International Journal of Management and Commerce Innovations ISSN 2348-7585 (Online)
Vol. 9, Issue 2, pp: (242-253), Month: October 2021 - March 2022, Available at: www.researchpublish.com

Secured File Storage and Retrieval Using Public Blockchain Network

Vilma Mattila; Prateek Dwivedi; Pratik Gauri, Md Ahbab

5ire (Sustainable Distributed Computing)

160 City Rd, London, United Kingdom

Email of Corresponding Author: muhammadahbab92@gmail.com

***Abstract*: With increased security from encryption, and cheaper from decentralizing cloud storage, the blockchain is transforming this business around the world. All industries have storage requirements not only to process but also to compute huge amounts of data. Blockchain-based storage is emerging as a better alternative to traditional cloud storage systems. This study shed lights on public blockchain network in secured file storage and prospects. The study conducted a secondary data analysis based on different academic and public databases and this qualitative study helps to identify some recent cases of using public blockchain network, impacts, and prospects.**

***Keywords:* Digital Transformation; Cryptocurrency; IoT; Cloud Storage; Bigdata; Blockchain.**

1. INTRODUCTION

Since there are hierarchical layers to organize and maintain data, the scope for human error is quite high (Shirley et al., 2015). That puts the security of our data at risk. Hence, what is the alternative? Few small teams and organizations in the world have started using blockchain-based storage. It helps them in three significant ways:

- Significantly reduces the possibility of human error (Faccia et al., 2019).
- It increases the security and general privacy of any data (Hassan et al., 2020).
- Compared to traditional cloud storage, blockchain-based storage is cost-effective and efficient (Arshad et al., 2021).

As for 20 years of digital communication and e-commerce platforms, blockchain transformed business models and technologies to revolutionize the way we people and companies interact. The blockchain allows to implement a public database distributed and immutable based on increasing sequence of blocks (Ortega et al., 2019). This database intrinsically provides fault tolerance in nodes, robustness against manipulation, and being public transparency. The uses of this technology are potentially immense and for that reason it is considered as a of the technologies with the most disruptive potential of the previous years(Wüst and Gervais, 2018). The possibility of having distributed database and immutable posteriori has a myriad of practical utilities that only begin to glimpse. Cryptocurrencies have been first successful application due to the security and transparency needs of the payment systems and the possibility of eliminating intermediaries (Wüst and Gervais, 2018). In the future, however, it is possible that finding blockchain systems compulsory in an infinity of contexts and systems. In this sense, use cases can be considered in scenarios such as the Internet of Things (IoT) and big data.

2. LITERATURE REVIEW

Blockchain means "block chain". These blocks, linked together linearly and chronologically, contain information such as transaction records as well as a “fingerprint” hash. When the number of records in a block reaches its capacity maximum, so other computers on the network work on validation to append it to the blockchain (Liu et al., 2019). In the bitcoin context, this validation process is known as mining. To validate the blocks, several machines work on the solution of a puzzle. Then it attaches the new block to the chain that is known as Proof of Work (Chin et al., 2020). Then the new block receives information from previous blocks. Information within the blockchain can be considered reliable, validated and attached to the block chain (Lemieux, 2017). Hash functions are unidirectional, with arbitrary length message input and fixed value hash output. This hash value is a type of signature for the incoming message. As it is a unidirectional function,

the calculation of hash value from a given message is simple. Hash functions are used in security applications such as authentication, integrity verification of messages, certificates and signatures digital. The security of these applications depends on the cryptographic strength of the function. Therefore, some security properties are needed to make a hash function H suitable for such cryptographic uses (Maetouq et al., 2018, Chen et al., 2021):

- **P1**. Given a hash value of *h*, it should be hard to find any message *m* such that $h = H(m)$
- **P2**. Given an m_1 message, it must be hard to find another one. message $m_2 \neq m_1$, where $H(m_1) = H(m_2)$.
- **P3**. It must be difficult to find different messages m_1 and m_2 so that $H(m_1) = H(m_2)$.

Thus, the hash is a mathematical function that generates a code unique identifier for each block of data that is appended to content of each transaction. If something changes in the block, then the result of that function also changes. The blockchain has numerous blocks linked to each other by these unique identifiers. New blocks are added linearly and chronologically (Bandara et al., 2018). Satoshi Nakamoto suggested a solution to the double spending problem using a peer-to-peer distributed timestamp server to generate proof computational analysis of the chronological order of transactions (Akbar et al., 2021). PoW involves solving a puzzle, which is not more than a consensus algorithm such as Proof of Stake (PoS). This depends on the hash function that is applied to the entire content of the block: hash value of the previous block, transactions and an arbitrary number – nonce. The nonce is the only part of the block that the node can change in order to solve the puzzle. The result must start with n number of bits zero. The average work spent in this process is exponential to the number n of zero bits required and can be verified by executing a single hash. Solving this problem is by "brute force" and needs of great computational power. PoW protocols are efficient for deter abusive attacks such as spam. Since the necessary computational effort has been spent to satisfy the PoW system, the block can be attached to the blockchain and should not be changed without this work being redone. As subsequent blocks are linked to that chain through the hash, the change work would require changes from later blocks as well (Altarawneh et al., 2020). In many cryptographic protocols, a tester tries to convince a verifier that he has knowledge of a secret or that certain mathematical relationship. In contrast, in a PoW, a tester demonstrates to a tester that he has performed a certain amount of computational work in a time span specific. As PoW is a consensus algorithm, it also determines representation of the majority in decision-making processes (Aste et al., 2017).

