ISSN No:-2456-2165

To Analyse How Blockchain Technology can be used to Securely Store Different Information Sources

Alastair Smith
MS in Artificial Intelligence, Northwestern University
New York, United States

Abstract:- Blockchain technology has emerged as one of the major disruptive innovations in last decade. Beginning from Bitcoin, the technology shows potential to be applicable in a wide range of fields and industries. This research work has been designed as an exploratory study based on quantitative design. The study seeks to examine the role of blockchain technology in enhancing security of storage of data from different sources. The study conducted a survey to gather empirical evidence and shows the level of security that blockchain can provide in storage and security of information from different sources

Keywords:- *Blockchain; Data Storage; Data Security; Information Security; Data Protection.*

I. INTRODUCTION

Blockchain as a technology has advantages in terms of data protection. However, given that the creation of the blockchain is closely linked to that of Bitcoin, and is also based on existing mechanisms, it is not so obvious to conclude how this technology is innovative in terms of Protection of personal data [34,16]. Indeed, it should be remembered that cryptography techniques have long been used in companies and for individuals (key exchange, secure connections, electronic signatures, certificates, etc.) [22,3]. These techniques were not created for cryptocurrency. However, we can attribute to Bitcoin the promotion of blockchain technology. We can consider that the blockchain is a new technology, however it remains based on already existing mechanisms (public and private keys, hashing, etc.) [43,39].

For example, blockchain technology allows the anonymity, or at least the pseudonymisation of the data that are registered on the register. Asymmetric encryption, and more precisely the public key of each user of Bitcoin, allows pseudonymisation during each of its transactions [47,10]. And if it is certainly this pseudonym that is registered in the public registry, it must be borne in mind that the encryption that allowed it occurred before the registration of the transaction in the blockchain [15,18].

Indeed, it is the intermediaries of exchange or storage of Bitcoin which, as soon as a user subscribes to his offer, gives him a public key, and therefore a pseudonym. Pseudonymisation and encryption are therefore security measures that are taken upstream by intermediaries, and not by blockchain technology itself [1,35]. In this respect, the only real interest of the blockchain in terms of data protection is the integrity and decentralisation of data. However, the blockchain is as reliable as the number of resources devoted to it. For example, the Bitcoin blockchain is extremely robust, while a private blockchain with only two servers would be extremely vulnerable [5,36].

Regarding the protection of personal data, the distinction between public and private blockchain takes indeed all its meaning. A public blockchain, made up of a public register accessible to all, allows us to remind anyone with a sufficient capacity of calculation to be able to validate a block by the resolution of a mathematical enigma [29,26,45]. Based on a principle of challenge, the resolution of this enigma, which consists of the calculation of a hash, allows the fastest miner to undermine the block, that is to say concretely to add it to the blockchain, provided that the solution of the riddle was previously validated by at least 50% of minors [4,14]. Therefore, the more "resources", that is to say, minors likely to make available their computing power to solve the mathematical challenge, the more people are likely to validate or not the calculation and so adding the block [24,28].

In summary, the more minors there are, the more the integrity of the data contained in the register is guaranteed. Indeed, unless more than 51% of the miners in the same blockchain, which is very unlikely if it is public, it is impossible to enter data (possibly personal) erroneous in his register [41,39,36]. In this way, the public blockchain complies with one of the essential principles of the processing of personal data, namely the accuracy of the data recorded there (article 5.1, d) of the RGPD). However, this is not the case of a private blockchain [30,59]. Since the approval process for blocks added to the register is limited to a very limited number of people, it is sufficient for the latter to agree to enter the information they would like on the register, without any third party cannot check the validity of this registration. Therefore, a private blockchain, to consider that it is actually a blockchain, does not present any real guarantee in terms of protection of personal data [44,20].

Beyond the integrity of data, the blockchain also aims, by its decentralized nature, to rebalance the balance of power between Internet users and trusted third parties such as GAFA. Indeed, as explained by Thibault Verbiest, Partner at DS Avocats, the blockchain is a way to "give back power" to the consumer, giving him the opportunity to decide what he shares [53,58]. More generally, he adds that "the blockchain has in it a promise hitherto not held by the Internet that of the autonomy of people in their trade, that of

passing the intermediaries, trusted third parties that are the GAFA. The latter have monopolized all the value of the data [44,27,27]. It is indeed one of the main objectives of the fervent supporters of the blockchain: to prove to the users that this technology could give rise to new economic models that would no longer be based on a massive collection of data [56,38].

