Review of Ownership Based Blockchain Frameworks in Government Applications

Deepika Sachdev*
Dr. Deepankar Chakrabarti**
Dr. Ankur Mittal***

Abstract

Blockchain Based Applications are becoming increasingly popular in the Government Sector due to increased needs of Trust and Transparency. Due to its Decentralized architecture, strong encryption algorithms and immutable timestamping it is being used in diverse applications including Health Care, Education, Voting and Smart Governance. Blockchain has many variants based on Ownership, Consensus Protocols and Tokenization Strategy. This paper analyses Blockchain Taxonomy based on Ownership and Access rights. It then reviews a multitude of Blockchain based Government applications based on their Ownership characteristics and needs for anonymity and Read as well as Write privileges. Based on the classification framework, the final objective is to create and verify the Blockchain Framework Mapping based on the Applications Business and Security requirements.

Key Words: Blockchain, Government, Permissioned, Public, Trust

1. Introduction

According to the Pew research centre Public trust in the government is at a historic low, where only 17% of the Americans say that they can trust the government. Blockchain with its key traits of decentralization, immutability and Cryptographic security helps to bring transparency and auditability to applications, which is a key factor for Trust enhancement by the public. Due to an increasing interest by Business and IT Firms, Blockchain has multiple variants to adapt to a vast variety of applications. This paper approaches Blockchain Applications for Government through the lens of Trust and Ownership. Blockchain is currently in use in Government Applications for multiple use cases including Land Reforms, Defence, Payments and Registries. The objective of this paper is to create a Blockchain Taxonomy with the goal of helping future Government Applications make optimized decisions on the right choice of Blockchain Framework based on Functional Needs. The methodology used to create this Framework starts with creating a Blockchain Framework based on Business, Technology and Trust Requirements. This is followed by an Evaluation of Application Use Cases in Government based on varying Trust and Business Requirements. This is followed by a thematic evaluation of the Use Cases to create a Taxonomy for Mapping the Optimized Blockchain Framework based on Application Requirements for Government Sector. This framework is finally verified by applying to existing Government Use Cases.

Deepika Sachdev*
VP Delivery Knowesis Pte Ltd, Singapore
Dr. Deepankar Chakrabarti**
Professor, Decision Sciences, School of Business,
University of Petroleum & Energy Studies, Dehradun
Dr. Ankur Mittal***
Associate Professor, School of Business,
University of Petroleum & Energy Studies, Dehradun

2. Theoretical Background

Blockchain Functional Pillars

The key Blockchain characteristics important for a Government application are:

- **Immutability**: once information is recorded, it cannot be altered.
- **Decentralization**: Multiple participants have access to information and hence there is no single owner of information
- **No Intermediary**: decisions are made by consensus and not controlled by a single party. Based on the type of Blockchain selected, the consensus can be owned by a central authority or can be public
- **Transparency**: all information can be accessible by all participants
- **Transaction Speeds**: Blockchains offer low to medium Transaction Speeds, varying based on the type of Blockchain Framework selected

Blockchain Schematic View

The Blockchain protocol created by Satoshi Nakamoto[19] is an append-only ledger with very restricted update or delete capability. Instead of storing individual transactions, it stores blocks of transactions which are cryptographically chained together. Blockchain which was started by Satoshi for a Finance as its applications is now rapidly spreading to other sectors. Due to its promise of True Decentralization and removal of the Middle Man, Blockchain is a killer application for the Government Sector, and as described in [8], Blockchain's goal is to enable Digital Autonomous Government (DAG).