3. METHODOLOGY

An in-depth study of blockchain technology conducted by addressing an analysis of qualitative characteristics of its procedures, architecture and operating core. Different techniques and means of use described to determine the purposes that a user could potentially use this technology. This study is dedicated to studying challenges and implementation for the public sector and analyzes the adoption challenges, conditions under which the technology adds public value and the preconditions for sustainable implementation. The overall study follows secondary data analysis from some public databases related to blockchain, random government press release and scenario cases.

4. ANALYSIS AND DISCUSSION

Lack of confidence to make transactions (economic, legal, bureaucratic) that has been for centuries a collective problem that humanity has tried to solve through actors that different parties trust(Aste et al., 2017). In many cases these actors have become both public and private institutions. For example, when two people who do not know each other want to make a transaction electronic payment, must have the participation of a third party (such as bank or credit card issuer) for the transaction to be carried out cape. In fact, the government often has to become an intermediary to legally validate documents, prove the identity of people or certify eligibility to access social programs, among others. Recently a technology has emerged with the potential to replace the need trusted with a cryptographic proof (Nakamoto, 2008). Applied initially to financial transactions through the cryptocurrency Bitcoin, blockchain technology can introduce distributed logic and decentralized to transact in a manner safe and reliable without the need for a trusted third-party participant. The addition of so-called smart contracts facilitates the automation of processes through the establishment of rules that will be executed without the need for intermediaries if certain requirements are met preset that added to the confidence that the technology promises, raises in principle important challenges to the public sector whose institutions are accustomed to operating in the antitheses of this logic (Kewell et al., 2017). At present many governments are beginning to explore blockchain technology to provide best services. The current situation of implementation of solutions based on blockchain generating more noise than blocks although there are many concepts and pilots that are being carried

out are few who go to a stage of deployment to scale. It is very likely that this low level of adoption obeys the nascent state of technology and a lack of enabling conditions that allow it to escalate (Grant et al., 2015).

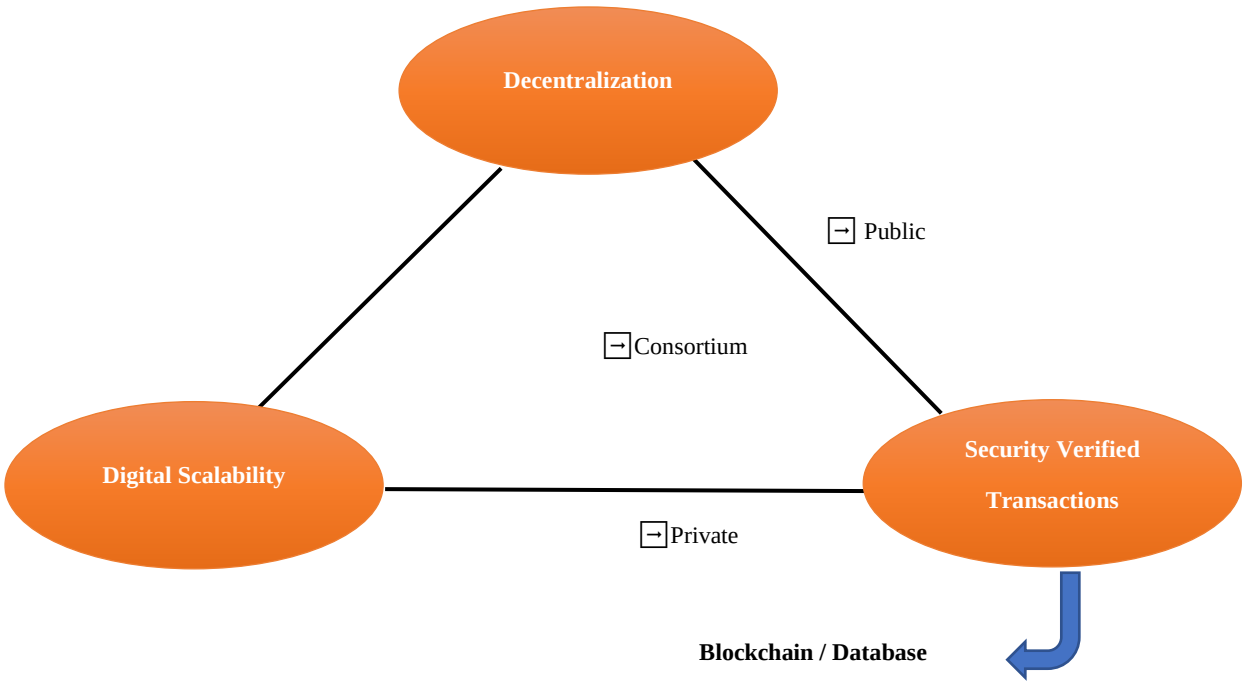
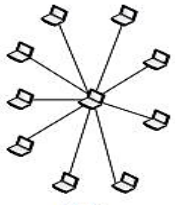
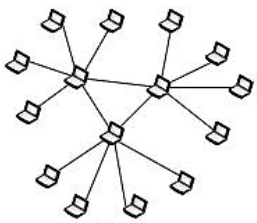