In recent years, these characteristics have led to the explosive development of ever new applications and to an unmanageable number of actors. These range from various startups to technology companies, e.g. IBM, SAP and consortia formed at different levels, e.g. Hyperledger, Project [8,46]. But individuals, governments, NGOs, universities, research organisations and venture capitalists are also researching and developing the next "killer app" that will become the blockchain, which was the browser for the Internet [57,31]. This hype cannot hide the fact that there are currently many more visions, theories, and concepts than actually existing, working examples. Because the still young and at the same time complex technology brings multifaceted challenges in the field of ICT basics as well as in the field of applications and attack scenarios [18,52]. The technology currently lacks infrastructures for the respective deployment, adequate capacities, scalability and short reaction times, a coherent governance model and the corresponding legal framework [40,5].

This paper aims to explore the degree to which blockchain technology increases security of data and information in different sources. The main research question is, therefore, to gather empirical evidence and assess whether blockchain is perceived as a safer and securer technology as compared to previous technologies that are adopted by people and businesses for information security.

II. LITERATURE REVIEW

A. Block Chain Basics

The ability of the blockchain to irreversibly store transactions and to delegate the authority of a certifying authority to distributed consensus discovery is based on the combination of different techniques in the following simplified process [25,46,56]. First, the transaction, such as the transfer of a cryptocurrency or registration of a document from which sender generates and digitally signs. This transaction is sent to the network and distributed to the nodes involved. The nodes of the network check the validity of the transaction and insert it into the blockchain. In this process, the transactions are stored in blocks, which are hashed to a standardized format. First, all individual statements are coded into hash values and then summarized hierarchically [38,17,2]. This hierarchical compression of the individual statements is referred to as hash or Merkle tree, with which a block of statements can be clearly represented. The coding of the statements is safe against manipulation attempts, since changing a statement would already change the hash value of the block, and thus the hash tree would no longer be consistent [19,12,59].

Blocks are connected by chaining with the already existing history of the blocks, so that a chain (block chain) is created. In order to include a new block in the existing chain as a new element, Bitcoin has to solve a cryptographic puzzle: which string provides a similar hash value as the encoding of the new block to be recorded [26,45]. The similarity of both values is defined by the number of places to be matched in the hash value. The degree of difficulty of similarity can be varied. Since the hash function is not reversible, there is currently no constructive method for deriving the string to guess for the given hash value. There are thus a variety of strings to try, which requires appropriate computing capacity [38,41]. If a node, i. a participant of the blockchain network has found a corresponding string (Mining), the new block is added as a new element in the chain (Blockchain) and thus the last valid block. For any other node in the network, the correctness is easy to understand by just calculating a hash value [41,15].

Thus, a correct linking of blocks to a block chain can be realized. For persistence, these chains are now distributed over a plurality of nodes, i.e. all nodes have the same basic knowledge. If new blocks are created in individual nodes as a supplement to the existing block chain, a consensus can be reached throughout the network on the change [56,10,24]. The cryptographic puzzle serves for this consensus finding. Once a knot has solved a puzzle, the solution is checked and adopted by all. Blocks that are still waiting for consensus are organised in a superscript list, in which blocks of concurrent links are also included in order to re-integrate them into the one global blockchain [17,5,42].

Thus, a blockchain with its individual blocks can be managed in a network of nodes. The consensus finding determines which block is adopted as the next element in the global block chain [58,30,9]. Originally, the cryptographic puzzle was used to create new blocks (called mining) called proof of work. For different confidentiality and security requirements, the severity of the puzzle can be adjusted. A documentation system for distributing power consumption in a smart grid e.g. can work with simple puzzles and thus also consider the computing power of the control nodes [49,42,22].

