Blockchain for Government Services – Use Cases, Security Benefits and Challenges

Ahmed Alketbi
Industrial Engineering and Engineering Management
University of Sharjah
Sharjah, UAE
u00045915@sharjah.ac.ae

Dr. Qassim Nasir
Electrical and Computer Engineering Department
University of Sharjah
Sharjah, UAE
nasir@sharjah.ac.ae

Dr. Manar Abu Talib
Computer Science and Software Engineering
University of Sharjah
Sharjah, UAE
mtalib@sharjah.ac.ae

***Abstract*— Public sector and governments have been actively exploring new technologies to enable the smart services transformation and to achieve strategic objectives such as citizens satisfaction and happiness, services efficiency and cost optimization. The Blockchain technology is a good example of an emerging technology that is attracting government attention. Many government entities such as United Kingdom, Estonia, Honduras, Denmark, Australia, Singapore and others have taken steps to unleash the potential of Blockchain technology. Dubai Government is aiming to become paperless by adopting the Blockchain technology for all transactions by 2021. The Blockchain is a disruptive technology that is playing a vital role in many sectors. It's a revolutionary technology transforming the way we think about trust as it enables transacting data in a decentralized structure without the need to have trusted central authorities. Blockchain technology promises to overcome security challenges in IoT enabled services such as enabling secure data sharing and data integrity. However, it also introduces new security challenges that should be investigated and tackled. In this paper, we review the literature to identify the potential use cases and application of Blockchain to enable government services. We also synthesized literature related to the security of Blockchain implementations to identify the security benefits, challenges and the proposed solutions. The analysis shows that is huge potential for Blockchain technology to be used in to enable smart government services. This paper also highlights future research in the areas of concerns that required further investigation.**

Keywords—blockchain; information security; threats; risks;

I. INTRODUCTION

Nowadays, we are witnessing a widespread adoption of the new technologies within many sectors, such as public, industrial, energy as well as the service sector. Governments and public services entities are also adopting new emerging technologies to deliver the government services. Blockchain, a Distributed Ledger Technology (DLT), is a revolutionary technology that is transforming the way we think about trust as it enables transacting data in a decentralized structure without the need to have trusted central authorities [1]. Blockchain provides trustless decentralized data management in a transparent, auditable and immutable manner. 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". It is also known as "Mining" for bitcoin cryptocurrency. Bitcoin is the first practical application of Blockchain technology, and it was introduced in a white paper published by "Satoshi Nakamoto" [2]. Bitcoin is a Digital Currency (also referred to as Cryptocurrency) and a payment system that is using peer-to-peer network for online payments, where payments can be made directly between bitcoin network users without the need to have centralized authority or intermediary. Bitcoin is not regulated currency nor owned by any central bank/authority.

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". It is also known as "Mining" for bitcoin cryptocurrency. The Blockchain was developed in different types and features, such as public, private, permissioned and permissionless Blockchain, where all share the same concept, but differ in the functionality and the implementation.

Despite the growing interest in the use of Blockchain technology across various sectors, little studies examined the Blockchain technology and the security features/implications associated with adopting this distributed ledger technology. This research gap was discussed in [3] and the need to answer questions such as; "how can both trust and anonymity be guaranteed in such a platform-mediated network, and how can the risks be identified and mitigated?". Moreover, finding the appropriate solution to mitigate the security threats is another challenge that should be tackled.

II. BLOCKCHAIN COMPONENTS AND SECURITY

The Blockchain has basic building blocks and components that are independent of the Blockchain type, however, the implementation of these components may differ depending on

978-1-5386-4817-9/18/$31.00 ©2018 IEEE

the Blockchain type and application. In this section, the building blocks of Blockchain are described in details.

A. Blockchin Transactions

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 [4]. The transactions in Blockchain are programable, 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 [2]. 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 form a Blockchain in a form of a ledger, and the history of all transactions are maintained by every authorized node in the network.

B. Data Store

The ledger is the data store in Blockchain, in which a set of transactions from the unconfirmed pool are bound in block using the consensus algorithm, and the generated block is chained to the chain of previous blocks. Each block includes the hash output of the previous block in the blockchain.

C. Cryptography & Digital Signatures

Blockchain relies extensively on cryptography and digital signature throughout various steps in Blockchain operations. It is used to establish identity, authenticity and to allow relevant access.