Fig. 1: Blockchain Valuation (Internet of Value and Smart Transactions)

Blockchain networks can be classified as public, consortium or private blockchain in order of decreasing degrees of openness available for participation by nodes (see figure below) (Ghosh et al., 2021). Here, we provide a brief overview of the three architectures. The public blockchain is also referred to as a permissionless blockchain since any node can enter and exit the network freely. The public chain is the earliest and most widely used blockchain architecture. Bitcoin is the most widely known example of the public blockchain. The private blockchain is also known as the permissioned blockchain and is only used in private organizations or institutions. Unlike public blockchains, private blockchains are generally not open to the outside world. The consortium blockchain is a hybrid architecture comprising of features from both public and private blockchains. A consortium blockchain is also a permissioned blockchain, in which participation is limited to a consortium of members to participate; each node might refer to a single organization or institution in the consortium.

Public Blockchain	
Private Blockchain	

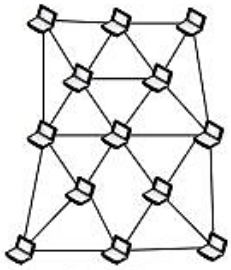
Consortium Blockchain	

Fig. 2: Blockchain networks

4.1. Implementation of Blockchain in The Public Sector

Introducing new technologies into the public sector can be a complex task that requires generating capacities within the administration and rules of the game clear for its proper implementation and, above all, lay the foundations - regulatory, budgetary, political - for its sustainability. At present several experiences using blockchain technology consist of pilots implemented in isolation with little relationship in other public institutions and in many cases deployed in parallel to the public policy design process and the current legal and regulatory framework. In part this may be due the lack of maturity of the technology, which prevents the use of all its attributes on a large scale due to issues such as speed of transactions, consumption of energy and the size of the blocks (Carson et al., 2018). However, just as described in the second part, several of these pilots have generated incentives positive factors to promote public innovation, efficiency in the provision of services and digitization of systems. Various studies that analyze the use of blockchain technology have focused on in evaluating the feasibility of its implementation (Khalil and Gervais, 2017).

4.2. Challenges Blockchain Technology in The Public Sector

Blockchain can become in a disruptive solution for governments since it enables the design of a distributed and decentralized logic in the provision of public services (Zambrano et al., 2018). In short, some government functions can greatly use blockchain such as log events (the change ownership of a vehicle or property), verify facts (for example, check the payment of taxes or grant education credentials) and verify compliance with standards (certificates sanitation for restaurants, between others) (Wang et al., 2022). Nevertheless, the implementation of a sustainable and successful blockchain technology faces some challenges: (i) organizational and governance, (ii) technological, (iii) regulatory, (iv) resources (v) use and generation of the ecosystem.

To eliminate the need for intermediaries, blockchain technology introduces rules-based governance determined code in the form of a protocol with a mechanism consensus depending on the type of actor. In these days, it is difficult to change governance systematically. High-level technology challenges are link to the governance to the use case under analysis and to decentralization of the storage of the information. Move from a centralized solution to a decentralized always implies greater complexity. At most basic level move from a system in which a single actor verifies one in the one that many actors share this responsibility requires the use of a consensus protocol, which adds delays depending on which one is chosen.

Similarly, move from a system in which a trusted third-party storage data in a centralized silo to one in which the data is stored in a distributed network often requires add layers of encryption to establish controls over who sees the information. Additionally, the high cost of store the data in a replicated way on the blockchain will force participating organizations to develop storage solutions outside of the chain, which will further complicate plus the way they are administered and secure the data (Pisa, 2018).

Another technological challenge is linked to architecture technological. In most cases of use that have been thought for the public sector, in addition to the chain there are two components that make up the technological solution: (i) the interface with users (usually on the web) that allows them to interact with the system and (ii) a base data, since the string should only store the resulting hashes to encrypt the information (López, 2018). It is important highlight that for a process can be migrated to a solution based in blockchain all information must be digitized so that it can be used and also the processes must be automated. In this regard, the interface of user is extremely important to democratize the use of the solution, therefore that it is recommended to pay special attention to design and user needs. So that the solution being

designed be safe and have potential to be scalable, a third challenge involves with public key infrastructure (PKI) that enables cryptographic transactions (for example, encryption, digital signature, electronic transactions). That is to say, to implement a solution based on blockchain, governments must have the right mix hardware, software, policies and procedures security to perform electronic transactions so safe. This infrastructure facilitates handling digital signatures in environments where the parties involved do not have the opportunity to verify authenticity of first-hand signatures, giving confidence that a firm digital represents the person who indicates. In addition, a PKI can facilitate the scalability of the solution, since the more parties are involved in a network it is more likely that parties do not know or trust the digital signatures of others. Despite of this, a traditional PKI introduces elements of intermediaries (authorities' certification and registration), for which models are emerging decentralized (decentralized public key infrastructure [DPKI]) trying resolve this issue. Anyway, it's worth noting that the blockchain permits such as the BFA will work as a PKI, since there is an authority centralized registry, and a decentralized certification Other related challenge are volume and type of data that is stored in chain.

