GSJ: Volume 7, Issue 11, November 2019, Online: ISSN 2320-9186

www.globalscientificjournal.com

An Overview of Blockchain Technology in Government Sectors Use Cases, Benefits and Challenges

Zahir Edrees
Department of Computer Engineering
Facuty of Engingeering-Karabuk Uinversity
Karabuk ,Turkey
E-mail: zahir-mohamed2010@hotmail.com

***Abstract - The* ability of using blockchain technology to record transactions on distributed ledgers offers new opportunities for governments to achieve strategic objectives such as citizen's satisfaction and happiness, service efficiency and cost optimization. Many government entities such as United Kingdom, Estonia and others have taken steps to use Blockchain technology in governments sectors. Dubai Government is aiming to become paperless by adopting the Blockchain technology for all transactions by 2021. Blockchain is much more than a foundation for crypto currency. It offers a secure way to exchange any kind of good, service or transaction. We review the literature to identify the potential use cases and application of Blockchain to enable government services and smart cities. The analysis shows that is huge potential for Blockchain technology to be used in to enable smart government services. This paper also highlights the challenges and limitations in application of Blockchain in government sectors.**

Keywords — blockchain; Smart contract; Smart city.

I. Introduction

The Blockchain technology will promise us the bright future. It can help to make the business, government and logistic systems more reliable, trusty and safety. The main role of government is to maintain trusted information about individuals, organizations, assets, and activities. Local, regional, and national agencies are charged with maintaining records that include, for instance, birth and death dates or information about marital status, business licensing, property transfers, or criminal activity.

Managing and using these data can be complicated, even for advanced governments. Some records exist only in paper form, and if changes need to be made in official registries, citizens often must appear in person to do so. Individual agencies tend to build their own silos of data and information-management protocols, which preclude other parts of the government from using them. In addition, these data must be protected against unauthorized access or manipulation. By using Blockchain technology could simplify the management of trusted information, Blockchain technology is a form of distributed ledger technology that acts as an open and trusted record (i.e., a list) of transactions from one party to another (or multiple parties) that is not stored by a central authority[1].

The Blockchain can be thought of as a database; however, instead of maintaining the records in a table, it groups the records into a block in a ledger. Each new block is chained to a previous block with the use of cryptographic hash; hence, the name Blockchain is created. The ledger can be shared with all nodes within the network where it can be verified and validated as well. The process of generating a block and validating it is called "Consensus"[2].

Blockchain systems are typically classified into three categories: public blockchain, consortium blockchain and private blockchain. The public blockchain is permissionless blockchain, while both consortium blockchain and private blockchain are permissioned blockchain. In the public blockchain, anyone is allowed to join the network, participate in the consensus process, read and send transactions, and maintain the shared ledger. Most crypto currencies and some open-source blockchain platforms are permissionless blockchain systems.

The consortium blockchain systems are generally used in business domain to record cross-organizational business transactions. Different from public blockchain systems, consortium blockchain systems only allow authorized entities to participate in the consensus process. The private blockchain is a distributed but still centralized network that is owned by an organization or entity[3].

Permissioned blockchain systems can be further divided into two categories: public and private permissioned blockchain systems. Both public and private permissioned blockchain systems allow only the authorized entities to participate in the consensus process, send transactions, and maintain the shared ledger.

The main difference between them is that public permissioned blockchain systems allow anyone to read transactions in the shared ledger, while in the private type of Permissioned blockchain systems, reading transactions is also restricted to the authorized entities. Most blockchain systems developed for business are permissioned blockchain systems.

TABLE I: COMPARISON OF TYPES IN BLOCKCHAIN

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	Within one organization
Read permission	Public	Public or restricted	Public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Efficiency (use of resources)	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Needs permission	Needs permission

The comparison among the three types of Blockchains is listed in Table I [4] as shown as below in details:

1. Consensus determination. In public blockchain, each node could take part in the consensus process. Only a selected set of nodes are responsible for validating the block in consortium blockchain.

   As for private chain, it is fully controlled by one organization and the organization could determine the final consensus.
2. Read permission. Transactions in a public blockchain are visible to the public while it depends when it comes to a private blockchain or a consortium blockchain.
3. Immutability. Since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public blockchain. Differently, transactions in a private blockchain or a consortium blockchain could be tampered easily as there are only limited number of participants.
4. Efficiency. It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public blockchain network. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium blockchain and private blockchain could be more efficient.
5. Centralized. The main difference among the three types of Blockchains is that public blockchain is decentralized, consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group.
6. Consensus process. Everyone in the world could join the consensus process of the public blockchain. Different from public blockchain, both consortium blockchain and private blockchain are permissioned.

This paper follows the following structure: Section II describes the Blockchain Components; Section III presents Key Characteristics of Blockchain Architecture; Section IV shows the fields of using Blockchain in government sectors; V shows Case Studies of Blockchain applications in the public sectors ;Section VI presents the Advantages of using blockchain technology in government sectors; Section VII discuss the Challenges and Security Threats of blockchain technology in government sectors, Section finally, Section VIII presents the conclusion.

II. BLOCKCHAIN COMPONENTS

We will describe the blockchain structure, its components, and their interaction:

a) Nodes: A node is simply a user or computer on a Blockchain platform that is running Blockchain software. The general job of "full nodes" is to store a full copy of a Blockchain ledger, receive data from other nodes, validate the data, and pass it to other nodes on the network so long as it is valid. In general ,two major types of node can distinguished:
   1) Validator nodes: meaning that they are able to validate the transactions in the system and participate in the consensus mechanism.
   2) Member nodes: meaning that they are able to transact but not able participate in the validation mechanism [5].In distributed networks, consensus mechanism is needed to maintain a unique version of ledger shared between all nodes[3].