- Hash

The hash function is a mathematical algorithm that takes any data as an input and generates a hash value as an output (value with a certain number of digits). The function generates completely different hash even if the input data is slightly changed. It is difficult to revert the original data by having the hash value only. This hash function is used in Blockchain for hashing the transaction message, and it is also used for the consensus algorithm such as Proof-of-Work. Miners need this algorithm to generate a hash value of all the transactions that is under a specific threshold [6].

- Public-Key Cryptography

Public-key cryptography uses public and private keys for encryption and decryption of messages. The sender can use the receiver's public key to encrypt the message, and only the receiver can decrypt the message using the private key (Nakamoto, 2008). This mechanism eliminates the need to share the keys between parties to encrypt and decrypt the message, known as symmetric-key cryptography. The public private keys are also used for the digital signature.

- Digital Signature

The cryptographic digital signature is used to prove authenticity of the data using the public-private key pairs. In digital signature, the sender encrypts the hash of the message using his/her private key, which then can be sent to the receiver along with the message. The receiver in this case also generates the hash value of the original message, and the authenticity can be verified against the hash value generated from decrypting the hash values that was sent by the sender using his/her public key [7].

D. Consensus – Synchronized Records

The blockchain maintains a single history of blocks using the consensus algorithms, which synchronize the records within the Blockchain to ensure blocks do not contain contradicting/invalid transactions. The consensus is known as mining in Bitcoin. There are multiple consensus algorithms used for Blockchain depending on its type and applications, this section discuss Proof-of-work and Proof-of-Stake [8].

- Proof-of-Work (PoW)

Proof of Work (PoW) is a mechanism to approve the distribution of ledger where it is used to confirm a block creation in Bitcoin. The block is created in Bitcoin after the successful generation of a hash value for a set of transactions from the unconfirmed transactions pool with a nonce. Nonce is arbitrary number, like a counter, that is used at most once within a session [9]. The participants in the network shall guess the nonce in order to be able to get a hash value that is smaller than a certain value set by the network. The network adjusts this value with the required level of complexity to keep the average processing time to 10 minutes. All network participants confirm and validate the block once a participant obtain the hash value, and the used transactions are at this stage are considered confirmed transactions. The participant that guessed the nonce value and created the block gets rewards of bitcoins [6]. The use of PoW proves that significant effort is spent in creating new blocks to prevent forgery of data, and it prevents double spending of bitcoins, and it makes modifications of confirmed transactions impossible [10]. In addition, the PoW helps in limiting the number of the blocks creation at the same time, but it is possible to have multiple blocks created at approximately the same time by different participants. This will result in accepting blocks creation by different nodes within the network, and it will result in having a fork in the chain of blocks. To resolve the fork, the network eventually agree on the longest branch to be approved as the confirmed Blockchain [11].

- Proof of Stake (PoS)

Proof of Stake (PoS) is a consensus algorithm alternative to PoW, in which the created block is chosen based on the wealth of the participant, hence the name Proof of Stack is given. The selection of the participant is in fact based on the randomized block selection or the coin age based selection [12]. In the randomized block selection, the selection is predicted in a random manner using a formula that uses the stack size (publicly known) and the lowest hash value. In the coin age based selection, the selection is based on the age of the coin in which participants holding coins for more than 30 days can start trying to sign a block. This selection method also uses the randomized block selection. Compared to PoW, it was shown that PoS has lower latency, requires less computational power, wastes fewer resources, and improves security for smaller chains [4].

III. Blockchain Technology Applications

Many sectors are exploring the use of Blockchain technology to enhance or lower the cost of their operations. Because of these drivers to adopt Blockchain technology, many applications were introduced for various sectors, and some applications were not thought of before the Blockchain invention. Swan categorized the potential applications of Blockchain into three categories, namely; currency, contracts and social applications beyond currency and financial markets [1]. These applications are summarized in Table I.

TABLE I. Blockchain applications discussed in [1]

	Currency	Contracts	Social Applications
Blockchain Applications	Currency transfer Remittance E-payment	Stocks Bonds Futures Loans Mortgages Smart property Smart contract	Government Health Science Literacy Culture Art

In addition, the applications of Blockchain were discussed in [6], which are related to digital identification, voting systems, and financial applications. The applications discussed in [13] are related to shared economy applications with the use of Blockchain and Internet of Things (IoT). The report published in [10] discussed that the Blockchain applications were expanded in the scope of recording and transferring the proof of ownership of various goods and rights. The expansion of the Blockchain applications was summarized in five stages as per the following:

A. Stage 1: Blockchain as a Ledger for Realizing Bitcoins

In 2008, Satoshi Nakamoto (known identity) published white paper introducing Bitcoin, which is the first Blockchain application [2]. Bitcoin is a Digital Currency (also referred to as Cryptocurrency) and a payment system that is using peer-to-peer network for online payments, where payments can be made directly between bitcoin network users without the need to have centralized authority or intermediary. Bitcoin is not regulated currency nor owned by any central bank/authority. In 2009, the Bitcoin was released as open source (version 0.2), and the Genesis Block (the first block in Blockchain) was created to enable the first Bitcoin transaction.