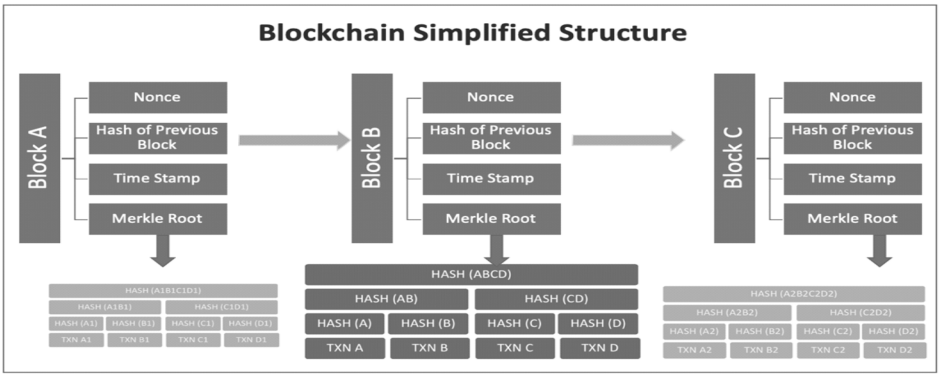

Figure 1: Blockchain Schematic

Blockchain as a Trust Enabler

At its core, Blockchain is a Decentralized Asset Managed Platform. Its unique characteristic is that it enables parties who do not have existing Trust Relationship to exchange Assets, which could vary from Physical Assets, Currency or Digital assets in a secure environment. The below diagram depicts Data Exchange Mechanics in Trusted versus Non Trusted Organizations:

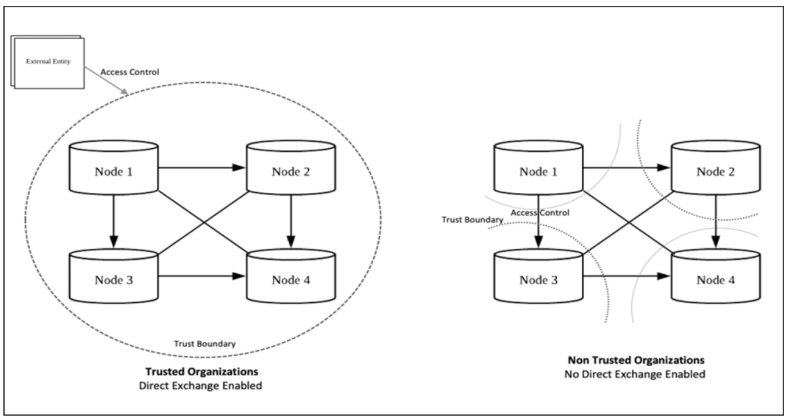

Figure 2: Data Exchange in Trusted and Non-Trusted Organizations

Blockchain technology is ideal for creating trust in information and scenarios where heterogeneous stakeholders are involved. Unlike traditional, centralised databases, where a single entity is generally responsible for collecting, securing and sharing information, blockchain platforms are based on decentralised, shared databases that are updated and verified by the community of users. Using Smart Contract Business Logic can be automated in the Blockchain for verification by Public Administrators, leading to substantial cost and time savings.

3. Data Integrity and Reliability

According to Oz Nathan et al. in "Decentralizing Privacy: Using Blockchain to Protect Personal Data"[23]centralized organizations including Public Sectorgather large quantities of personal and sensitive information. The individuals have limited control over the data and how it is used.[5]. In continuation, Nathan et al. continue to create Blockchain based frameworks where the Users have full control of their data and do not need to trust third parties with their information. As mentioned by Ahmed Alketbi et.al in[2] a key advantages of the Blockchain is that it is resistant to outages due to its Decentralized architecture.

4. User Privacy

Also as mentioned in[17], Blockchain is expected to increase the reliability of information through use of consensus mechanisms which ensure that information exchange happens only upon getting consent from all relevant parties. As mentioned in[2] the Blockchain promises data integrity and prevention of the unauthorized change of data by the use cryptography. Security is maintained through decentralized Ledgers which are controlled by a consortium and not Individual Owners. Blockchain is very good at creating trusted audit trails of information, making it simple to create platforms to track when and where data was entered.

5. Decentralized Access Control

Paradoxically, blockchain also make it relatively easy to keep data both private and easily shareable. Depending on how a system is designed, administrators can develop complex permission schemes to control who has access to what kinds of information, what can be shared by whom, and so on. In contrast to databases, Blockchain enables such capabilities among large, diverse groups without relying on or having to trust a single authority to do the job. In the paper [23] Nathan et. have created a novel Blockchain based Framework where access-control policies would be securely stored on a blockchain and only the authorized users are allowed to change it.