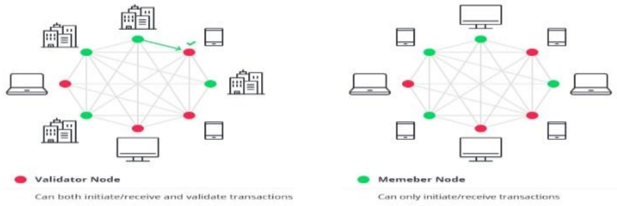
● Validator Node
Can both initiate/receive and validate transactions
● Memeber Node
Can only initiate/receive transactions

Fig 1: Node types in blockchain technology

b) Transaction : The transactions of blockchain enable the transfer of value between two parties without the need to have trust established between the parties, nor the need to have a centralized authority [6]. The transactions in Blockchain are programmable, and hence the transaction can hold the data that is applicable for that application. The sender creates the transaction, which must include the receiver public address, the transaction value, and the message digital signature . The digital signature is used to prove the authenticity of the message. This transaction is then transmitted to the network, where the nodes need to check the transaction authenticity using the digital signature, and if validated, it gets transferred to the "unconfirmed/unordered transactions pool" [5].The transactions in Blockchain are stored in blocks that every authorized node in the network maintains form a Blockchain in a form of a ledger, and the history of all transactions.

c) Block (Data store): a data structure used for keeping a set of transactions which is distributed to all nodes in the network, each block includes the hash output of the previous block in the blockchain. The first block of a blockchain is called genesis block which has no parent block. We then explain the internals of blockchain in details as shown in Fig 2. A block consists of the block header and the block body In particular, the block header includes:

- Block version: indicates which set of block validation.
- Merkle tree root hash: the hash value of all the transactions in the block.
- Timestamp: current time as seconds in universal time since January 1, 1970.
- nBits: target threshold of a valid block hash.
- Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation.
- Parent block hash: a 256-bit hash value those points to the previous block.
- Difficulty: A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction.

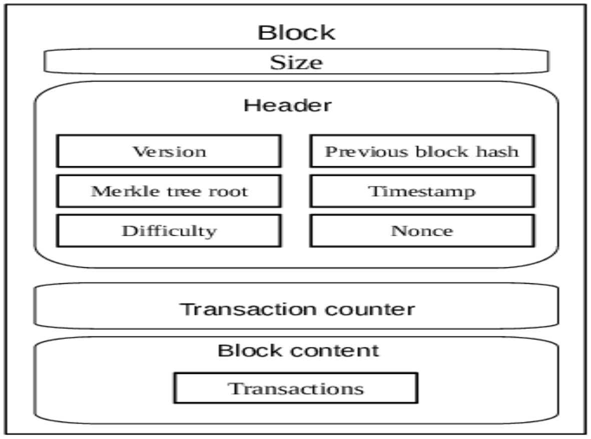

Fig 2: block structure

The following Fig 3 is a blockchain diagram that shows how blockchain actually works each blockchain block consists of certain data, the hash of the block and the hash from the previous block. The data stored inside each block depends on the type of blockchain. For instance, in the Bitcoin blockchain structure, the block maintains data about the receiver, sender, and the amount of coins. A hash is like a fingerprint (long record consisting of some digits and letters). Each block hash is generated with the help of a cryptographic hash algorithm (SHA 256). The moment a block is created, it automatically attaches a hash, while any changes made in a block affect the change of a hash too. Simply stated, hashes help to detect any changes in blocks. The final element within the block is the hash from a previous block. This creates a chain of blocks and is the main element behind blockchain architecture's security.

d) Chain: a sequence of blocks in a specific order as shown in Fig 3.

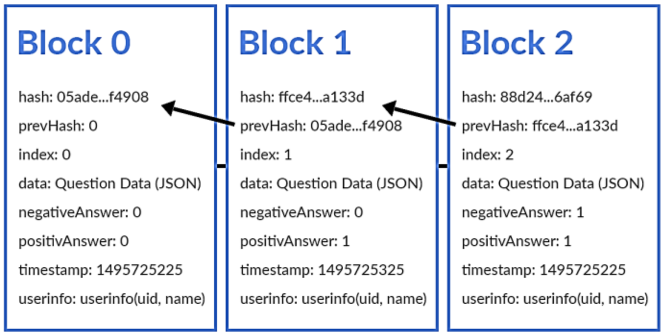

Fig 3: block structure as sequence of blocks

e) Miners: specific nodes which perform the block verification process before adding anything to the blockchain structure.

f) Consensus (consensus protocol) : A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, In the applications of blockchain, we need to solve two problems- double spending and Byzantine Generals Problem. Double spending problem means reusing the currency in two transactions at the same time. The traditional currency is the entity, so we will not face the problem of double spending while using traditional currency.

We can also solve the double spending problem in the Internet transactions with the centralized trusted institutions. Blockchain solves this problem with the method of verifying the transactions by many distributed nodes together. Byzantine Generals Problem is the problem in the distributed system. The data can be delivered between different nodes through peer-to-peer communications. However, some nodes may be maliciously attacked, which will lead to the changes of communication contents. Normal nodes need to distinguish the information that has been tampered and obtain the consistent results with other normal nodes[7]. We next present several common approaches to reach a consensus in blockchain.

PoW (Proof of work) is a consensus strategy used in the Bitcoin network . In a decentralized network, someone has to be selected to record the transactions. The easiest way is random selection. However, random selection is vulnerable to attacks. So if a node wants to publish a block of transactions, a lot of work has to be done to prove that the node is not likely to attack the network. In PoW, each node of the network is calculating a hash value of the block header. The block header contains a nonce and miners would change the nonce frequently to get different hash values. The consensus requires that the calculated value must be equal to or smaller than a certain given value[8].

When one node reaches the target value, it would broadcast the block to other nodes and all other nodes must mutually confirm the correctness of the hash value. If the block is validated, other miners would append this new block to their own Blockchains. Nodes that calculate the hash values are called miners and the PoW procedure is called mining in Bitcoin [9],[10].

PoS (Proof of stake) is an energy-saving alternative to PoW ,Miners in PoS have to prove the ownership of the amount of currency. It is believed that people with more currencies would be less likely to attack the network. The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. Compared to PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Many blockchains adopt PoW at the beginning and transform to PoS gradually[11].