B. Stage 2: Blockchain for Managing Other Virtual Value

This stage also involved other virtual currencies, in which Blockchain was developed as open source and various cryptocurrencies were created as a result of recognizing Blockchain potential and effectiveness.

C. Stage 3: Application as Transaction Records

Considering the fact that Blockchain does not require a centralized authority to manage transaction, Blockchain was applied to manage transactions of goods and services and not only information such as the cryptocurrencies. Examples of such applications are the transfer of assets ownership such as vehicles or real estates.

D. Stage 4: Application as Records of Rights

At this stage of Blockchain applications expansion, the Blockchain is used as a record of ownership and rights to guarantee its authenticity. Examples of such applications are documents preservations and casting votes.

E. Stage 5: Records of Future Procedures and Processing (Automatization)

The automatization of processing is the aim to be achieved with Blockchain, in which programs are utilized to record future procedures and processing. For instance, the Blockchain can be used to escrow transactions, automatic execution of smart contracts and automatic processing by other devices such as in IoT use cases. For example, the blockchain can be used in IoT environment to manage IoT devices configurations, store sensor data and enable micro-payments [14].

IV. Blockchain Use Cases for Governments and Public Sector

Blockchain technology creates multiple opportunities when used in government services such as; operations cost reduction, reducing fraud and payments' errors and transparency of transactions between government agencies and citizens [15]. Various government entities around the globe are exploring the potential of Blockchain technology. The UK government released a report about the Distributed Ledger Technology potential for government services [15]. The report recommended exploring and testing blockchain technology in government services. In 2016, the UK government approved the Fintech startup Credits [16] to be the supplier for Blockchain technology for government services, and the UK government approved the use of Block-as-a-Service [17], [18].

Dubai Government has set up Global Blockchain Council, which is a public private initiative that brings government entities with local and international business/startups to foster Blockchain development with test cases. Dubai Multi Commodities Centre is engaged in a test case related to the authentication and the transfer of Kimberley certificates. The Emirates Integrated Telecommunication corporation (Du) is piloting a use case for health record to share data records between service providers [19].

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 & Record Keeping

This use case will help government entities to manage and maintain digital identities of individuals to support the processing various government applications. in this use case, individuals are having full control over their personal data, and

it allow the sharing of personal data with counterparties. In this case, counterparties do not need to store individual data which in result, reduce risks and increase compliance [20]. Estonia government is collaborating with Bitnation (the world's first operational Decentralized voluntary nation [21] to offer public notary 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, land titles, and other from anywhere in the world [8].

B. Value Registry

The use case of Assets registry started the second half of 2013 beyond cryptocurrencies use cases and it was called "Blockchain 2.0" [22]. The value registry use case overcomes the challenge of traditional document validation that relies on central authority. Due to the fact that Blockchain does not require centralized authority, users can store documents along with the signature and timestamp which can be validated by any participant in the network having the user's discretion [22]. Factom platform stores and proves the authenticity of records, documents or other types of data [23]. The first use case of Factom is Land Registry initiative in coordination with the government of Honduras, where Factom will store proof of land ownership that other government entities can rely on [24]. Government of Honduras are welling to use Blockchain to circumvent the land rights abuse that lasted for decades [25].

C. Voting systems

Governments can also utilize the Blockchain technology for implementing voting systems, which provide transparency in the voting process and maintains immutable records for the voting. This use case was first implemented by Danish political party [6]. The voting systems using blockchain can also be implemented with Liquid Democracy where voting can be delegated to other members, and it can be implemented with Random-Sample Elections models where voting is only for randomly selected member [1]. The voting can also be done for ideas that are published in Blockchain which gets the highest support by other members. Such complex discussion making system that maintains democracy is now feasible with the use of Blockchain technology [1].

D. Healthcare

The use of Blockchain will enable government entities to better provide health care services through keeping the health records of patients that can be shared with other service providers. And patients have the discretion to grant access to their health records to doctors, pharmacies, insurance companies, and other parties as needed. Another advantage of this use case is the transparency over the health care services and the associated cost. Moreover, storing the health records in Blockchain will support health research by having access to private and pseudonymous records of patients that is required for the research [1]. Blockchain will also enable governments in this use case to track delegations and accountability of health service providers advocacy, advice, and decision making for patients. Since IoT is also being used in healthcare facilitates in which it can integrate medical devices to use the generated data to have better medical decision, we believe the Blockchain will be used for such implementation to secure patient health records and give the data owner control over the sharing of their health records data.