Known Challenges of Blockchain with Government

Domain	Challenge	Reference
GDPR Compliance	Right to Forget & Data Portability	GDPR applies to Personal Data including data which has been Pseudo Anonymized. It is applicable for 3rd party entities which own Subscriber Data known as "Data Controllers". GDPR enforces that all private data be pseudo anonymized and only minimal data be shared with 3rd Parties. One of the key components of this is the "Right To Be Forgotten" i.e. when the individual removes his consent from the organization, it should be immediately deleted from the system. However, the key attribute of Blockchain is immutability which opposes the Right to Forget.
Verification of Source Data	Lack of Trusted Information	• 78% of the land is unregistered in Ghana[9] • In Haiti, a large earthquake in 2010 destroyed all the municipal buildings that stored documents[6] • In India, millions of rural families lack legal ownership of the land they work on.

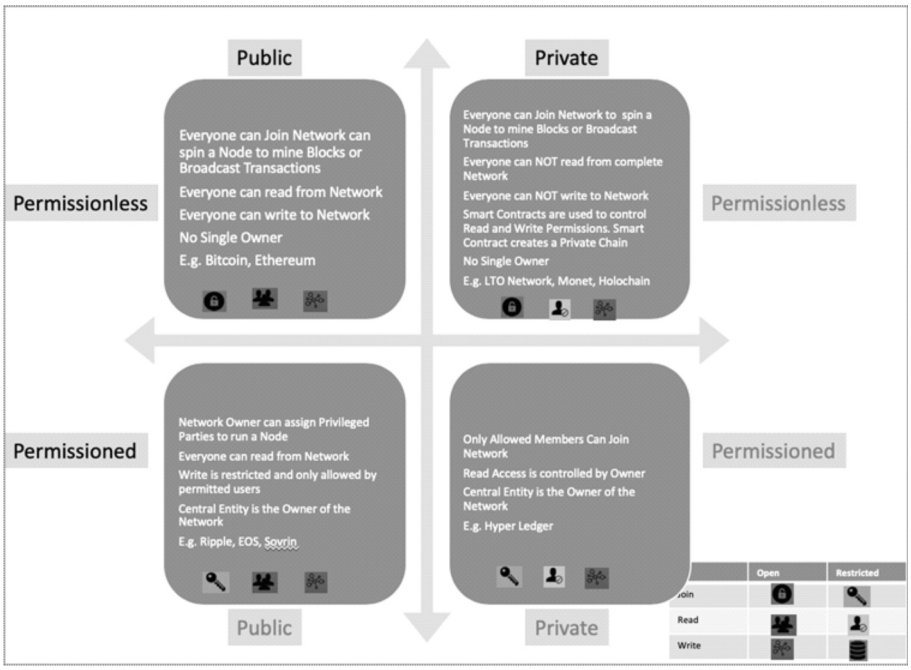

Figure 3: Ownership Based Blockchain Quadrant

Ownership Based Blockchain Frameworks

The below diagram depicts the Blockchain Quadrant based on Ownership and highlights key characteristics for each:

Permissionless Blockchains

Permissionless Blockchains have Public Ownership and are open and transparent. As mentioned in [14] if anyone can join the Blockchain, it is called Permissionless and such networks are highly censorship resistant. However, they are relatively slower compared to Permissioned Blockchains.

Public Permissionless Blockchain

These are publicly accessible to everybody. Any participant can record transactions, take part in the validation of the blocks or read data in the Blockchain. Consensus is reached through protocols like Proof of Work or Proof of Stake where any of the participants can start a node and start recording transactions. Bitcoin and Ethereum are the most common examples of Public Permissionless Blockchains. However, these have limitations on number of Transactions supported per second[15]. All Users have access for Read and Write in the public Permissionless Blockchain.

Private Permissionless Blockchain

In these there is no restriction on which participant can take part in the Consensus Mechanism. However there is restriction on who can read and write the content in the Blockchain.

Permissioned blockchains

Permissioned Blockchains typically have Private Membership, are trusted and overcome the Performance problem of Permissionless Blockchains.Governance is closed and the network of nodes is permissioned and new nodes can only join with permission from the validator nodes as mentioned in [15]

Public Permissioned Blockchain

Public Permissioned have rules that determine who can take part in the validation process and start nodes.Whitelisted nodes can participate in the Consensus Mechanism. This is normally used by Public institutions like Government Agencies, Corporates or Educational Institutes. The owner creates Validator Nodes that define the Governance

rules for the Blockchain including parties that can create new nodes or write to the Blockchain However, read access is available to all making the Blockchain publicly accessible as mentioned in [15].