Blockchain technology currently does not have the capacity to store large volumes of data due to high cost of replication to multiple nodes and their consequent synchronization (Serale et al., 2019). For this reason, it is recommended store non-transactional data on a basis of separate data and only store the hashes of this data in the string of blocks. While this architecture ensures the integrity and security of the original data, one of the fundamental characteristics of blockchain technology: distribution of the data and its verifiability (Holotescu and Software for EducationBucharest, 2018).

In addition, there is a linked challenge to computational processing consumption and energetic technology in public networks with certain consensus protocols. For encourage competition for mining of blocks - which consists of finding the code that concatenated to the data of the block results in a hash valid - which guarantees the safety of chain, several consensus mechanisms that reward with cryptocurrency to the winner of that competition for each block. Some of these, such as the so-called proof of work (PoW) which is currently the most known for its use in cryptocurrency Bitcoin and on the Ethereum platform, incite the "miners" to employ high computational processing volumes, which entails a very high energy. At the software level, the technological challenges consist of getting the networks are capable of processing a higher number of transactions per second that the permitting of new nodes and channel operation private in public-permissioned networks are more efficient and that different networks are interoperable (Liu et al., 2020). However, achieving this goal does not it's so easy because different networks have different consensus protocols, and there is currently no standard for exchange data between the different blockchains.

4.3. Successful Implementation of Blockchain Technology in Business or Public Sector

Blockchain has characteristics that make it an attractive technology for the elimination of intermediaries and enable a series of public information registry services. However, as in any decision technology, it is important to analyze which technology is best suited to the current requirements and possible future business scenarios.

If it is determined that blockchain is the appropriate technology for a process to be digitized or made more efficient, however, it is necessary to analyze the framework regulatory and the demand for computing infrastructure to be used, before taking a definitive decision (López-Zambrano et al., 2021). It cannot be ignored that there is still confusion about the use of blockchain technology and that much of the information that the market handles come from companies' technology providers, which often promote their own solutions above international standards that would favor greater interoperability. This misinformation causes characteristics to be attributed to blockchain that are not native or that can be achieved by other technological means at a much lower cost. As for example: information security, ease of integration, automation of contracts, among other aspects.

Without trying to skew the possibility of each organization analyzing its own processes to determine the applicability of blockchain, some questions arise general issues that must be resolved for a successful implementation:

Considerations for the decision
➢ How many nodes will make up the network?
➢ Is the network large enough in number of nodes and processing to be safe?
➢ Should my organization have processing and storage capacity for the network-wide transactions?
➢ Are there restrictions and / or regulations related to data protection? Is there information to be shared? And which of it can be shared with the entire network?

➢ Who owns the original information and that generated by the network?
➢ Are there restrictions on the persistence and storage of the data?
Implementation Considerations
➢ Are the cases that are being implemented in blockchain focused on the transformation of operational processes?
➢ Is my solution open and neutral? What does this mean for my business?
➢ Do you use agile development methodologies that allow incremental implementation to analyze the success of the development and the eventual impacts it generates on other areas and systems?
➢ In case of problems, do I have the possibility to go back?
➢ Can I have the capacity to correct quickly and cheaply, without affecting my daily operations?
Performance Considerations
➢ How much is the investment required to provide the level of storage and processing required to meet blockchain needs? Does this investment will it generate profits for the business?
➢ Are the response times projected by the solution consistent with the nature of my business? This is especially important when transactions are sensitive to fluctuations in values in short periods of time, such as commodities, currencies and other internationally tradable securities.
Considerations related to logistics business rules
➢ What is the real cost and return on investment (ROI) of a blockchain development?
➢ Can blockchain expectations be satisfied by another technological alternative? For example, smart contracts are not an exclusive application of blockchain, it is also possible with other mature technologies that allow the same at a lower cost.
➢ When is it too early / late to develop blockchain solutions?
Considerations related to data management and information security
➢ Does it represent any risk for the company to share the commercial information?
➢ Who is the owner of the data recorded and stored by the blockchain, especially when these are open and public or hybrids?
➢ Who has the right to collect, access, modify, delete or commercialize this data?
➢ When data is “property” of the system, who is responsible?
➢ How is incorrect data modified ("delete data") on the blockchain?
➢ Does this have accounting or business rule implications?
Considerations related to market regulations by the authority
➢ Can the government promote a national / regional standard among the different logistics actors? Does my development meet those standards?
➢ How to prevent blockchain from becoming a barrier to entry to certain markets? How do we protect and promote the participation of SMEs in this type of developments?
➢ What incentives can the authority provide to favor this type of IT development?

Although originally the blockchain was created to store transaction history of bitcoin with the passage of time it has been seen great potential to be applied in other areas due to the properties it offers. The blockchain provides an immutable distributed database based on an increasing sequence of blocks (Ozdayi et al., 2020). These blocks, being public, make up an open system that enhances trust based to the transparency and solidity of the technique of construction of the blockchain. The system though it is open, it is also semi-anonymous: users are identified with public keys (pseudonyms),

not with their real identities. In this context, we can find a first relationship between blockchain and big data: the need to ensure a legal and fraud-free payment environment has led to the development of analysis tools based on big data techniques to process the large quantity of data represented in the blockchain (Hofmann et al., 2017). Therefore, the previous one is a possible use case of big data to improve the data insertion processes in the blockchain.