PBFT (Practical byzantine fault tolerance) is a replication algorithm to tolerate byzantine faults. A new block is determined in a round. In each round, a primary would be selected according to some rules[12]. And it is responsible for ordering the transaction. The whole process could be divided into three phase: pre-prepared, prepared and commit. In each phase, a node would enter next phase if it has received votes from over 2/3 of all nodes. So PBFT requires that every node is known to the network. Like PBFT, Stellar Consensus Protocol (SCP) is also a Byzantine agreement protocol[13].

In PBFT, each node has to query other nodes while SCP gives participants the right to choose which set of other participants to believe. Based on PBFT, Antshares has implemented their dBFT (delegated byzantine fault tolerance). In dBFT, some professional nodes are voted to record the transactions.

DPOS (Delegated proof of stake). The major difference between PoS and DPOS is that PoS is direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and validate blocks. With significantly fewer nodes to validate the block, the block could be confirmed quickly, leading to the quick confirmation of transactions[14]. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by delegates[8].

Ripple is a consensus algorithm that utilizes collectively-trusted subnetworks within the larger network. In the network, nodes are divided into two types: server for participating consensus process and client for only transferring funds. Each server has an Unique Node List (UNL). UNL is important to the server. When determining whether to put a transaction into the ledger, the server would query the nodes in UNL and if the received agreements have reached 80%, the transaction would be packed into the ledger. For a node, the ledger will remain correct as long as the percentage of faulty nodes in UNL is less than 20% [15].

According to the previous section, it is better to use the corresponding consensus algorithm in different scenarios. A public blockchain means that it is accessible to all the people in a public area. Everyone can become one of the nodes and make contributions to obtain the rewards following the rules. There are no trust relationships among the nodes. Public blockchain is completely open and decentralized. All transactions on the public blockchain can never be changed or revoked. PoW, PoS, and DPoS consensus algorithms are common choices of public blockchain.Private blockchain means that the owner of the blockchain has the highest authority to change the information. The rest of the nodes have limited access to read. Compared to the public blockchain, the private blockchain has the characteristics of easy modification and low transaction cost.

Transaction verification of the private blockchain only need some designated high credit nodes. Private Blockchain is applied to more closed networks such as the intranet. It is more important to solve the crash faults than Byzantine faults. We can use PBFT consensus mechanisms according to the network size.

Permissioned blockchain means that the blockchain is composed of many parties and the main nodes are pre-specified by the participants. The members of the permissioned blockchain do not fully trust the others. Each participant selects its own consensus node according to the rules. Transactions need to be recognized by most consensus nodes. The degree of openness and centralization of the consortium blockchain lies between the public and private blockchain. The permissioned blockchain is suitable for the semi-closed network, which is built by different enterprises. There may be conflicts among different enterprises and some nodes can become malicious nodes, so it is better to use PBFT in this scenario.

g) Smart contract: is a code program identified by an address in the Blockchain network. The main components of the smart contract are a set of executable functions and state variables[16]. Each transaction has input parameters, which are, required a function in the contract. During the execution of a function, the status of the state variables is changed depending on the logic implementation.

The smart contract code is written in high-level languages such as Solidity and Python for Ethereum applications. The code is compiled into bytecode using compilers as Solidity or Serpent. The contract code will be uploaded into the Blockchain network once the compiler is executed without any errors. Each contract will be assigned a unique address by the Blockchain network. Any User in the Blockchain network can trigger the functions of sending any kind of transactions.The contract code is executed on each node member in the Blockchain network as a part of his or her verification of new blocks. Smart contracts deployed on a Blockchain network can send messages to other contracts.

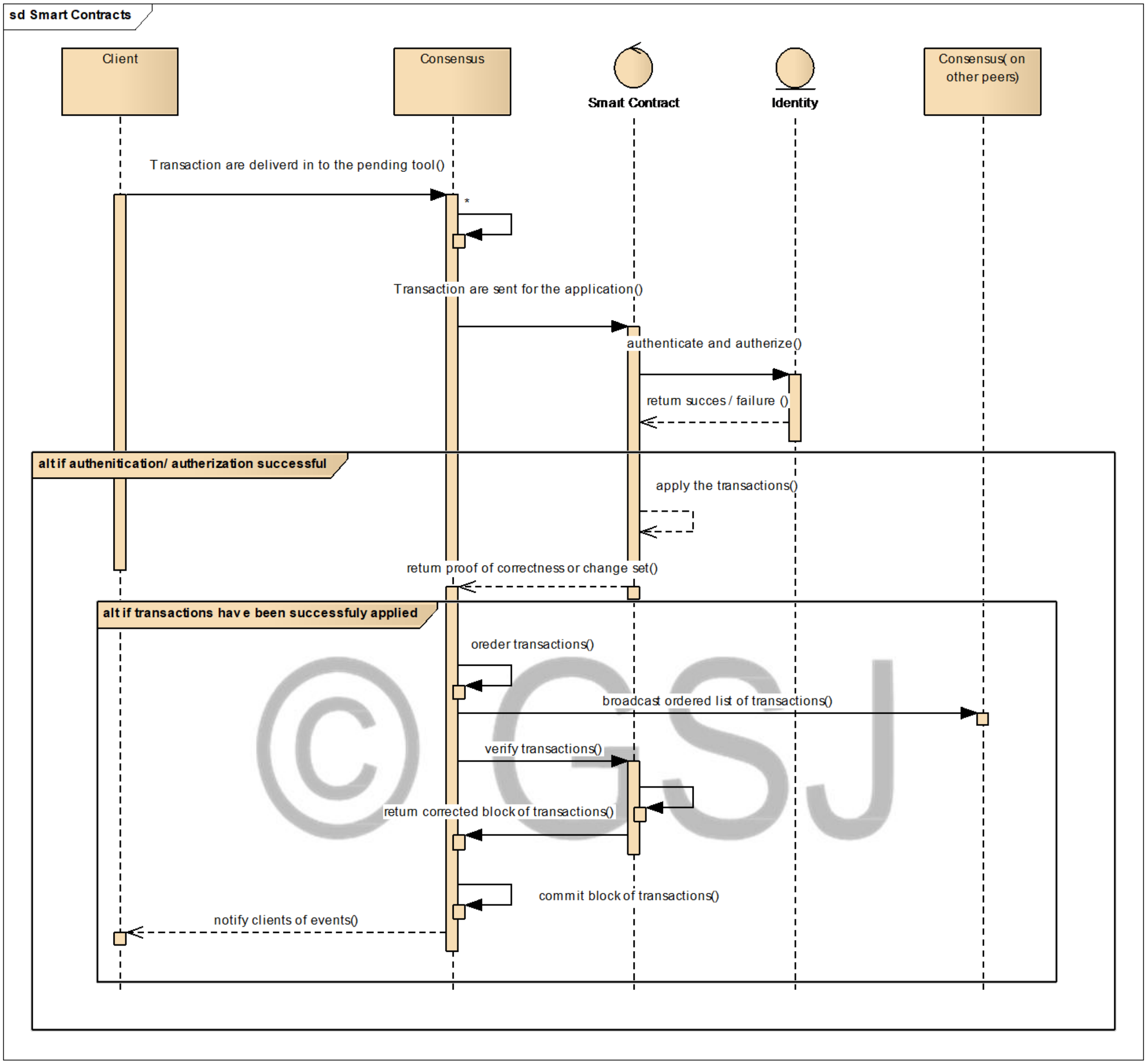
sd Smart Contracts
Client
Consensus
Smart Contract
Identity
Consensus(on other peers)
Transaction are deliverd in to the pending tool()
*
Transaction are sent for the application()
authenticate and autherize()
return succes / failure ()
alt if authenitication/ autherization successful
apply the transactions()
return proof of correctness or change set()
alt if transactions have been successfuly applied
oreder transactions()
broadcast ordered list of transactions()
verify transactions()
return corrected block of transactions()
commit block of transactions()
notify clients of events()