Other types of consensus finding (see 2.4) may, for example, consider shares in a system. Consensus is reached when the majority of the shareholders reach the same result (proof of stake) [6,37]. Alternatively, nodes may be honoured as miners for consensus finding (umpires), or lottery-oriented selections may be made. In addition, there are other possibilities and also combinations of the mentioned types of consensus finding are possible [2,42]. Blockchains can thus be more easily described as distributed databases that are organised by the participants in the network. Compared to central approaches, blockchains are much less error-prone and in particular prevent Byzantine errors. However, these systems also bring with them various challenges [36,25,8]. The high level of redundancy of the data is currently being discussed

particularly critically. By keeping the same data in the network many times, a lot of storage space is needed [7,47,43]. Furthermore, the consensus mechanisms often limit the performance of the blockchain. Despite the fact that blockchain technology is still at the beginning of its development, it has undergone several changes in the recent past, most notably its use in a closed business context. There is a fundamental difference - also due to the different objectives - between public and non-public (private) blockchain [18,33,53].

Public Blockchain are public systems that anyone with a copy can access. This is not synonymous with automatic reading and writing on a blockchain. This is done via so-called full nodes, which process the approval-free requests of a user. Examples of public systems are e.g. Ethereum or the First Generation Blockchain behind Bitcoins [14,14,6]. Private or non-public blockchain describe systems that are only used for a consortium that has been closed. B. are available from organisations [50,21,30]. Closely related to the public character are the access rights. While on public blockchains basically every user has access rights and can write data, private blockchains have access rights are administered or limited to a consortium (Consortia Blockchain) [52,22,12]. In most cases, these are approval-based blockchain systems. Popular examples of private blockchains are the Hyperledger project with the open source solutions "fabric", "iroha", "sawtooth" and the project "MultiChain" [31,54].

➢ *Cryptography*

Cryptography is an essential cornerstone of blockchain technology. It is the foundation for block mining, the integrity of the blockchain itself, and the authenticity of all transactions and participants. Without reliable cryptographic primitives, e.g. Hash functions, blockchains in any form are therefore unthinkable [13,48]. The still young blockchain technology measured by the standards of cryptographic research poses some challenges to science. While most blockchains use proven cryptographic primitives for signing transactions and generating proof-of-works. However, no statement can be made about the future security of cryptographic primitives [45,6]. Over time, more and more efficient attacks on cryptographic algorithms are being developed, the computing power available to an attacker is steadily increasing, and previously unrealistic attack scenarios are suddenly gaining relevance, such as Logjam1 and SHAttered [39,48,18]. In addition, the security of cryptographic systems is far from dependent only on the selection of suitable algorithms. Rather, much of the attack is aimed at the way it is used and the concrete implementation. There are plenty of examples of this, from trivial implementation errors such as Heartbleed 3 [37,8], which may remain unrecognised over years, to more sophisticated attacks that use deviations in system behavior as so-called "oracles" to obtain information about cryptographic keys, to page channels Attacks, which, for example, evaluate the timing behavior of implementations [10,9].

Much of today's blockchain technology neglects these attack possibilities and relies almost exclusively on cryptographic primitives, which are considered secure at the moment. However, since Blockchain applications are designed for extremely long lifetimes - think of a notary function, for example - it is essential that these systems be able to handle new attacks and possibly broken cryptographic primitives in the future [10,15,25]. For secure communication protocols, one typically uses a selection of several cryptographic algorithms, which are available for each connection setup, so that algorithms that have become unsafe can be easily exchanged. For blockchains such a "crypto agility" does not exist so far [23,34]. Rather, recent research has shown that, for example, the bitcoin blockchain is not resistant to possible attacks on some cryptographic components: Should it be possible in the future to falsify ECDSA1 signatures, Bitcoins could be stolen. If it becomes possible to invert the SHA2562 hash function, an attacker could be injured. efficiently calculate the proof of work and take control of the blockchain [9,40,19].

Countermeasures against such attacks - should they ever become possible - are extremely complex. Although the protocol may introduce a new hash function with loss of backward compatibility, design-wise old blocks with block hashes must be preserved from the old, insecure hash function [9,1]. As a result, the new clients would now have to solve two proof-of-works instead of just one. So, science faces several challenges here.

- Firstly, the development of cryptographic primitives which are also effective against future attacks, e.g. by quantum computer, are resistant [33,12].
- Second, the design of blockchain protocols that support crypto-agility and still provide security guarantees for transactions in the event of effective cryptographic attacks on individual primitives [25,29].
- Thirdly, the development of procedures that demonstrably correctly implement critical operations in blockchain protocols to avoid fatal implementation errors such as those most recently encountered in OpenSSL [54,27].

