing transactions. To ensure security, privacy and access control to the stored records encryption and digital signature are used in the network. Moreover, to control at least 51% of the network peers in order to alter a record, most of the blockchain consensus algorithms like DPoS require an attacker. which is generally impossible to archieve. More precisely, an attacker has to modify every copy of that block in the network and then convince most of the nodes that the new block is the valid one, in order to change any block in the blockchain. Also, all user's blocks are hashed and an incomprehensible hashes of the transactions are stored in the blockchain to increase the privacy of the data stored in the proposed network. The security of privacy sensitive data and the security of distributed networks can be potentially improved by the blockchain. For example, PKIs are usual public key infrastructures that are frequently at risk to single point of failure due to the hardware and software flaws or malicious attacks. A privacy-aware PKI is constructed by blockchain while simultaneously improving the reliability of conventional PKIs Privacy protection. Additionally various mobile services and social network providers are collecting our sensitive data which increasing risk of the publicity of our private data to malwares.For example, Facebook has collected more than 300 petabytes of personal data Usually, the collected data are stored on central servers of service providers, which are susceptible to malicious attacks. Blockchain has the potential to propose a decentralised personal data management system that ensures the user ownership of their data and to improve the security of privacy sensitive data. This system is implemented on the blockchain which protect the data against some privacy issues such as data transparency and auditability, data ownership, and access control.

7. Conclusion And Future Work

Blockchain technology is an innovative, general purpose technology, that offers a new ways of organization in many domains.It also offers prospective benefits in the domain of e-government. The technological revolution geared by blockchain will enable government leaders to increase security, improve process management, and make more efficient transactions. The trade-offs of this emerging technology are required to be understood by the government administrations. In this study work, we have surveyed blockchain usage in different areas including Voting, digital certificates, asset registrations, agriculture, identity management and public service based applications. A timely summary for entities with an interest in blockchain technology is presented in our paper. Furthermore, the discussion will motivate many more domains about the applications of blockchain. This study paper shows an organization of opportunities for blockchain application and implementation within government enterprises, with a possibile approach in suggesting deployment details. By means of interdisciplinary research the government needs to explore the implications towards blockchain applications. The proposed framework will assist to assess the feasibility of pursuing blockchain projects highlight the opportunities to transform public service delivery. Finally, it presents a call for more research on Blockchain and government, especially as it relates to governance and the regulatory framework insights on how to best control block chain technology to improve outcomes and productivity. More intensive research in this area is still necessary to advance the maturity of this field of research. Particularly, to study the various potential benefits of blockchain adoption empirical studies using rigorous research protocols should be enforced in government context. The reliability, clarity, the validity, and limitations of the advantages and potential benefits of blockchain technology in e-government will increase by experimental studies. Blockchains have also been used in education, healthcare, logistics, real estate industry, transportation, charity, and food supply chain. A future direction is to include these applications in a more detailed empirical survey.

REFERENCES

[1]. Al Awadhi & Morris (2009). Factors influencing the adoption of e-government services. *Journal of Software, 4*, 584–590.

[2]. Alketbi, et al., (2018). Blockchain for government services—Use cases, security benefits and challenges. *Learning and Technology Conference (L&T), 2018 15th* (pp. 112–119).

[3]. Lin, and Liao, (2017). A Survey of Blockchain Security Issues and Challenges. IJ Network Security, 19(5), 653-659.

[4]. F. Rizal Batubara, et al., Challenges of Blockchain Technology Adoption for e-Government: A Systematic Literature Revie. In *Proceedings of 19th Annual International Conference on Digital Government Research (dg.o'18). ACM, New York, NY, USA,*

[5]. Woodside Joseph, et al., (2017) "Blockchain Technology Adoption Status and Strategies," Journal of International Technology and Information Management: Vol. 26: Iss. 2, Article 4.

[6] Lemuria Carter & France Bélanger 2005 *The utilization of e-government services:citizen trust, innovation and acceptance factors Info Systems J*(2005) 15 , 5–25

[7]. Bélanger & Hiller, (2005) A framework for e-government:Privacy implications. *Business Process Management Journal*, 11.

[8] Sebastian Schuetz, & Viswanath Venkatesh 2019, Blockchain, adoption, and financial inclusion in India: Research Opportunities, International Journal of Information Management,

[9] Svein and Arild Jansen 2017 Blockchain Technology as s Support Infrastructure in e-Government, Springer International Publishing EGOV 201, pp. 215–227.