Fig 5: shows how smart contracts fit in with the other blockchain architectural layers

In general, the smart contract layer works very closely with the consensus layer. Specifically, the smart contract layer receives a proposal from the consensus layer1 shows in table II.This proposal specifies which contract to execute, the details of the transaction including the identity and credentials of the entity asking to execute the contract and any transaction dependencies. The smart contract layer uses the current state of the ledger and input from the consensus layer to validate the transaction. While processing the transaction, the smart contract layer uses the identity services layer to authenticate and authorize the entity asking to execute the smart contract. This ensures two things: that the entity is known on the blockchain network, and that the entity has the appropriate access to execute the smart contract. Identity can be provided through several methods: simple key-based identities, identities and credentials managed through the ledger, anonymous credentials, or managed identity services from an external certificate authority. After processing the transaction, the smart contract layer returns whether the transaction was accepted or rejected. If the transaction was accepted, the smart contract layer also returns an attestation of correctness, a state delta, and any optional .

Blockchain Layered Approach: The technological components underlying the Blockchain layers include transactions, block, consensus, applications and smart contract.

TABLE II: SMART CONTRACTS MESSAGES

	Message	From Object	To Object
1	Transaction are delivered in to the pending tool	Client	Consensus
2		Consensus	Consensus
3	Transaction are sent for the application	Consensus	Smart Contract
4	authenticate and authorize	Smart Contract	Identity
5	return success / failure	Identity	Smart Contract
6	apply the transactions	Smart Contract	Smart Contract
7	return proof of correctness or change set	Smart Contract	Consensus
8	ordered transactions	Consensus	Consensus
9	broadcast ordered list of transactions	Consensus	Consensus(on other peers)
10	verify transactions	Consensus	Smart Contract
11		Smart Contract	Smart Contract
12	return corrected block of transactions	Smart Contract	Consensus
13	commit block of transactions	Consensus	Consensus
14	notify clients of events	Consensus	Client

h) All these components are separated into different layers, which are equivalent to the blockchain eco-system. The key aspects of blockchain can be divided into six layers listed as follows: network, transaction, the blockchain, trust, application and security layers. Each of these layers has different properties and characteristics as shown in the following Fig 6. The network layer refers to P2P network with Ethereum or Hyperledger nodes. The transaction layer refers to transactions triggered by the users or smart contract. The Blockchain layer has used to refer to the block status containing all the necessary information whereas the trust layer refers to the consensus protocol for the block and transactions validation. The application layer encompasses applications, state machine, and smart contract. This layer is always separated from the blockchain layer with the smart contract to be the most important component. The security layer is very vital for the Blockchain technology[17].

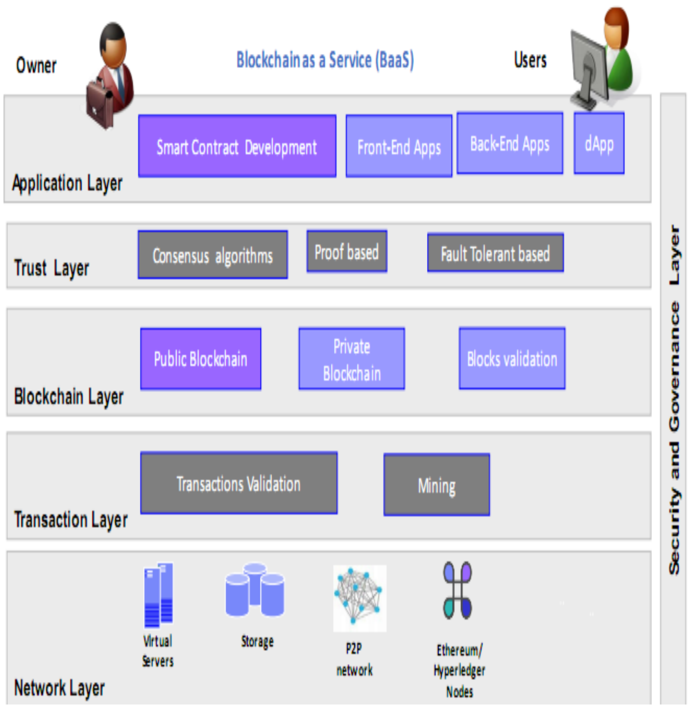

Fig 6: blockchain layers

III. KEY CHARACTERISTICS OF BLOCKCHAIN ARCHITECTURE:

a) Cryptography: is the act of creating codes that allow data to be kept secret. Cryptography converts this data into a format that can only be read/decoded by authorised user, in cryptography using different mechanisms like hash algorithm, public key cryptography and digital signature [18].