E. Smart Cities & Internet of Things (IoT)

The IoT 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 has recently lunched Dubai Internet of Things strategy which aims at building the world's most advanced IoT ecosystem for Dubai smart city to improve people's lives. The integration of Blockchain with the Internet of Things has many use cases as it allow peer-to-peer communication between IoT devices, hence it enables the peer-to-peer market. Moreover, the Blockchain enables the tracking of assets throughout the supply chain using IoT. in this use case, the blockchain chain will be recording details about the asset such as status and location from IoT devices without the manual intervention from users [26].

Table II shows the use cases identified from the literature and its applicability to Dubai government services.

TABLE II. INTERNATIONAL USE CASES AND ITS APPLICABILITY TO DUBAI GOVERNMENT SERVICES

Use cases from international case studies	Applicability of the use case to Dubai government context
Identity Management and Record Keeping	Emirates ID Authority can manage electronic identity of UAE citizens, for record keeping and the use of this identity for any other government services
Value Registry & Assets Management	The registration of assists ownership such as vehicles for Dubai Road and Transport Authority, or lands in Dubai Land Department. This also has to facilitate a transfer mechanism of ownership in case of trading.
Voting System	Voting system can be used by the government for Federal National Council elections
Health Care Record keeping	Dubai Health Authority may use Blockchain technology to securely maintain health record data and enable the sharing of Data

V. BLOCKCHAIN SECURITY

This section presents the Blockchain security benefits and issues that were identified from the literature. The results are categorized according the CIA triad of Confidentiality, Integrity, and Availability, in addition to the Privacy and Accountability.

A. Availability

One of the advantages of the decentralized structure of Blockchain is the resistant to outages [27]. However, in [28], the authors discussed the possible Denial of Service (DoS) attacks in Blockchain and its impact on the availability of the network. The DoS attack can target slowing down the processing time of the miners by sending large number spam transactions, and

make the miners unavailable to confirm legitimate transactions. In Bitcoin, this attack impact can be further increased by allocating higher transactions fees to the spam transaction, which in turn will result in having higher priority for the processing of the spam transactions by the miners. In the permissioned Blockchain, such spam transactions can be detected and ignored, however, this can be also circumvented if the adversary has control over large number of nodes within the network.

B. Users Data Privacy

The privacy is one of the advantages of Blockchain Technology. In [29], the authors proposed a framwork using Blockchain enables users to have the control over sharing the community resources while preserving their privacy. This proposed framwork shows how the blockchain can be used to provide privacy for open and decentralized environments. Moreover, the model presented in [30] addresses the challenge of data sharing in open and decentralized environment such as the IoT. The proposed model allows users to have control over the access to the data they own on IoT devices. This model also enables users to share the data with other organizations or individuals while preserving the privacy by having a user oriented data dissemination and distribution system. The use of Blockchain in this model was in having a data store system to provide a decentralized storage for the access control. This model shows how the blockchain can be used with other systems to preserve users' data privacy, however, this research does not discuss the privacy benefits/challenges of Blockchain specifically.

Likewise, in [31], the authors used Blockchain to preserve users' data privacy by constructing a personal data management platform. In this platform, a protocol was implemented to use blockchain as an automated trustless access-control manager. The privacy is achieved in this platform by storing pointers to encrypted data in the ledger rather than transacting the data itself which in this case will be transparent to all nodes within the network. The user data privacy was also discussed in [32], where the authors implemented a proof of concept for the use of Blockchain technology for decentralized token-based energy trading system. This implementation used Blockchain technology combined with multi-signatures and anonymous encrypted message streams to achieve system security and privacy. Furthermore, a research conducted in [33] applied blockchain techniques in pervasive social network (PSN) based healthcare system. The implemented system aims at maintaining health data privacy by using the blockchain to share health data between PSN nodes.

It was concluded from the above research that in spite of decentralized structure of Blockchain, the user's data privacy can be preserved with the use of other combined techniques that is suitable for the application. In most of these cases, the argument is that the privacy can be achieved through the anonymity, where Blockchain can maintain the privacy of the data in case the transactions are encrypted and pseudonymous [32]. The authors in [34] argue that Blockchain implementations (such as Bitcoin) do not preserve the privacy of user data as the transactions flow transparently and exposed on the Blockchain. This applies to the blockchain implementations that use smart contracts, as the actions of smart contract are visible on the Blockchain to all nodes across the network.