➢ *Consistency and Scaling of Distributed Systems*

Distributed systems are all those computer systems that use multiple computers to accomplish a common task. A simple example of this is a web browser that uses the Internet to retrieve a web page from a server. More complex systems are e.g. the transaction systems of a stock exchange or flight booking systems: here, for load distribution reasons, several computers are necessary [27,32,52]. At the same time, however, it must be ensured that a transfer similar to a database transaction is executed exactly once. It must not matter whether the systems work correctly at any time: A software error or hardware defect must not change a transfer. This problem is known in computer science under the keyword "Byzantine Generals" [7,51]: Imagine a city surrounded by several armies led by one general. The armies are only able to take the city with a joint attack. To

coordinate the attack, the generals send messengers with messages to the other armies [5,44,23].

In this thought experiment it is easy to reconstruct different fault conditions from distributed systems: what happens when a messenger is intercepted on the way? What if a messenger maliciously changes the message? Or by chance? [3,37,4] A "byzantine fault tolerant" system is one that remains stable despite such errors, e.g. guarantees the transaction properties. The blockchain is an example of such a system [50,24]. However, the highly distributed P2P nature of the blockchain suffers from this robustness with time delays: e.g. in the Bitcoin block chain, on average, 10 minutes to find a block - and only after six blocks can you be really sure that your own transaction has been correctly recorded in the blockchain. To compensate for this disadvantage, one could also centralize this aspect of the blockchain again [9,16,11].

To do this, the P2P network would be replaced by a smaller number of service servers that are in contact with each other, like the generals in the above analogy. These servers communicate with each other and provide a sufficiently redundant execution of the blockchain. In order to protect against false news, news losses, etc. procedures such as Raft [48,8,28] can be used. In addition, this partial centralisation simplifies the import of updates and bug fixes enormously. Blockchain technology offers many potentials for business use. However, aspects such as compliance or timely bug fixes are difficult to integrate into the highly distributed structure of the current blockchain systems [42,38,13]. One task for the future will be to adapt these systems so that the requirements of the company's operations can be met [2,18,16].

In terms of distributed data storage, the blockchain concept relies on the storage and replication of all managed transactions, i. of the entire database in all participating nodes of the P2P network. With the lifetime of a blockchain, the replicated dataset continuously grows, leading to a critical assessment of the scalability of the block [29,22]. In order to avoid the rapid growth of the blockchain, therefore, no large data objects are stored in the blockchain, but primarily only the essential transaction information and, if necessary, references to the associated data objects. These are stored in an external database if the data object is to be available directly via the transaction [30,36,39]. Alternatively, instead of a reference, a fingerprint of the data object may also be stored in the form of a hash value. In this alternative, the hash value can be used simultaneously for retrieval from an external database and for verifying integrity, in which the fingerprint of the reconstructed object is compared with the fingerprint stored in the blockchain [32,32].

However, this method can also be used when using a blockchain for the management of high-frequency transactions, as described e.g. Sensing data in the Internet of Things prevents the blockchain from growing continuously [1,34,7], increasing the computational and memory capacity requirements of the nodes in the distributed system. For this reason, further research is needed to avoid these technical requirements leading to unwanted centralisation [21,47]. One approach is to consolidate the blockchain to the "Unspent Transaction Output" (UTXO), i. a kind of balancing whereby the size of the blockchain can be reduced since transactions that no longer contribute to the determination of a user's credit are deleted [49,56]. Another approach is to shard the blockchain, with the nodes managing only parts of the blockchain, while still maintaining the integrity of the entire chain. Despite these initial approaches, scaling challenges in terms of size and transaction throughput provide interesting research potential for the future [15,51,46].