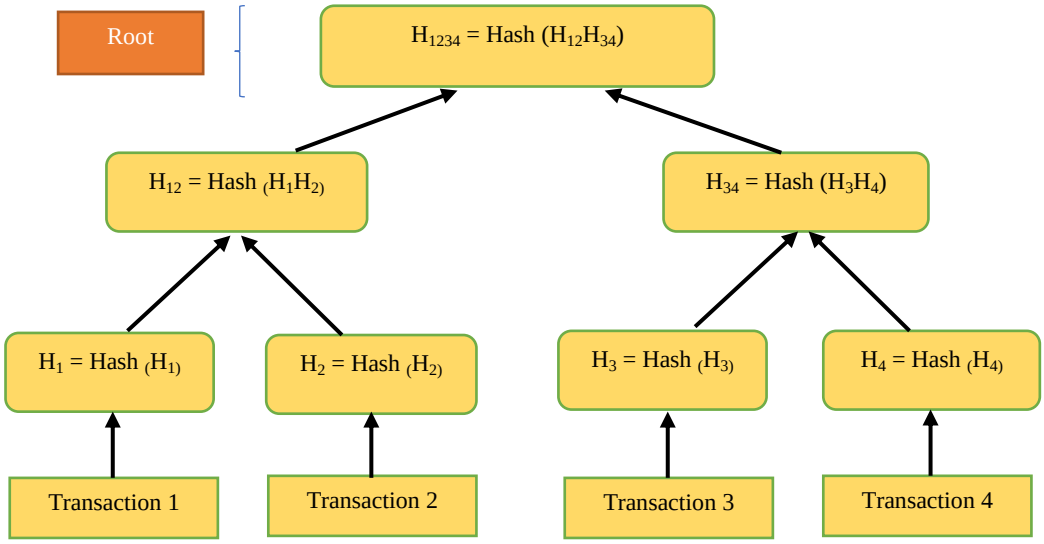


Fig.3: Hash Tree (Source: self-made)

However, we can also find cases of use in reverse where it is used blockchain technology to improve processes in the big data environment. In this sense, the blockchain can provide robustness, security, transparency, and scalability to big data systems which allows to face a wide range threat. This would include from information leaks through the blockchain, these threats can combat each other by individually tracing all actions made on the data, resulting in a constant audit. Finally, another use case for the blockchain it could occur in the field of Internet of things. An example is the distribution secure and reliable firmware to IoT devices using a peer-to-peer filesystem over blockchain (Hamledari et al., 2021). In this use case, the blockchain could use to store updates firmware in a decentralized way and safe (Smith and Christidis, 2016).

4.4. Big Data Security Through Blockchain

Various big data techniques are currently in use to analyze the blockchain and increase its levels of security. These techniques allow to deduce the identities of the nodes in the cryptocurrencies, detect fraud and map actual money flows (Farell, 2015). The inverse relationship uses blockchain technology to give security and verifiability to business environments of big data. It is about of data that usually come from various sources, in various formats, and are used in various processes by different departments of the company. The dangers of these systems are obvious: manipulation of data by part of internal workers, malicious suppliers, data corruption, storage failures, defective use, non-compliance with laws regarding personal data and a long and so on. In this context, the blockchain has a lot to do by providing transparency, verifiability, portability, and scalability. Through blockchain, each addition in the data, every change, every extraction for your use or each display could be made using a transparent and secure registry. The data could be accompanied by evidence of low-level integrity in the case of extraction of specific signatures that allow their traceability. These environments allow a degree of security and sufficient verifiability to comply with regulations quite restrictive while being intrinsically distributed, scalable, and interoperable. The legal requirements regarding the retention of data are no longer a problem because it is in the very nature of blockchain being able to deduce the state database at any point.

4.5. Generate Added Value in The Public Sector

Considering the initiatives that are being explored in the public sector in the region and depending on the attributes of the technology can be identified four broad categories where it could be thought that a technology such as blockchain could be useful for the public sector: (i) disintermediation of information, (ii) tokenization of assets, (iii) automation of processes and (iv) interoperability at the edge.

- *Disintermediation of information*

In many instances the generation of information in the public sector is based in a composite process chain by different people or entities. Through the technology, information can register safely with reliability and make the network a kind of digital data notary and transactions. Potentially including these processes in blockchain will allow to do without some of these intermediaries, increase the traceability of each stage of the process reliably and reduce costs both in time and resources.

- *Tokenization of assets*

The use of technology can allow express different assets as tokens so that they can be represented digitally and thus tell with a reliable record of changes property (or location, in the case production or distribution chains). This feature also allows the possibility of atomizing the property of a single asset among many owners.

- *Automation of processes*

An advantage of smart contract registration in a distributed ledger is the possibility of automating processes through establishment of rules that must be followed to a certain action (execution of the contract) automatically without trusted intermediaries. The automatic pay transfers when conditions are met predefined the collection of goods and services after they have been delivered or enforcing various regulations can be translated into rules included in smart contracts.