b) Immutable: means that something is unchanging over time or unable to be changed.In the context of Blockchains, it means once data has been written to a Blockchain, no one, not even a system administrator, can change it. Immutability allows senders, receivers, and any interested party to be able to verify that data have not been altered[19].

c) Pseudonymous On many Blockchain platforms, user identities can be anonymous but their accounts are not, as all of their transactions are visible to all other users. On these platforms, user accounts can be created without any identification or authorisation process. This allows users to use a pseudonym – a fictitious name. However, some permissioned Blockchains may require and a user's identity be verified before they are able to access or interact on the Blockchain[1].

d) Provenance - refers to the fact that it is possible to track the origin of every transaction inside the blockchain ledger.

e) Decentralization - each member of the blockchain structure has access to the whole distributed database. As opposed to the central-based system, consensus algorithm allows for control of the network.

f) Transparency - the blockchain system cannot be corrupted. This is very unlikely to happen, as it requires huge computing power to overwrite the blockchain network completely.

IV. Blockchain in Government Sectors:

Blockchain technology creates multiple opportunities when used in government services such as; operations cost reduction, reducing fraud and payments' errors and citizens [20]. This section discusses the use cases and applications of Blockchain technology in the government services and public sector identified from the literature.

a) Identity management:

Blockchains could be used to establish digital identities for citizens, residents, businesses, and other government affiliates. In addition to using Blockchain technology to manage identity, multiple aspects of the identity could be managed using Blockchain technology. For example, birth certificates, passport and visa information, and death records could be managed via Blockchains , Estonia government is collaborating with Bitnation the world's first operational Decentralized voluntary nation to offer publicnotary services to Estonian e-Residents. Estonian e-Residents has electronic IDs that are signed by the government, and these electronic IDs can be used to notarize official documents such as birth certificates, marriage arrangements, testaments, business contracts, and other from anywhere in the world [8].

b) Personal records (health, insurance, financial, etc.):

Personal records may be managed with Blockchains. Health records, for example,could be made accessible and interoperable to all hospitals in a network or in a country. In Switzerland, medtech companies have taken an interest in blockchain health data management. One company doing this is the HIT foundation. The company has launched an application that facilitates clinical trials with blockchain. This solution would allow for the creation of a database containing information on each new drugs and the medical records of individual patients taking part in the studies. Pharma blockchain supply chain tracking is also a fascinating trend. The use of blockchain technology to store medical records of patients and other sensitive data on treatment and disease progression, which will enable the acceleration of data exchange between doctors, clinics and other medical facilities [21].

c) Financial services and banking:

Blockchain technology can be used by governments to ease the overhead of transferring funds among parties. It enables more open, inclusive, and secure business networks, shared operating models, more efficient processes, reduced costs, and new products and services in banking and finance. It enables digital securities to be issued within shorter periods, at lower unit costs, with greater levels of customization. Digital financial instruments may thus be tailored to investor demands, expanding the market for investors, decreasing costs for issuers, and reducing counterparty risk. the technology has matured for enterprise-grade use demonstrating the following benefits[22]:

- Security: Its distributed consensus based architecture eliminates single points of failure and reduces the need for data intermediaries such as transfer agents, messaging system operators and inefficient monopolistic utilities. Ethereum also enables implementation of secure application code designed to be tamper-proof against fraud and malicious third parties— making it virtually impossible to hack or manipulate.
- Transparency: It employs mutualized standards, protocols, and shared processes, acting as a single shared source of truth for network participants
- Trust: Its transparent and immutable ledger makes it easy for different parties in a business network to collaborate, manage data, and reach agreements
- Programmability: It supports the creation and execution of smart contracts— tamper proof, deterministic software that automates business logic – creating increased trust and efficiency
- Privacy: It provides market-leading tools for granular data privacy across every layer of the software stack, allowing selective sharing of data in business networks. This dramatically
- Improves transparency, trust and efficiency while maintaining privacy and confidentiality.
- High-Performance: It's private and hybrid networks are engineered to sustain hundreds of transactions per second and periodic surges in network activity
- Scalability: It supports interoperability between private and public chains, offering each enterprise solution the global reach, tremendous resilience, and high integrity

d) Supply chain management and asset tracking:

Blockchain transactions can be used as a means of documenting every transfer of an asset from its origin. Governments could track an asset from its creation, through potentially multiple stages of transportation, and eventually through purchase and even managing asset inventory.

e) Copyrights:

Governments often allow for the registration of copyrights or need to adjudicate disputes related to copyrights. Blockchains are excellent tools to "timestamp [artists' and content producers'] work.

f) Smart Cities:

the Blockchain has promising use cases for Smart Cities which include but not limited to, emergency management, healthcare, smart building management, transportation and power & utilities services. Dubai Government city government hopes to become the first-ever blockchain-powered government by the year 2020[6]. The main aim of the plan is to leverage the power of blockchain technology in facilitating license renewals, payment of bills, and visa applications. Dubai is a prominent holiday destination with millions of tourists and visitors every year.

A lot of manhours are dedicated to processing an estimated 100 million documents every year. By using blockchain technology for these tasks, a large percentage of those manhour's can be saved which translates into huge government savings. By making the move to a paperless transaction system that is hosted entirely on the blockchain, the Dubai government could potentially year. The table III below shows that the top ten countries that applied blockchain in different sectors[23].