Private Permissioned Blockchain

These Blockchains are controlled by Unique group of one or many owners who decide participants in the Consensus Mechanism. Only a select group of whitelisted users can read or write to these Blockchains as is suggested in [11].These are typically a network of partners that are connected through Business Operations and benefit by sharing data in an immutable database. As mentioned in [15], if public verifiability of the records is not required then Private Permissioned Blockchain should be considered. As described in [3], Hyperledger the most popular Permissioned Blockchain can scale up to 3500 TPS.

Blockchain Framework Based on Ownership

Based on the above analysis, the below matrix captures a framework to capture the Blockchain characteristics based on Application Business requirements:

Blockchain Framework	Owner	Transaction Volumes	Access Control for Consensus	Participants have existing Relationship	Shared Write Access	Anonymity Requirement	Business Rule Complexity	Security	Time for Contract Closure
Permissionless Public	No Single Owner	Low	All	Not Required	All	Visible to All	Low	Very High	High
Permissionless Private	Consortium	Low to Medium	All	Good to Have	Can Control Write Access based on User Roles	Permissioned Access to Read Data	Medium	Depends on the Validating Entities	Low to Medium
Permissioned Private	Consortium	Medium to High	Restricted	Required	Can Control Write Access based on User Roles	Permissioned Access to Read Data	High	Depends on the Validating Entities	Low
Permissioned Public	Consortium	Low to Medium	Restricted	Required	Can Control Write Access based on User Roles	Visible to All	Medium	Very High	Medium

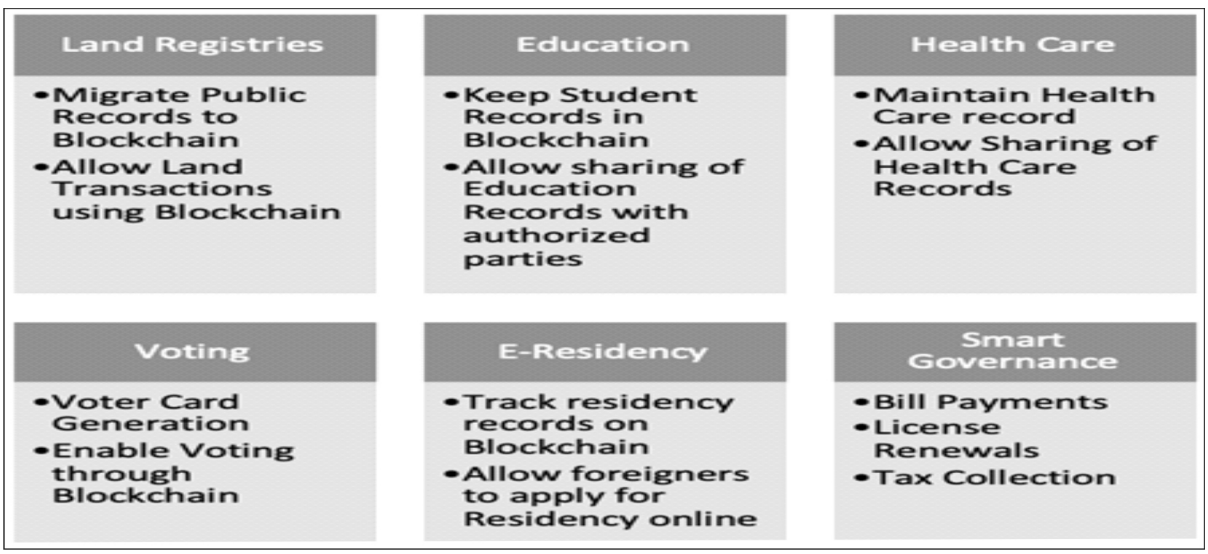

Figure 4: Blockchain Use Cases in Government

6. Government Use Cases for Blockchain

The Government provides three categories of functions to its citizens namely: Civil Service, Legislative and an Enabler of Economy for managing and regulating assets for its citizens. In all the three functions of the Government, Proof Of Concept Blockchain projects have been implemented in various countries to verify for the feasibility of Blockchain to help bring decentralization, increase transparency and help reduce the time to implement.