- *Interoperability at the edge*

One of the main challenges for the provision integrated government services is the need to connect the different systems of public entities and private safely and reliably. The use of blockchain for certification of citizen information can allow that the citizens themselves help different systems operate each other without the need for them to be integrate. This approach has also the advantage of allowing a greater traceability in access to information of citizens. It is important to note that these categories do not represent exclusive benefits of technology.

For better illustration, the potential added value of blockchain in such cases have been collected among the four categories which are listed in *Table* below. For each case, analyze the characteristics of the technology are briefly discussed and reviewed the assumptions that must be met in each case in order to implement a blockchain-based solution.

TABLE I: Analysis of potential added value of blockchain in some used cases

Type	Used cases	Example
Disintermediation of information	Increase the transparency of Processes	Subsidies for artists in Bahia Blanca (Argentina)
	Facilitate auditing information	Pilot for public purchases (Mexico)
	Ensure data integrity	Land ownership registry (Georgia)
Tokenization of assets	Intellectual property	Works of art
Automation of processes	Facilitate the automation of public processes	General Administration of Services (GSA) English United States)
Interoperability at the edge	Generate digital credentials	Educational certificates (Bahamas)
	Build a sovereign identity	Barrio 31 (Argentina)

4.6. Increase Transparency of The Processes

Blockchain has the potential to facilitate the registration and publication of data and processes public regardless of intermediaries who can manipulate or delay the procedure (Ducas and Wilner, 2017). The elements intrinsic to the technology that facilitate this objective are the distribution of information, the availability of data in multiple nodes that can be outside the public administration and the possibility of integrity verification information on the part of each of them. For example, through the implementation of smart contracts can be allocated subsidies in a way more transparent and efficient. The moment someone starts making transactions in the system, they create a history of all interactions and transactions that is available for all participants which generates a high level of transparency, traceability, and confidence

in the integrity of the network. Additionally, technology enables the notarization of information that can certify that certain information it has not been altered while a distributed private network can add restrictions on who can write or read transactions, retains the common access feature to set of transactions (Chowdhury et al., 2018). On the other hand, not only within public administration organizations with competence in the process or with audit roles but in organizations outside of the public administration. The solution will be more likely to increase the transparency and integrity of the information.

4.7. Blockchain For the Improvement of Public Procurement: The Case of Chile

In recent years Chile has focused on improving its processes and making them more transparent and reliable for which it has experimented with various technologies that allow to meet this goal. In this context it has implemented a pilot study based on the use of blockchain to certify purchase orders of a way to achieve traceability in the bidding or government procurement process (Pareti and Núñez, 2021). The pilot started with micro purchases which are acquisitions of low amounts that can be made through electronic payments and are managed through the Public Market portal. The content of the purchase orders of three State agencies (the Comptroller General of the Republic, the Directorate of Procurement and Public Procurement and the Internal Revenue Service) in the public network Ethereum; the data of the purchase order becomes a hash that later it is certified on the network and incorporated into the blockchain. In this way, providers and interested persons can corroborate that the information has not been altered or manipulated; For this, a friendly interface has been designed that allows verify the trust certificate linked to the order. Given the success of the pilot, Chile is currently evaluating scaling up the use of blockchain in the offers of the bidding processes (starting with a process simplified) and the automation of its evaluation.

4.8. Ensuring The Integrity of The Data

Blockchain allows to improve and protect the integrity of the data by making it very difficult the possibility of manipulating them without leaving a trace (Wei et al., 2020). Due to its intrinsic design the technology prevents further manipulation of data stored in blocks of the chain without being noticed by the rest of the participants. Consistency in data between all nodes generates security on its integrity which encourages the elimination of intermediaries. An important function of the government is to maintain reliable information on individuals, organizations, assets, and activities. The management of these records is usually complicated mainly because most of this information is found on paper. Government agencies tend to build their own silos data and information management protocols, which prevents other parties from government use them. Storing a land registry on a distributed network greatly improves safety by eliminating the risk of a single point of failure and making it more difficult its manipulation. This can also increase transparency and maintain the integrity of the records allowing certified agents (including potential auditors or non-profit organizations) monitor changes performed in near real-time registration and improve efficiency by reducing the time and money associated with property registration (Pisa and Juden, 2017).

4.9. Building a Digital Identity as a Pillar of Service Improvement: The Case of Illinois US

In 2001, the Illinois state government in the United States deployed the PKI to facilitate the certification of digital legal documents by agencies, boards, commissions, Illinois state universities, municipal government, and business partners, helping to determine the identity of different people, devices and services. Despite the incremental benefits that the public key infrastructure offers to the services of the government, it cannot be seen as a security solution for all data and management identity but is a piece of the puzzle. The data that make up the Citizens' identities are often stored in state databases in all agencies, increasing the chances of fraud, security breaches and errors (Morris et al., 2018). Illinois follows a proactive approach in identifying the potential of new technologies for the public sphere, that adapts its services to the needs of the people. A study conducted in 2017 by the Illinois Blockchain and Distributed task force Ledger Task Force has analyzed the potential of blockchain technology to improve economic and public processes. According to this study, technology can connect disparate entities within and between regional, municipal and regional entities states around citizens, companies and assets (Morris et al., 2018). The study suggests that there are multiple advantages to establishing an ecosystem of digital identity using blockchain technology, where the government plays a role fundamental as a manager of personal data and service provider. To make the management of digital identity more flexible, the state of Illinois decided implement a pilot of a decentralized public key infrastructure solution (DPKI) based on blockchain technology. The DPKI infrastructure leverages blocks as a store of values and is seen as a more flexible way of manage the public key infrastructure (Morris et al., 2018). The core elements of the technology-based digital identity solution pilot blockchain are as follows:

- Citizen attributes portfolio: decentralized identifiers in a blockchain and verifiable claims can be used to form the basis of the identity of a citizen.