TABLE III: TOP 10 COUNTRIES TO ADOPT BLOCKCHAIN

Country		**Areas of blockchain Application**
1	Malta	Financial services and banking
2	China	Healthcare , e-voting ,financial services and banking
3	Switzerland	financial service, insurance, logistics, Energy and healthcare
4	Japan	financial service, insurance ,education, energy, health care, and Road and Transport
5	The United States	financial service
6	Singapore	education
7	Belarus	financial service
8	The Cayman Islands	financial service
9	Estonia	financial service
10	United Arab Emirates (UAE)	financial service

V. Case Studies of Blockchain in the public sectors:

The case studies presented in this paper offer a non-exhaustive view of how the public sector is currently using Blockchain technology. Using Smart contracts are enabling new forms of digital payments and provision of social services and aid over Blockchains. Complex issues are now being discussed and their possible implications evaluated.

- Case study 1:

Name: Global Blockchain Council
Organization: Dubai Future Foundation
Project lead: Noah Raford, COO
Launched: 2016
Where: Dubai, United Arab Emirates (UAE)
Website: http://www.dubaifuture.gov.ae/our-initiatives/global-blockchain-council/

THE PROBLEM:

As Blockchain technology develops in what Noah Raford calls the 'pre-legal stage', companies and administrations in Dubai lack a clear strategy and way forward to develop its use at systemic levels. There is a need for some form of centralising platform that opens the way for knowledge sharing and best practices.

THE SOLUTION:

The development of a large, multi-stakeholder Global Blockchain Council, where both private firms and public agencies are invited to understand the technology better, its implications and impacts, and the way forward in terms of experimentation, institutional support, and drafting the future of regulation. Furthermore, it provides ways to talk about Blockchain in accessible ways to non tech-savvy managers and decision-makers, by focusing on what the technology enables rather than what it is. It facilitates the development of public-private partnerships (PPPs) while creating in substance a new eco-system around Blockchain – always asking the question "how can Blockchain be useful to you?". Within this new space, the Dubai Future Foundation aims to ensure and enhance the governance structure of this eco-system to ease relationships with the city of Dubai and open the way for experimentation in both public and private sectors.

RESULTS AND IMPACT:

The Council board is now made of 46 leaders in the field from both private, technology-geared firms and public agencies from Dubai and the UAE. Fifteen experimentation pilots have been introduced, almost all of which are PPPs, with firms taking the role of technical and technological providers. Furthermore, the city of Dubai is now ready to have 100% of monetary transactions run through the Blockchain. For this to occur, the Smart Dubai Office, in charge of the Implementation of the Blockchain technology strategy, has trained 14,000 public servants in data science and technological literacy.

The impacts are not limited to Dubai and the UAE. While Noah Raford easily recognizes that the size of the Emirates' public service is nowhere near that of larger countries, he claims that the Global Blockchain Council redefines the landscape of possibilities with regard to emerging technologies. It sets goals other national administrations can look to and see that it can be done.

- Case study 2:

Name: Project Ubin
Organization: Monetary Authority of Singapore (MAS), in partnership with Deloitte
Project Lead: Stanley Yong
Launched: Phase one was run from November to December 2016 (six weeks)
Where: Singapore
Website: http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx

THE PROBLEM:

The Monetary Authority of Singapore (MAS), as part of its mandate, ran an industry study on industrial and financial problems Blockchain technology could bring a possible answer to. It was found that Blockchains could serve the purpose of more efficient, cheaper and faster inter-bank payments for cross-border monetary and government securities transactions.

THE SOLUTION:

MAS partnered with R3 – a consortium of banks and regulators specialized in digital ledger technologies – to develop and apply a Blockchain-based transaction process with a digital Singaporean dollar. This would not only allow incorruptibility through a decentralized trust system, but it would allow transactions to run 24 hours a day with no centralized – i.e. human-based – checks required. It invited a number of different banks – the main beneficiaries – to participate in the early development and trials of the technology. The prototype uses the Ethereum platform to make best use of smart contracts. Furthermore, it makes full use of the MAS MEPS+, a Singaporean-run system that enables real-time and irrevocable transfer of funds and Singapore Government Securities. Project Ubin thus uses what already exists in terms of digital transaction mechanisms (MEPS+) and adds a Blockchain 'layer' for higher security and efficiency – both time and costs – of transactions.

RESULT AND IMPACT:

By the end of Phase 1 in December 2016, Project Ubin demonstrated that a working interbank transfer prototype on a private Ethereum network was successfully built, and a Smart Contract codebase developed. More importantly, it managed to fully integrate existing technologies on digital transactions with a rather new Blockchain technology.

LIMITATIONS AND THINKING AHEAD:

Due to the very nature of financial transactions, some level of privacy is required to protect transactional actors. There is a crucial need to develop some types of privacy settings within a system – Blockchains – which very principle is full information in a decentralized decision-making context. Phase 2 of the project thus aims to develop such privacy settings and answer the complex question of: How can I prove that a transaction has occurred and the necessary funds to the transaction are indeed present, without showing you the transaction, and without having to refer to a centralized authority? Answers reside in the drafting of complex mathematical protocols that exist, at this point in time, as mere prototypes and beta versions.

- Case study 3:

Name: Sweden Land Registry on Blockchain
Organization: Swedish Land Registry Authority
Project Lead: Mats Snäll, Chief Digital Officer
Launched: 2017
Where: Sweden

THE PROBLEM:

The Sweden Land Registry seeks to go beyond existing digital systems to record land transactions and ownership – for more efficient, faster and tailored services to citizens. From a more general perspective, the centralized system of information storing that was developed in Sweden no longer respond to the demands from greater transparency and accountability. Finally, it appears to be of necessity for Swedish Government agencies, including the Land Registry Authority, to be on top of the digital and technical scene.

THE SOLUTION:

Granted that Blockchain technology is the "best and most advanced technology available"[24] the Land Registry Authority seeks to "explore and investigate if the Blockchain may be an alternative to support the process of a real property transaction; sale and purchase; finance and mortgage; apply and register title/ownership; instead of having the traditional technical database and web application solutions". The project is split in three phases. Phase 1 developed a theoretical understanding of what Blockchain technology is and how it works, and why it would be relevant in the context of the Land Registry Authority. Phase 2 aimed to develop the technology to best respond to needs and demands from title owners and the Government. Both these phases were successfully completed. The last phase to come is one of experimentation, with the goal of developing a working and efficient Proof-of-Concept. Finally, it allows digital actors in the Swedish public sector to learn more about the technology – it is a way to be "on the frontline even if we don't implement the Blockchain technology right now".