The below matrix, provides a summary of some of the key implementations which have been done globally, tangible benefits achieved and also the Blockchain framework which has been used to enable the same:

Strategy	Country	Implementation Use Case	Technology Used
Land Registries	Georgia[20]	Land Registration process in Georgia cost varied from 50-200$ and a Minimum of 1 Days. The average price of Registration is expected to come down to 5-10 cents per Registry after the pilot launch. Georgia had maintained a verified account of land titles in its NAPR database, which was crucial for the success of a Blockchain project. Bitfury did not attempt to build a brand new Blockchain based land registry. It only created a time stamping layer on top of the existing digital land records of NAPR. As part of the proposed Phase 2, Georgian citizens will be able to access their property information on the NAPR website and put it up for sale. The network nodes verify that the buyer has sufficient funds and that the seller owns the property before the transaction is concluded.	A pilot project was developed in collaboration with the Bitfury Group, the National Agency of the Public Registry (NAPR), and the Blockchain Trust Accelerator[12]
	Brazil	Bitcoin Blockchain to Mirror Land records. Hash records of the original records is kept to ensure that they become tamper proof.	Public Blockchain[20]
	Estonia	Blockchain technology is used to regulate changes in data about real estate in the e-Land register or statements documented in the e-Court system including author, time stamp and modus of change.	Distributed Ledger Technology[12]
	Sweden	Land Records are stored in Post Chain which is a Database that acts as a manager for the Blockchain.	Private Permissioned Blockchain[13]

Strategy	Country	Implementation Use Case	Technology Used
	Amravati, India	According to consulting firm McKinsey due to distortion created by large-scale corruption and inefficiency in India's land markets has shaved 1.3% off the country's GDP every year, Earlier, farmers had to pay a document writer up to 70USD or more to prepare registration papers. Blockchain is now facilitating automated documents at zero cost. Not to reduce transaction time, QR Code marked documents are transferred directly to the registrar's office at the time of appointment.	Private Blockchain which has a total of 58 attributes such as names, mobile numbers, boundaries with latitude and longitude coordinates, Aadhaar numbers,neighbouring plots, roads etc. are linked to each property and recorded in the Blockchain.
E-Residency	Estonia	Estonia has E-Residency for foreign nationals also enabled on Blockchain called ID-Kaarts[21]	As mentioned in [21], Estonia uses 2048 Bit Encryption to guarantee privacy for its citizens. Document Hashes are stored in the Blockchain which are protected by KSI Keys.
Smart Governance	Dubai	Visa Applications, Payments of Bills, License Renewal. Plans to save 1.5 Billion$ every year by the use of Blockchain	As mention in [2] Dubai Government plans to use IoT integrated with Blockchain for Smart Cities
Voting	West Virginia	Voatz, a Private Blockchain for enabling Voting in a Decentralized Manner	Private Blockchain with 8 Verified Nodes. As mentioned in [10], Voatzcan accept 10 different official documents.
	Voting-Estonia	Digital Voting using Unique Voter Cards	Estonian KSI Blockchain technology protects Estonian e-services such as the e-Health Record, e-Prescription database, e-Law and e-Court systems, e-Police data, e-Banking, e-Business Register and e-Land Registry as mentioned in [5]

Strategy	Country	Implementation Use Case	Technology Used
Health Records	Estonia	Govt Health Records are online and Access Controlled. The Estonian e-Health Record uses electronic health cards for user identification to ensure data integrity and mitigate internal threats to the data. This has been built on Guard Time System[13]. Estonians can log into their records using their identities and get access to audit log of View histories in there transactions.	Private Permissioned Blockchain

7. Blockchain Application Framework for Government Use Cases

Based on varying Business needs described in the above matrix, the Blockchain Framework Needs for an Organization vary. As mentioned in [4], clustering Blockchain analysis based on similar attributes helps in cluster analysis. The below matrix establishes to define "Blockchain Needs" for an Organization based on their Business Process Requirements. Some of the dimensions required in blockchain framework are:-

Use Case	Owner		Transaction Volumes			Anonymity Requirements			Shared Write Access		Business Rule Complexity			Time for Contract Closure		
	No Single Owner	Consor-tium	Low	Medium	High	Pseudo Anony-mous	Anony-mous	Public Visible	All Parti-cipant	Only Privile-ged Users	Low	Medium	High	< 1 Minute	< 10 Minute	< 1 Hour
Education		X	X					X		X		X				X
Health Information Exchange		X		X			X			X			X		X	
Land Registries	X		X			X			X				X			X
E-Residency	X			X				X		X	X					X
Voting	X				X		X		X		X			X		
Smart Government	X				X		X			X			X			X

(a) Owner: Can be owned by None or by a Consortium based on the Regulatory and Privacy requirements of the Application.