- Identity attributes and attachments: each government agency can verify and add new cryptographically signed identity attributes to the wallet digital of a citizen. In this model, the wallet would be managed by the user or a service provider, while the integrity of the attributes it is maintained by the government entity.

- Asset and Property Records: Under this architecture, for assets and property can also be issued decentralized identifiers and attributes. A property or vehicle title can be represented as an attribute and be added to a citizen's wallet.

In this model the government would become the verifier rather than the custodian of people's identity. Encrypted and stored personal data through this architecture government add security since they are accessed through the private keys in the hands of citizens that serve to unlock data stored on citizen's personal device. People in turn can share selectively verify identity attributes to protect privacy (Datta, 2021).

5. CONCLUSION

Blockchain is such a new technology that there is no accepted definition yet for all. On the one hand, it is true that technology offers several attributes that could be of interest to the public administration. On the other, it is probably one of the most expensive ways to store information. In this sense, it is important to understand the limitations of technology, as well as the cases in which these benefits are violated or disappear. For instance, the lack of trust between the parties could disappear with a private network and / or allowed, which requires a level of trust between participants, since these networks can reduce the degree of difficulty of changing written information in the chain by having a smaller number of nodes and / or different consensus protocols that of public networks not permitted. Four spaces have been identified where it is considered that technology can support the public administration by improving or making the provision more effective of public services: Information disintermediation, Asset tokenization, Process automation, Interoperability at the edge.

REFERENCES

[1] AKBAR, N. A., MUNEER, A., ELHAKIM, N. & FATI, S. M. J. F. I. 2021. Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses. 13**,** 285.

[2] ALTARAWNEH, A., HERSCHBERG, T., MEDURY, S., KANDAH, F. & SKJELLUM, A. Buterin's scalability trilemma viewed through a state-change-based classification for common consensus algorithms. 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), 2020. IEEE, 0727-0736.

[3] ARSHAD, U., SHAH, M. A. & JAVAID, N. J. V. C. 2021. Futuristic blockchain based scalable and cost-effective 5G vehicular network architecture. 31**,** 100386.

[4] ASTE, T., TASCA, P. & DI MATTEO, T. J. C. 2017. Blockchain technologies: The foreseeable impact on society and industry. 50**,** 18-28.

[5] BANDARA, E., NG, W. K., DE ZOYSA, K., FERNANDO, N., THARAKA, S., MAURAKIRINATHAN, P. & JAYASURIYA, N. Mystiko—blockchain meets big data. 2018 IEEE international conference on big data (big data), 2018. IEEE, 3024-3032.

[6] CARSON, B., ROMANELLI, G., WALSH, P., ZHUMAEV, A. J. M. & COMPANY 2018. Blockchain beyond the hype: What is the strategic business value. 1.

[7] CHEN, Y., LOMBARDI, A., MA, F. & QUACH, W. Does Fiat-Shamir Require a Cryptographic Hash Function? Annual International Cryptology Conference, 2021. Springer, 334-363.

[8] CHIN, Z. H., YAP, T. T. V. & TAN, I. K. 2020. On the trade-offs of Proof-of-Work algorithms in blockchains. *Computational Science and Technology*. Springer.

[9] CHOWDHURY, M. J. M., COLMAN, A., KABIR, M. A., HAN, J. & SARDA, P. Blockchain as a notarization service for data sharing with personal data store. 2018 17th ieee international conference on trust, security and privacy in computing and communications/12th ieee international conference on big data science and engineering (TrustCom/BigDataSE), 2018. IEEE, 1330-1335.

[10] DATTA, A. 2021. Blockchain Enabled Digital Government and Public Sector Services: A Survey. *Blockchain and the Public Sector*. Springer.

[11] DUCAS, E. & WILNER, A. J. I. J. 2017. The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. 72**,** 538-562.

[12] FACCIA, A., MOSTEANU, N. R. J. J. O. I. S. & MANAGEMENT, O. 2019. TAX EVASION_INFORMATION SYSTEM AND BLOCKCHAIN. 13.

[13] FARELL, R. 2015. An analysis of the cryptocurrency industry.

[14] GHOSH, B. C., BHARTIA, T., ADDYA, S. K. & CHAKRABORTY, S. J. A. P. A. 2021. Leveraging Public-Private Blockchain Interoperability for Closed Consortium Interfacing.

[15] GRANT, G., HOGAN, R. J. J. O. C. A. & FINANCE 2015. Bitcoin: Risks and controls. 26**,** 29-35.