In [35] the authors analyzed the anonymity of the transactions in bitcoin and demonstrated the ability to map Bitcoin addresses directly to IP address, even though new pseudonymous public keys were used. Similar research and anonymity attacks were demonstrated in [36] and [37] to analyze the anonymity of Bitcoin using transactional graph structures. The analysis conducted in [38] shows that Bitcoin exchange services' user can be linked to be provided identifying information. Additionally, the ledger can be downloaded and explored by all nodes within the permissionless ledger, in which the history can be viewed. Another challenge with the use of blockchain technology is the removal of transactions from the ledger (also known as the "right to be forgotten") as the ledger is immutable [28]. Smart contract access to data also forms another challenge with user data privacy, as a smart contract may leak the data in case it has access to it [28]. The authors in [34] proposed a framework from Blockchain system that uses smart contract and retains transactions privacy through encrypting the transactions. The authors argued that the developed framework guarantee security by achieving transactions privacy and contractual security. The contractual security includes the confidentiality, authenticity and the financial fairness between the parties in the contracts in case of cheating.

C. Data Integrity, Reliability and Authenticity

The Blockchain promises data integrity and prevention of the unauthorized change of data by the use cryptography. These features are behind the adoption of the Blockchain technology in may applications. In [39], the authors proposes a security framework for smart cities & IoT that uses Blockchain for the database layer. In [40], the authors proposed the use of Blockchain to ensure the integrity of IoT devices firmware, by maintaining reference integrity metric (RIM) of the firmware to facilitate compromised firmware detection and self-healing. In [41], the authors proposed a blockchain-based framework that can be used as a Data Integrity Service for IoT data. The framework can be used by IoT data owners or consumers to verify data integrity without relying on third party auditors.

Moreover, the authors in [42] explored the potential security benefits of a blockchain for information distribution in IoT. it was learned that the Blockchain can overcome the security challenges in IoT such as the Identification and trust management of IoT devices, Provenance verification and information tracking, Authentication and Access control, and finally, the Accountability in IoT based applications. Nevertheless, the integrity of blockchain was discussed in some publications to be in question due to the consensus hijack (also known as "51%" attack). In the 51% attack, in which malicious/dishonest nodes owns the majority of the network processing power, which allows tampering the validation process and producing new blocks faster than the rest of the network. The faster production of the block will result in considering this chain as a valid chain by the rest of the network [28]. This will eventually help the adversary in performing double spending attack [43].

In [44], Jennifer explored the fraud and malicious activities that can be prevented by blockchain technology in financial application. According to Jennifer, double spending and record tampering are the malicious activities that can be prevented due to the complexity of the mining process and the distributed consensus of Blockchain. This research also discussed the attacks to which blockchain remains vulnerable, such as the 51% attack, identity theft, illegal activities and system hacking. The research recommended defensive and preventive measures that can be used to mitigate the risk of the malicious activities, these recommendations are summarized in Table III. The recommended defensive and preventive techniques are discussed on a high level and no novel security measure was proposed as part of this research, further research is required on the proposed recommendations.

TABLE III. MALICIOUS ATTACKS TO BLOCKCHAIN AND DEFENSIVE MEASURES [44]

Malicious Attack	Defensive & Preventive Measures
51% Attack	Detection techniques; wide adoption of the blockchain technology
Identity Theft	Identify and reputation blockchains
Illegal Activities	Detection techniques; laws and regulations
System Hacking	Robust systems and advanced intrusion detection methods

Victoria Lemieux explored in [25] the value of Blockchain technology as a solution to the creation and preservation of digital records for a land registry system in a developing country. Lemieux also presented some of the limitations risks and opportunities of the proposed approach. In a nut shell, the analysis suggested that Blockchain technology can maintain records integrity and address the related security issues. This is true with the assumption that appropriate infrastructure controls are in place. On the other hand, the analysis showed that blockchain does not guarantee reliability of records due to several threats/vulnerabilities. These threat/vulnerabilities are summarized below;

- Control of Blockchain

The fact of not having control over the nodes, which validates the transactions (given the nature of public ledge technology), may result in having records authenticity issues. If the transactions validation is controlled by malicious nodes then inauthentic records may be added to the blockchain. A report published in [45] shows that a secretive group owns six sites for massive mining operations. The six sites generates more than a $1.5 million a month which is equivalent to 3% of total Bitcoin network. This is also a concern for the blockchain use case for record keeping and how the records authenticity are controlled.