(b) Transaction Volumes in TPS: Refers to the theoretical maximum amount of Transactions Per Second that a Consensus Protocol can achieve as mentioned in Comparative Analysis of Blockchain Algorithms[18]. As described by Thurimella et. Al in [22] a key factor going down for Public Blockchains is the ability to support higher Volumes of Transactions.

(c) Anonymity Requirements: Based on Business Requirements, data in the Blockchain can either be available for read to all Users or to a select group of users based on Access Rights. As mentioned in Global Benchmarking Study[7], Transactionsdata need to have a certain level of privacy; on the contrary, in public blockchains, by design all transactions should be visible to every participant.

(d) Need for Shared Write Access: Based on the Business requirements, some or all Users will have Write Access. In the consortium, it is possible that Read Access is granted to all members, but Write Access is granted only to limited Super Users.

(e) Business Rules Complexity: As described by Thurimella et. Al in [22], since in a Permissioned Blockchain, the participants have given permission upfront it is much easier to build innovative applications.In Permissionless Blockchains, since the Nodes are run by multiple owners, to make any change in the Business Rules implemented by Smart Contracts, it needs to be accepted by majority of Node Owners before the Business Change can be implemented in the complete Blockchain. As mentioned in [1] it is difficult to enforce laws in a Permissionless blockchain on individuals without impacting the whole blockchain Infrastructure.

(f) Time for Contract Closure: As mentioned in Global Benchmarking Study[7] it is mandatory for enterprise applications that once transactions are confirmed they cannot be reversed. In Public Blockchains, settlement finality is only probabilistic since an alternate long chain can reverse the current transactions.

8. Framework Verification through Case Study

In order to verify, the mapping Framework for Business Requirements based on ownership and the Blockchain Framework, we shall apply real world Use Cases where Blockchain Frameworks were used to solve Business problems globally by Government.

Voting – Moscow's Active Citizen Program

In December 2017, the city of Moscow's Active Citizen program used Blockchain for voting and making the results auditable by public as described in [10] Nir Kshetri et al. After the voting was complete, the results were listed on a ledger containing all the previous results. In one Use case the participants were asked to choose if temporary accommodation should be provided in case the residential building in which they live is demolished.The popular polls were reported to have participation of up to 220,000.The platform peaked at approximately 1000 transactions per minute. It was public Blockchain access to all citizens, however citizens had to download node software for getting permission to join. As mentioned by Talib et al in [2] voting can be done in Blockchain for complex discussions to maintain democracy.

Land registry – Ubiquity in Brazil

As highlighted by Victoria L. Lemieux in [12] in April 2017 Ubiquity announced a pilot project to create a blockchain based registry to lower costs and improve transparency.

This was developed on Bitcoin for transaction recording as a Public Permissionless Blockchain. It used "Colored" Coins to tokenize the land and has a Web based front end to capture information. Multi Sig wallets were used when multiple parties need to be involved in case of Transaction Sale and Purchase.

Health records – Estonia Health Guard program

As mentioned by Matthias Mettler[16], In 2011 Estonia started a platform for storing Health Care information on Blockchain by doing a partnership with Guard Time. The log files which store data processing

	Moscow's Active Citizen Program for Voting	**Estonia Health Records using Guard Time**	**Brazil Land Registry by Ubiquity**
Owner	Consortium	Consortium	No Single Owner
Transaction Volumes	Medium	Medium	Low
Anonymity Requirements	High	High	No
Need for Shared Write	Yes	User Role Based Access Control for Write	Yes
Business Rule Complexity	Medium	High	Low
Time For Contract Closure	< 10 Minutes	< 1 Minute	< 1 Hour
Blockchain Framework	Public Permissioned	Private Permissioned	Public Permissionless

activities for Health Care are maintained in the blockchain. All users have secure authentication using either there ID Card or the Mobile Number. It is used to perform digital timestamp of the records and stored securely through cryptographic hashing.As mentioned in [5], the digital hash of the document is stored in the Permissioned Blockchain using KSI technology.