[16] HAMLEDARI, H., FISCHER, M. J. J. O. L. A., ENGINEERING, D. R. I. & CONSTRUCTION 2021. Role of blockchain-enabled smart contracts in automating construction progress payments. 13**,** 04520038.

[17] HASSAN, M. U., REHMANI, M. H., CHEN, J. J. J. O. P. & COMPUTING, D. 2020. Differential privacy in blockchain technology: A futuristic approach. 145**,** 50-74.

[18] HOFMANN, F., WURSTER, S., RON, E. & BÖHMECKE-SCHWAFERT, M. The immutability concept of blockchains and benefits of early standardization. 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), 2017. IEEE, 1-8.

[19] HOLOTESCU, C. J. T. T. S. C. & SOFTWARE FOR EDUCATIONBUCHAREST, A. 2018. Understanding blockchain technology and how to get involved. 19**,** 20.

[20] KEWELL, B., ADAMS, R. & PARRY, G. J. S. C. 2017. Blockchain for good? 26**,** 429-437.

[21] KHALIL, R. & GERVAIS, A. Revive: Rebalancing off-blockchain payment networks. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017. 439-453.

[22] LEMIEUX, V. L. Blockchain and distributed ledgers as trusted recordkeeping systems. Future Technologies Conference (FTC), 2017.

[23] LIU, Y., HE, D., OBAIDAT, M. S., KUMAR, N., KHAN, M. K., CHOO, K.-K. R. J. J. O. N. & APPLICATIONS, C. 2020. Blockchain-based identity management systems: A review. 166**,** 102731.

[24] LIU, Y., WANG, K., LIN, Y. & XU, W. J. I. T. O. I. I. 2019. $\mathsf {LightChain} $: a lightweight blockchain system for industrial internet of things. 15**,** 3571-3581.

[25] LÓPEZ-ZAMBRANO, M. C. R., CAMBEROS-CASTRO, M. & VILLARREAL-PERALTA, E. M. J. R. 2021. The determinants of trust and perceived risk on bitcoin users. 11**,** 22.

[26] LÓPEZ, M. A. J. B. I. D. D. 2018. Cómo desarrollar confianza en entornos complejos para generar valor de impacto social.

[27] MAETOUQ, A., DAUD, S., AHMAD, N., MAAROP, N., SJARIF, N. N. A., ABAS, H. J. I. J. O. A. C. S. & APPLICATIONS, B. 2018. Comparison of hash function algorithms against attacks: A review. 8.

[28] MORRIS, C., MIRKOVIC, J., O'ROURKE, J. & CAYHOLL, C. J. S. O. I. G. R. 2018. Illinois blockchain and distributed ledger task force final report to the general assembly.

[29] NAKAMOTO, S. J. T. C. M. L. 2008. Re: Bitcoin P2P e-cash paper.

[30] ORTEGA, D. R., OIKONOMOU, C. M., DING, H. J., REES-LEE, P., ALEXANDRIA & JENSEN, G. J. J. P. O. 2019. ETDB-Caltech: a blockchain-based distributed public database for electron tomography. 14**,** e0215531.

[31] OZDAYI, M. S., KANTARCIOGLU, M. & MALIN, B. J. B. M. G. 2020. Leveraging blockchain for immutable logging and querying across multiple sites. 13**,** 1-7.

[32] PARETI, S. & NÚÑEZ, I. J. R. I. D. S. E. T. D. I. 2021. Blockchain as an Information System in Chile: The Case of Open Energy Project-Chilean's Ministry of Energy. 554-568.

[33] PISA, M. & JUDEN, M. J. C. F. G. D. P. P. 2017. Blockchain and economic development: Hype vs. reality. 107**,** 150.

[34] PISA, M. J. I. T., GOVERNANCE, GLOBALIZATION 2018. Reassessing expectations for blockchain and development. 12**,** 80-88.

[35] SERALE, F., REDL, C. & MUENTE-KUNIGAMI, A. 2019. ADMINISTRACIÓN PÚBLICA.

[36] SHIRLEY, R. B., SMIDTS, C., LI, M. & GUPTA, A. J. A. O. N. E. 2015. Validating THERP: Assessing the scope of a full-scale validation of the Technique for Human Error Rate Prediction. 77**,** 194-211.

[37] SMITH, B. & CHRISTIDIS, K. IBM Blockchain: An enterprise deployment of a distributed consensus-based transaction log. Proc. Fourth International IBM Cloud Academy Conference, 2016.

[38] WANG, T., HUA, H., WEI, Z., CAO, J. J. I. J. O. E. P. & SYSTEMS, E. 2022. Challenges of blockchain in new generation energy systems and future outlooks. 135**,** 107499.

[39] WEI, P., WANG, D., ZHAO, Y., TYAGI, S. K. S. & KUMAR, N. J. F. G. C. S. 2020. Blockchain data-based cloud data integrity protection mechanism. 102**,** 902-911.

[40] WÜST, K. & GERVAIS, A. Do you need a blockchain? 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2018. IEEE, 45-54.

[41] ZAMBRANO, R., YOUNG, A. & VERHULST, S. J. G. O. 2018. Connecting refugees to aid through blockchain-enabled ID management: world food programme's building blocks.