- Reliability

The record reliability depends on the control exists for the creation of records if the entries are created outside the Blockchain system by specific authority. In the context of the land registration discussed by Lemieux, the registration of land is done by a "Property Institute" which is then added to the blockchain platform. Therefore, unreliable records may be created in the blockchain due to the lack of control over the records outside the platform.

- Authenticity

Even though the Blockchain technology is immutable and promises transactions integrity, there are cases where the records authenticity maybe impacted. Table IV shows the vulnerability/attacks that may affect records authenticity.

D. Authorization, Accountability and Identity Management

On the accountability, the application proposed in [46] uses the Blockchain technology to authorize users connecting to public WiFi networks, and that enables the accountability and allows disabling malicious usage of the network. In addition, this implementation uses Blockchain to enable the encryption of the communication with the use P2P network addresses as encryption keys.

Furthermore, the Blockchain was used in [47] to address the identity management challenge that exists in reputation systems, which is ensuring the user has only one identity to prevent exploiting the reputation system with multiple identities for the same user. The proposed system used the IP address to link the identity creation in the Blockchain. The argument for that is that IPV4 addresses are becoming expensive to purchase. However, this method does not prevent the user from creating multiple identities.

TABLE IV. AUTHENTICITY VULNERABILITIES/ATTACKS PRESENTED IN [25]

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 requests repeatedly 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

E. Smart Contract Management

The smart contract management is another challenge that has to be considered and tackled when adopting Blockchain technology. The creation of the smart contract is susceptible to errors as it is based on code, and the errors increase proportionally with the complexity of the smart contract. Peter Vessense conducted a quality review on Ethereum contracts and identified that likely bugs per line of code exceeds 100 per 1000 lines, and the majority of these bugs are security flaws [48]. One example of such bug is the vulnerability exploited in Decentralized Autonomous Organization (DAO) that is based

on Ethereum Blockchain and smart contract. This attack was called “recursive split“ and it took place on 17 June 2016. The vulnerability existed in the DOA smart contract which has a split function that was called recursively to update the token balance of the attacker and to withdraw funds more than what they should. This attack resulted in stealing more than $59m in Ether which is equivalent to $150M [49].

The challenge with smart contract management was also reported in the European Union Agency For Network and Information Security (ENISA) report titled “Distributed Ledger Technology & Cybersecurity” [28]. As a good practice for smart contract management, ENISA is suggesting the code review of smart contract and the standardizations of regular functions in into libraries that can be approved for use. Nevertheless, even with adopting these good practices, it is still possible to have unknown vulnerabilities within the smart contract code [28].

Another challenge with smart contract management is the use of proof-of-stack consensus. This is because the proof-of-stack is a deterrence control against malicious act, in which the value of the coin will be reduced if malicious act is detected [50]. This deterrence control may not be effective for smart contract management. Therefore, the authors in [50] proposed a new consensus method which is based on the collapse of credibility in addition to the coin value (as in proof-of-stack method).

F. Key management and Cryptography Challenges

The Key management refers to the generation, exchange, storage use and revocation of cryptographic keys. The Blockchain operations depend mainly on the use of public and private keys to produce and verify digital signature and to encrypt data. Therefore, the unauthorized access to a user’s private keys will result in a compromise of the confidentiality, integrity and authenticity of the user transactions. The unauthorized access to the private keys can be achieved using the traditional attack techniques such as malware infections. On the other hand, the attacker could attempt the reproduction of the user’s private keys since these attempts can be done passively without the knowledge of the target and it is not limited [28].

The complexity behind the key management can be attributed to the fact that effective key management includes defining system policy, users security awareness, organizational and departmental coordination and interactions. This complex key management makes the private keys vulnerable to unauthorized access [25]. Another challenge is the creation of weak encryption keys which makes the keys vulnerable to brute force attacks. The reason behind the weak encryption keys can be due to the use of misconfigured software or the use of random number generators with limited range [28].

VI. Conclusion

Blockchain is a revolutionary technology that is transforming the way we think about trust as it enables transacting data in a decentralized structure`` without the need to have trusted central authorities. Blockchain is Distributed Ledger Technology (DLT) that provides trustless decentralized data management in a transparent, auditable and immutable manner. This study explored the potential applications and use cases of the Blockchain technology for government services. The study shows that there is huge potential in the use of Blockchain for government services since it can deliver government services in a cheaper, distributed and voluntary way. In addition, this research included literature review to identify the possible security benefits and challenges of Blockchain technology. 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 IoT implementations, and further study has to focus in the security benefits and challenges of Blockchain when implemented for IoT environments.