RESULTS AND IMPACT:

Clear impacts on land transaction and ownership are not yet clear – though Blockchains theoretically responds well to the demands of a secured and transparent system of information sharing and gathering by a governmental agency.

LIMITATIONS:

At this point in time, there is no legal recognition of digital signatures on Smart Contracts. Though Blockchains as a system may work, they would not have a legal value – transactions and contracts signed on a Blockchain may not be legally binding. More must be done on this regulation aspect.

It also remains fairly unclear how the governance framework would work around the Blockchain – which is likely to be a more "theoretical and legal issue" [24]and focus on questions of prerogatives and the role of the State in the development of the technology.

VI. Advantages of using Blockchain in public sectors:

The main benefits of applying blockchain technology in governments are claimed to be [3]:

a) Reduced economic costs, time and complexity in inter-governmental and public- private information exchanges that enhance the administrative function of governments.
b) Reduction of bureaucracy, discretionary power and corruption, induced by the use of distributed ledgers and programmable smart contracts.
c) Increased automation, transparency, auditability and accountability of information in governmental registries for the benefit of citizens.
d) Increased trust of citizens and companies in governmental processes and record keeping driven by the use of algorithms, which are no longer under the sole control of government.
e) Reducing human errors, Automatic transactions and controls reduces the making of errors by humans[25].
f) Persistency and irreversibility (immutable), once data has been written to a blockchain it is hard to change or delete it without noticing. Furthermore, the same data is stored in multiple ledgers.

VII. Challenges and Security Threats:

In this section, we identify the challenges and Security threats that may be faced in adopting blockchain technology for e-Government systems as presented in the selected papers. In order to categorize the challenges, we adopt the technology - organization - environment (TOE) framework as shown in table IV; this framework has been extensively used by researchers to study information technology adoption. In this framework, three contexts are used to identify technological innovation adoption decisions, which are the technological, organizational and environmental.

TABLE IV. CHALLENGES OF BLOCKCHAIN ADOPTION IN GOVERNMENT

Aspects	Challenges	Authors
Technological	Security	Ahram et al[5], angaral et al [26]
	Interoperability/compatability	Kamanashis Biswas [2]
Organizational	Risk errors for complex business rules	Engelenburg et.al[27]
	New governance model	Heng Hou [28]
Enviromental	Support infrastrucre	Ross, OmriDüdder[29]

Security: There are quite a few potential security issues and there is more and more literature on that subject. Here are a couple of examples[10]:

- 51% attacks: It will happen when two miners are calculating the hash of the block at the same time and get the same results. In this case, the Blockchain will split and as the result, users have two different chains, and both are considered true.
- Forks that can be caused by Sybil nodes or selfish mining
- selfish mining: miners trying to increase their rewards by keeping blocks private
- DNS attacks: sending peers wrong information
- mempool attacks: flooding new blocks with transactions
- DDos attacks: achieving denial of service.
- consensus delay: preventing peers from reaching consensus
- double spending attacks: creating two transactions from the same unspent transaction
- Theft of wallets

Interoperability/compatibility: In the Blockchain world, interoperability defines as an ability of blockchain protocols and applications to communicate and work with each other seamlessly. It is hard to move the transaction from one chain to another. A third-party app, also known as cross-chain interaction, is required to resolve the issue.

Interoperability is not essential to purchase or send cryptocurrency to another account.But, it plays a significant role in developing decentralized applications (dApps), smart contracts, and multi-chain solutions. The cross-chain compatibility can help in increasing the user base in dApps in which all, the digital assets can be purchased and traded within the app. Hence, it allows deploying the entire cross-chain dApp ecosystem. In some banks, it is allowed to use only one currency. They restrict all international transfers as well as exchanging of payments in different currencies. It makes the business limited. It is a similar condition to blockchain projects. Therefore, many protocols realized the importance of dApps and their interoperability solutions.

The following Security threats that may be faced in adopting blockchain technology for e-Government systems:

i) Threats on Availability- are concerned with the (unauthorized) upholding of resources.

ii) Threats on Integrity- include unauthorized change to data such as manipulation and corruption of information.

iii) Threats on Confidentiality- include disclose of sensitive information by unauthorized entity [2] ,even though the Blockchain technology is immutable and promises transactions integrity, there are cases where the records authenticity maybe impacted. Table V shows the vulnerability/attacks that may affect records authenticity.

TABLE V. AUTHENTICITY VULNERABILITIES/ATTACKS PRESENTED IN [30]

Malicious Attack	Description
Man-in-the-middle attack	Intercepting and altering the communication, when; New record entry are interested in the Blockchain system, and when system enters a directory block to the blockchain
SYN Flood attack	Denial of Service (DoS) attack using SYN requestsrepeatedly and rapidly to make the target system unresponsive
Sybil attack	Controlling nodes in Blockchain network in order to not relay blocks or transactions, disconnect communications,alter communications relayed to other nodes in the network
Timing errors	Reporting inaccurate transactions' timestamp in the network, and slowing down or speeding up network time counter
Key management	Complexity in key management that is vital for Blockchain operations, and the probability of private keys compromise.
Audit server attack	Hijacking the audit server that is used by Factom (the Blockchain used for land registration) to verify transactions, this may lead to entries' manipulation

VIII. Conclusion

The blockchain is new type of database, which solved some of the problems in the centralized system; this paper explored the potential applications and use of blockchain technology in government sectors. The paper shows that there is a huge in the use of blockchain technology in government services; In addition identify challenges and security threats of blockchain adoption in government sectors.

Future research needs to identify novel solutions to overcome the discussed security challenges of Blockchain technology. In addition, future research needs to investigate the other applications of Blockchain in government sectors, and further study has to focus in the security benefits and challenges of Blockchain when implemented in government sectors, Also future research needs to identify Blockchain testing Recently different kinds of Blockchains appear and over 700 cryptocurrencies are listed in [31] up to now. However, some developers might falsify their blockchain performance to attract investors driven by the huge profit. Besides that, when users want to combine blockchain into business, they have to know which blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different Blockchains.