➢ *P2P Networks*

In peer-to-peer (P2P) networks, only peer computer nodes exist, i. Unlike client-server architectures, all participants in the network can perform the same functions [11,20,37]. As a result, P2P networks are very robust to failure because all computer nodes can perform all functions necessary for the operation of the network [12,19]. Furthermore, aspects of load sharing and self-organisation are quite easily solvable due to the structure of a P2P network. As a result, large P2P networks reach e.g. based on the BitTorrent protocol and the high number of connected computer nodes a very high throughput [26,55,40]. At the same time, however, this architecture also leads to greater complexity. The basic challenges of P2P networks are [51,25]:

- Intentional Manipulation: Nodes in the P2P network do not necessarily all have to pursue the same goal and may attempt to viciously affect the functioning of the network in their favour [4,45,29]. If the network is e.g. used for payment processing, a node could try to simulate a payment that actually did not exist. Such misinformation must be detected and rejected by all other nodes [28,7,41].
- Defective information e.g. Software errors or communication problems, as well as deliberate manipulation, can lead to network problems [53,49,1]. These must - just like manipulation attempts - be detected and processed accordingly [52,23].
- For many applications, it must also be ensured that a transaction in the P2P network is performed exactly once and completely - that is, has the properties of a database transaction [28,13].

The blockchain solves these problems by ensuring consensus. In contrast to highly complex consensus algorithms such as e.g. [43,9,38], through the construction of the data structure, assures the blockchain the integrity of the information within the blockchain. This design solves all the challenges described above. A disadvantage of a P2P network, however, is that the program logic is stored in all participating computer nodes [40,31,48]. If e.g. found an error so all computer nodes must import an update. Particularly with Ethereum it came through a protocol error to the erroneous posting of account balances, which could be remedied only by a Hard Fork and a not backwards-compatible software version [36,53].

➢ *Consensus Building and Validation*

The technique of consensus building is another cornerstone of Blockchain. The methods used here are based on concepts that have already been studied for a long time in the context of distributed networks and distributed systems [11,1,34]. The best-known method currently used by a blockchain implementation is the proof-of-work of the Bitcoin blockchain. The actual proof-of-work concept was already proposed in 1993 to curb junk emails [12,41,5]. It is based on an asymmetric approach in which a service user, i. the e-mail sender must perform work performed by a service provider, i. the email network provider can be easily checked. In the context of the blockchain, users are the miners who spend a lot of time on the proof-work, and the vendors are all nodes that easily check that the successful miner has correctly calculated the proof-of-work [24,28,58]. In the Bitcoin blockchain, the proof-of-work algorithm is based on the method presented by Adam Back as Hashcash [27,50]. The goal of the algorithm is to find a number (nonce = number used only once) that, in combination with the new block to be appended to the already existing blockchain, gives a hash value consisting of a certain number of leading zeros consists. If several miners simultaneously find such a value and attach it to the blockchain, this results in a branching of the blockchain as this new block is distributed to all nodes of the P2P network [20,33]. Find e.g. 3 Nodes almost at the same time a matching nonce, then attaching the new blocks would divide the existing block chain into 3 branches. To re-consolidate this split, the majority vote is to select the branch that represents the longest chain, represents most transactions or most of the work. The other two blocks expire, and the transactions contained therein, which are not contained in the attached block, are again included in the pool of transactions yet to be validated [17,4].

This proof-of-work method is CPU-based, i. the computational speed of nodes has a significant impact on who resolves the puzzle and finds a matching nonce value. As the miners are rewarded with new Bitcoin for finding the nonce, a competition is created, which leads them to invest in more and more computing power [39,2]. This would reduce the time needed to find a valid nonce, but this contradicts a Bitcoin network rule that a new block should only be generated approximately every 10 minutes [31,59,32]. This is due to the fact that the reward of the successful miners with so-called newly created Bitcoins takes place. If the intervals at which new blocks were generated would be shortened, the money supply would increase too quickly. For this reason, the difficulty of the puzzle is always increased when the time is shortened by newly added computing capacity [45,3,14]. This means for the miners who operate the compute nodes an increased effort with less chance of success. Since the effort in addition to the investment in computing power Consumed energy, this approach is not useful for all blockchain applications [14,43]. This is especially true for private blockchain solutions where such competition is not required. For this reason, alternative proof-of-work methods have been developed that are either memory-based or network-based [35,26]. In memory-based approaches, the puzzle cannot be solved by computing power but by a corresponding number of memory accesses. In the network-based approach, only by communicating with other network nodes, e.g. to collect information from there that is needed to solve the puzzle [57,4,54].