Acknowledgment

We would like to thank Sharjah University Graduate Studies office, Dubai Electronic Security Center, Emirates Islamic Bank, and OpenUAE Research and Development Group at University of Sharjah for funding this research.

References

[1] M. Swan, Blockchain: Blueprint for a new economy., CA, USA: O'Reilly Media, Inc, 2015.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 7 March 2017].

[3] J. R. M. a. T. V. Lindman, "Opportunities and risks of Blockchain Technologies in payments – a research agenda," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, Hawaii, 2017.

[4] M. Swan, Blockchain: Blueprint for a new economy., CA, USA: O'Reilly Media, Inc, 2015.

[5] M. N. P. P. V. S. K. V. Crosby, "BlockChain Technology: Beyond Bitcoin," *Applied Innovation Review,* no. 2, pp. 6-19, 2 June 2016.

[6] M. Pilkington, "Blockchain Technology: Principles and Applications," 2015.

[7] D. M. A. a. V. S. Johnson, "The elliptic curve digital signature algorithm (ecdsa)," *International Journal ofInformation Security,* vol. 1, no. 1, pp. 36-63, 2001.

[8] J. Mattila, "The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures," *ETLA Working Papers,* 2016.

[9] P. Rogaway, "Nonce-Based Symmetric Encryption," in *International Workshop on Fast Software Encryption*, Delhi, India, 2004.

[10] Nomura Research Institute, "Survey on Blockchain Technologies and Related Services," Nomura Research Institute, 2016.

[11] M. Rosenfeld, "Analysis of hashrate-based double spending," arXiv preprint arXiv:1402.2009, 2014.

[12] S. a. N. S. King, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," 2012.

[13] S. B. R. W. M. a. B. N. Huckle, "Internet of things, blockchain and shared economy applications," in *International Workshop on Data Mining in IoT Systems (DaMIS 2016), Procedia Computer Science*, 2016. ``

[14] R. D. M. Samaniego, "Blockchain as a Service for IoT," in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2016.

[15] UK Government Chief Scientific Adviser, "Distributed Ledger Technology: beyond block chain," Government Office for Science , 2015.

[16] "Credits," 2017. [Online]. Available: https://credits.vision/. [Accessed 28 April 2017].

[17] D. Palmer, "Blockchain-as-a-service approved for use across UK government," 3 August 2016. [Online]. Available: http://www.zdnet.com/article/blockchain-as-a-service-approved-for-use-across-uk-government/. [Accessed 28 April 2017].

[18] L. Barber, "The UK government now has its first official blockchain provider for public services," 1 August 2016. [Online]. Available: http://www.cityam.com/246605/uk-government-now-has-its-first-official-blockchain. [Accessed 28 April 2017].

[19] S. Kerr, "Dubai turns to blockchain for domestic challenges," 7 October 2016. [Online]. Available: https://www.ft.com/content/48ff547c-53e7-11e6-9664-e0bdc13c3bef. [Accessed 28 April 2017].

[20] D. W. W. a. P. A. Shrier, "Blockchain & Infrastructure (Identity, Data Security)," Massachusetts Institute of Technology, 2016.

[21] "BITNATION: Governance 2.0," 2017. [Online]. Available: https://bitnation.co/. [Accessed 28 April 2017].

[22] Labs in EVRY Financial Services, "Blockchain: Powering the Internet of Value," EVRY Financial Services, 2015.

[23] "Factom - Making the World's Systems Honest," 2017. [Online]. Available: https://www.factom.com. [Accessed 28 April 2017].

[24] S. Underwood, "Blockchain Beyond Bitcoin," *Communications of the ACM,* vol. 59, no. 11, pp. 15-17, November 2016.

[25] V. L. Lemieux, "Trusting records: is Blockchain technology the answer?," *Records Management Journal,* vol. 26, no. 2, pp. 110-139, 2016.

[26] M. D. K. Christidis, "Blockchains and Smart Contracts for the Internet of Things," *SPECIAL SECTION ON THE PLETHORA OF RESEARCH IN INTERNET OF THINGS (IoT),* vol. 4, pp. 2292-2303, 2016.

[27] H. a. Z. Z. Zhu, "Analysis and outlook of applications of blockchain technology to equity crowdfunding in China," *Financial Innovation,* vol. 2, no. 29, pp. 1-11, 2016.