References

[1] J. Berryhill, T. Bourgery, and A. Hanson, “Blockchains {Unchained},” *OECD Work. Pap. Public Gov.*, no. 28, 2018.

[2] K. Biswas and V. Muthukkumarasamy, “Securing smart cities using blockchain technology,” *Proc. - 18th IEEE Int. Conf. High Perform. Comput. Commun. 14th IEEE Int. Conf. Smart City 2nd IEEE Int. Conf. Data Sci. Syst. HPCC/SmartCity/DSS 2016*, pp. 1392–1393, 2017.

[3] D. Allessie, M. Sobolewski, and F. Vaccari, *Blockchain for digital government*. 2019.

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017.

[5] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain technology innovations,” *2017 IEEE Technol. Eng. Manag. Soc. Conf. TEMSCON 2017*, no. 2016, pp. 137–141, 2017.

[6] A. Alketbi, Q. Nasir, and M. A. Talib, “Blockchain for government services-Use cases, security benefits and challenges,” *2018 15th Learn. Technol. Conf. L T 2018*, pp. 112–119, 2018.

[7] N. Fedotova and L. Veltri, “Byzantine generals problem in the light of P2P computing,” *2006 3rd Annu. Int. Conf. Mob. Ubiquitous Syst. Netw. Serv. MobiQuitous*, 2006.

[8] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain Challenges and Opportunities : A Survey Shaoan Xie Hong-Ning Dai Huaimin Wang,” *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 1–24, 2017.

[9] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” *2017 IEEE Int. Conf. Syst. Man, Cybern. SMC 2017*, vol. 2017-Janua, pp. 2567–2572, 2017.

[10] J. Golosova and A. Romanovs, “The advantages and disadvantages of the blockchain technology,” *2018 IEEE 6th Work. Adv. Information, Electron. Electr. Eng. AIEEE 2018 - Proc.*, pp. 1–6, 2018.

[11] S. R. Niya *et al.*, “Adaptation of Proof-of-Stake-based Blockchains for IoT Data Streams,” no. c, pp. 15–16, 2019.

[12] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, “Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric),” *Proc. IEEE Symp. Reliab. Distrib. Syst.*, vol. 2017-Septe, pp. 253–255, 2017.

[13] T. J. Mizoguchi and S. J. Lippard, “Synthetic models of the deoxy and oxy forms of the non-heme dioxygen-binding protein hemerythrin [24],” *J. Am. Chem. Soc.*, vol. 120, no. 42, pp. 11022–11023, 1998.

[14] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, “Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism,” *IEEE Access*, vol. 7, pp. 118541–118555, 2019.

[15] B. Chase and E. MacBrough, “Analysis of the XRP Ledger Consensus Protocol,” 2018.

[16] University of Illinois at Chicago. Library., *First Monday*. Munksgaard International Publishers, 1996.

[17] I. Karamitsos, M. Papadaki, and N. B. Al Barghuthi, “Design of the Blockchain Smart Contract: A Use Case for Real Estate,” *J. Inf. Secur.*, vol. 09, no. 03, pp. 177–190, Jun. 2018.

[18] Techopedia, “What is Broadcasting? - Definition from Techopedia,” *Techopedia.com*. 2018.

[19] A. Alketbi, Q. Nasir, and M. A. Talib, “Blockchain for government services-Use cases, security benefits and challenges,” in *2018 15th Learning and Technology Conference, L and T 2018*, 2018, pp. 112–119.

[20] UK Goverment, “Distributed ledger technology: Beyond block chain,” *Gov. Off. Sci.*, pp. 1–88, 2015.

[21] “What Switzerland can teach the world about blockchain health.” [Online]. Available: https://espeoblockchain.com/blog/swiss-pharma-blockchain-health/. [Accessed: 27-Oct-2019].

[22] “Blockchain Technology in Banking &amp; Financial Services.” [Online]. Available: https://consensys.net/enterprise-ethereum/use-cases/banking-and-finance/. [Accessed: 03-Nov-2019].

[23] “Top 10 Friendly Countries For Blockchain Startups | Blockchain Council.” [Online]. Available: https://www.blockchain-council.org/blockchain/top-10-friendly-countries-for-blockchain-startups/. [Accessed: 24-Oct-2019].

[24] M. Snall, “Blockchain and the Land Register-a new &quot;trust machine&quot;?,” no. 572, 2014.

[25] S. Ølnes, J. Ubacht, and M. Janssen, “Blockchain in government: Benefits and implications of distributed ledger technology for information sharing,” *Gov. Inf. Q.*, vol. 34, no. 3, pp. 355–364, 2017.

[26] S. Angraal, H. M. Krumholz, and W. L. Schulz, “Blockchain technology: Applications in health care,” *Circ. Cardiovasc. Qual. Outcomes*, vol. 10, no. 9, pp. 1–4, 2017.

[27] S. van Engelenburg, M. Janssen, and B. Klievink, “Design of a software architecture supporting business-to-government information sharing to improve public safety and security: Combining business rules, Events and blockchain technology,” *J. Intell. Inf. Syst.*, vol. 52, no. 3, pp. 595–618, 2019.

[28] H. Hou, “The application of blockchain technology in E-government in China,” *2017 26th Int. Conf. Comput. Commun. Networks, ICCCN 2017*, 2017.

[29] B. Düdder and O. Ross, “Timber tracking: Reducing complexity of due diligence by using blockchain technology (position paper),” *CEUR Workshop Proc.*, vol. 1898, 2017.

[30] V. L. Lemieux, “A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation,” *D. Allessie, M. Sobolewski, F. Vaccari, Blockchain Digit. Gov. 2019.*, vol. 2018-Janua, no. 1, pp. 2271–2278, 2018.

[31] Coinmarketcap, “Cryptocurrency Market Capitalizations | CoinMarketCap,” *Coinmarketcap*, 2019. [Online]. Available: https://coinmarketcap.com/. [Accessed: 07-Nov-2019].