9. Summary

The literature review focusses on an objective assessment of the potential use cases of Blockchain in Government, the categorization of the Use Cases based on the functionality, and then a subjective framework that helps identify the best Blockchain framework to be applied based on the application Use Case. The applicability of the same has been verified through real world scenarios. There can be further research done on the same to extend the Blockchain categorization based on Consensus Protocols underlying the Blockchain technology.

10. References

1. W. Al-Saqaf, N. Seidler, Blockchain technology for social impact: opportunities and challenges ahead, J. Cyber Policy. 0 (2017) 1–17.
2. A. Alketbi, Q. Nasir, M.A. Talib, Blockchain for government services-Use cases, security benefits and challenges, 2018 15th Learn. Technol. Conf. L T 2018. (2018) 112–119.
3. E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukoliæ, S.W. Cocco, J. Yellick, Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains, (2018).
4. M.C. Ballandies, M.M. Dapp, Decrypting Distributed Ledger Design - Taxonomy, Classification and Blockchain Community Evaluation, (n.d.).
5. T.H.E. European, U. Blockchain, FOR GOVERNMENT AND PUBLIC, (n.d.).
6. J.M. Graglia, C. Mellon, Blockchain and Property in 2018: At the End of the Beginning, Innov. Technol. Governance, Glob. 12 (2018) 90–116.
7. G. Hileman, M. Rauchs, 2017-09-27-Ccaf-Globalbchain.Pdf, (2017).
8. M. Jun, Blockchain government - a next form of infrastructure for the twenty-first century, J. Open Innov. Technol. Mark. Complex. 4 (2018) 7.
9. N. Kshetri, 1 Blockchain's roles in meeting key supply chain management objectives, Int. J. Inf. Manage. 39 (2018) 80–89.
10. N. Kshetri, J. Voas, Blockchain-Enabled E-Voting, IEEE Softw. 35 (2018) 95–99.
11. O. Labazova, From Hype to Reality/ : A Taxonomy of Blockchain Applications From Hype to Reality/ : A Taxonomy of Blockchain Applications, (2019).
12. V.L. Lemieux, Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective, Eur. Prop. Law J. 6 (2017) 392–440.
13. V.L. Lemieux, A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation, Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017. 2018-Janua (2018) 2271–2278.
14. I. Martinovic, Blockchains: Design Principles, Applications, and Case Studies, 7 (2018).

15. W. Meng, E.W. Tischhauser, Q. Wang, Y. Wang, J. Han, When intrusion detection meets blockchain technology: A review, IEEE Access. 6 (2018) 10179–10188.

16. M. Mettler, Blockchain technology in healthcare: The revolution starts here, 2016 IEEE 18th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2016. (2016) 16–18.

17. S. Ølnes, J. Ubacht, M. Janssen, Blockchain in government/ : Bene fi ts and implications of distributed ledger technology for information sharing, 34 (2017) 355–364.

18. T. Osterland, S. Augustin, T. Rose, S. Augustin, Engineering Sustainable Blockchain Applications, (2018).

19. Satoshi Nakamato, Bitcoin: A Peer-toPeer Electronic Cash System, (2013) 1–9.

20. Q. Shang, A. Price, A BLOCKCHAIN- BASED LAND TITLING PROJECT IN THE REPUBLIC OF, (2015).

21. C. Sullivan, E. Burger, E-residency and blockchain, Comput. Law Secur. Rev. Int. J. Technol. Law Pract. (2017) 1–12.

22. R. Thurimella, Y. Aahlad, The Hitchhiker's Guide to Blockchains/ : A Trust Based Taxonomy, (2018) 1–28.

23. G. Zyskind, O. Nathan, A.S. Pentland, Decentralizing privacy: Using blockchain to protect personal data, Proc. - 2015 IEEE Secur. Priv. Work. SPW 2015. (2015) 180–184.