An alternative method, which is particularly relevant to private blockchains, is the proof-of-stake method at the node, which can validate a new block, selected according to your shares in the cryptocurrency or via a random procedure [6,29,17]. A combination of proof-of-work with proof-of-stake procedures is also possible. The selection of the most appropriate method depends on the specific case of application and the use of the Blockchain solution, as private or public or free from approval or approval. Another important aspect is the scalability in terms of the number of transactions, especially in applications of the Internet of Things [58,17].

➢ *Smart Contracts*

Blockchain not only enables the decentralisation of transaction management, but also the automation of processes, regulations and organisational principles. The transactions can be supplemented by rules for preserving consistency and then become so-called smart contracts. They specify what to check in a transaction and what follow-up activities are to be initiated [3,7]. Frequently mentioned examples of smart contracts are e.g. electronic door locks that automatically check whether the user has paid the usage fee and still in possession of the necessary legitimacy such a driving license [54,43,26]. Thanks to smart contracts and the associated automation, many processes can be radically improved in the context of re-engineering and, in some cases, can also be facilitated by certified inspection bodies if the consistency of the information is ensured by a smart contract and audit-proof storage. Classic principles of the Re-Engineering Manifesto of Hammer and Champy such as the "capture only once" can thus be implemented in a natural way with Blockchain as an enabler [12,54,49]. Once information has been confirmed, it is documented in an audit-proof manner and can be integrated in a variety of contexts. Thus, from a technological point of view, the blockchain is a natural tool for process optimisation. If, for example, it is only possible to import a video in a community platform if the corresponding audio rights are available, the entire monitoring and monitoring processes can be omitted. However, this consistency is easy to maintain through smart contracts [47,56,51].

The blockchain technology thus has not only diverse effects on the processes, but also on structures of governance, which can significantly change the distribution of tasks between process participants [32,2,20]. The new distribution of responsibilities and changes in governance also raises the question of new business models for the new value chain after re-engineering the process. Because of the disruptive potential of the blockchains, classical forms of process optimisation seem rather inappropriate [8,6,3]. A revival of classical reengineering methods seems possible as they have analysed processes from a strategic and

customer value perspective. Also, re-engineering takes into account stakeholder role changes [59,11,33].

- *Trustworthiness and Security of Smart Contracts*

Smart Contracts are small programs that run as part of individual transactions in the blockchain during validation of transactions by the peers. Only smart contracts make a blockchain more than just a distributed secure store and enable automated and trusted modification of information in the blockchain. For example, Bitcoin Smart Contracts can be used to manage various types of transactions, such as to realize escrow [35,24,47]. While Smart Contracts in Bitcoin can only consist of a few operations and cannot implement loops, the Ethereum Blockchain offers a "quasi-turing full" language, the execution of which costs "gas" in a dedicated virtual machine. This ensures that a smart contract terminates, even though the language itself is Turing-complete and therefore allows infinite loops [20,58,21]. The Hyperledger blockchain goes further and allows you to run almost any program. These are called chaincodes, which can be written in various high-level languages such as Java or Go and run by trusted "validating peers" [51,53,57]. During execution, the chain code has access to the information stored in the blockchain and can read it or store further information. Furthermore, chaincode is only isolated from the rest of the environment by Docker containers when running. the execution does not take place in a virtual machine, but directly on the processor of the peer [55,57].

The correctness of smart contracts is of the utmost importance, because unlike, for example, desktop or web applications, continuous updates of smart contracts are not readily possible [19,11]. This means that once inserted SmartContract code cannot be revised without questioning the integrity of the data stored in the blockchain. In fact, in the past, attacks on smart contracts have been reported repeatedly, some of which have been made possible by hard-to-detect programming errors in the smart contract (unchecked-send, reentracy, solarstorm) [1,52,15]. In addition, however, the execution environments for smart contracts are also partially uncertain. For example, Hyperledger cannot currently guarantee that Chaincode will terminate. At the same time, because the executing environment can use the validating peer's unlimited CPU resources, smart contracts can easily be used as a denial-of-service attack on the peer [16,49]. Furthermore, chaincode is not limited to communication with the blockchain, but can also call external services, and thus also harmful smart contracts are conceivable, e.g. Send spam or act as bots within the blockchain [5,23,35].