[28] Hon, W. K. Palfreyman, J. and Tegart, M., "Distributed Ledger Technology & Cybersecurity," European Union Agency For Network And Information Securit (ENISA), 2016.

[29] P. R. J. a. L. K. Kianmajd, "Privacy-Preserving Coordination for Smart Communities," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, San Francisco, CA, USA, 2016.

[30] S. H. F. F. R. P. C. R. H. Hashemi, "World of Empowered IoT Users," in *First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Berlin, Germany, 2016.

[31] G. N. O. P. A. Zyskind, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *Security and Privacy Workshops (SPW), 2015 IEEE*, San Jose, CA, USA, 2015.

[32] N. a. S. D. Aitzhan, "Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and Anonymous Messaging Streams," *IEEE Transactions on Dependable and Secure Computing,* vol. PP, no. 99, pp. 1-1, 12 October 2016.

[33] J. X. N. a. H. X. Zhang, "A Secure System For Pervasive Social Network-Based Healthcare," *Special Section on Trust Management in Pervasive Social Networking (TruPSN),* 29 December 2016.

[34] A. M. A. S. E. W. Z. P. C. Kosba, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in *In Proceedings of the 2016 IEEE Symposium on Security and Privacy*, SP '16, 2016.

[35] P. K. D. a. M. P. Koshy, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," in *International Conference on Financial Cryptography and Data Security . FC 2014: Financial Cryptography and Data Security*, Christ Church, Barbados, 2014.

[36] S. P. M. J. G. L. K. M. D. G. e. a. Meiklejohn, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *Communications of the ACM,* vol. 59, no. 4, pp. 86-93, 2013.

[37] D. S. A. Ron, "Quantitative Analysis of the Full Bitcoin Transaction Graph," in *International Conference on Financial Cryptography and Data Security*, Berlin, Heidelberg, 2013.

[38] P. a. I. A. S. M. Reynolds, "Tracking digital footprints: anonymity within the bitcoin system," *Journal of Money Laundering Control,* vol. 20, no. 2, pp. 1-16, 2017.

[39] K. a. M. V. Biswas, "Securing Smart Cities Using Blockchain Technology," in *IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems*, Sydney, NSW, Australia, 2016.

[40] J. L. K.-K. C. M. Banerjee, "A blockchain future to Internet of Things security: A position paper," in *Digital Communications and Networks*, 2017.

[41] X. L. Y. S. C. X. X. a. L. Z. B. Liu, "Blockchain based Data Integrity Service Framework for IoT data," in *IEEE 24th International Conference on Web Services*, 2017 .

[42] a. N. F. G. C. Polyzos, "Blockchain-assisted Information Distribution for the Internet of Things," in *IEEE International Conference on Information Reuse and Integration (IRI)* , 2017.

[43] C. R. C. Pinzon, "Double-spend Attack Models with Time Advantange for Bitcoin," *Electronic Notes in Theoretical Computer Science (ENTCS),* vol. 329, no. C, pp. 79-103, December 2016.

[44] J. J. Xu, "Are blockchains immune to all malicious attacks?," *Xu Financial Innovation ,* 2016.

[45] E. Franco, "Inside the Chinese Bitcoin Mine That's Grossing $1.5M a Month," 6 Feb 2015. [Online]. Available: https://motherboard.vice.com/en_us/article/chinas-biggest-secret-bitcoin-mine. [Accessed 29 March 2017].

[46] T. a. I. H. Sanda, "Proposal of New Authentication Method in Wi-Fi Access Using Bitcoin 2.0," in *5th Global Conference on Consumer Electronics*, Kyoto, Japan, 2016.

[47] R. O. G. Dennis, "Rep on the block : A next generation reputation system based on the blockchain," in *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, 2015.

[48] P. Vessenes, "Ethereum Contracts Are Going To Be Candy For Hackers," 16 May 2016. [Online]. Available: http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/. [Accessed 17 April 2017].

[49] P. Daian, "Analysis of the DAO exploit," 18 June 2016. [Online]. Available: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/. [Accessed 17 April 2017].

[50] H. F. S. N. A. M. Y. A. A. K. J. Watanabe, "Blockchain Contract: Securing a Blockchain Applied to Smart Contracts," in *2016 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2016.

[51] J. F. S. a. Y. J. Zhao, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," *Financial Innovation,* vol. 2, p. 1, December 2016.

[52] "Blockchain Technology Glossary," 2016. [Online]. Available: http://www.blockchaintechnologies.com/blockchain-glossary. [Accessed 29 March 2017].

[53] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things Journal,* vol. 1, pp. 3-9, 2014.