When using smart contracts, two things have to be ensured: on the one hand, the smart contract itself must be correct and secure against attacks such as reentrancy. In practice, this is not trivial to ensure, as the DAO attack has shown. On the other hand, it must be ensured that no malicious smart contracts enter the blockchain [11,44]. This is especially true for blockchains with powerful SmartContract languages such as Hyperledger and Ethereum. While Ethereum is taking the first steps in the right direction with the support of formal verification of smart contracts through the why3 framework, such techniques are still too laborious for most developers and require too much background knowledge to be useful [7,19,50]. In general, there is still a high need for R & D in the area of secure smart contracts - both in using formally verifiable languages, as well as in assisting developers and validating code prior to inclusion in the blockchain [34,16].

III. METHODOLOGY

This study is designed as an exploratory research, because the aim is to explore the impact of blockchain technology on security of data and information. This is a subject that has been little studied at present since it is something very novel and of little interest on the part of the experts and scholars of the area. One of the most important issues to address, from this exploratory research, are the direct and indirect consequences that will bring the use of Blockchain by people and companies in society. We know that it is a flexible exchange rate currency and that it is very volatile, which attracts all kinds of investors and people interested in the subject. Another important thing to analyse is the use, by users, that is currently giving this new virtual currency peer to peer, as well as the future perspective that may have it. The specific objective of this research is to discover the viability that this new technology may have in the society and economy. In addition, we will seek to identify what are the different difficulties that arise for the adoption of Blockchain and understand the reasons for acquisition and use of it.

This study was based on quantitative design using surveys as the data collection method and statistical analyses as data analysis techniques. The instrument to be carried out for the research methodology of this work is the realisation of surveys aimed at all types of people (professionals or not), with the aim of seeing the general interest of people on the subject and their level of knowledge about it.

The survey was distributed to 500 individuals through email and Facebook. In response only 306 responded back, among which 33 were incomplete and thus discarded. Therefore, the results below are based on 273 participants.

IV. RESULTS

The objective of these surveys was to analyse the general knowledge on the part of society about this new technology and the acceptance of it. In principle we can highlight that we managed to complete 273 surveys, where it was published on the Internet, both in social networks (Facebook) and via email or email to each of the stakeholders.

The demographic characteristics of the participants are as followed. In principle we observed that of the total of people surveyed, 59% were men (162 men) and 41% were women (111 women). On the other hand, we also see that in 86% of the people surveyed are between 19 and 30 years old (235 people), 10% would be between 31 and 50 years

old, and the rest of the participants with less participation are both people under 18 years and those over 50. With this we can reach the simple observation that this new technology called Blockchain is of greater interest in youth, that is, people from 19 to 30 years, and this is fairly reasonable since the same It was created in 2009 and, therefore, is very new for society being difficult to understand by children under 18 and over 50. Also, this assumption can be observed by the level of study of the participants, since 79% of the total of them are currently doing university studies, which agrees with the majority age range that these aforementioned participants already possess (between 19 and 30 years old).

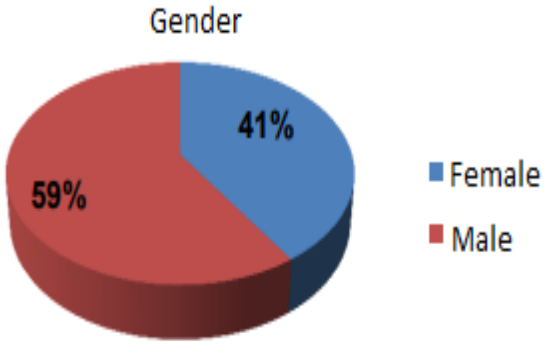

Fig 1

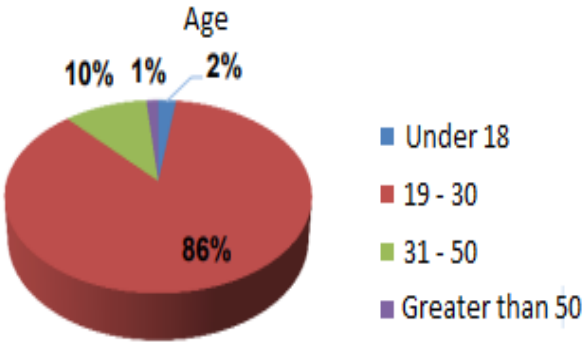

Fig 2

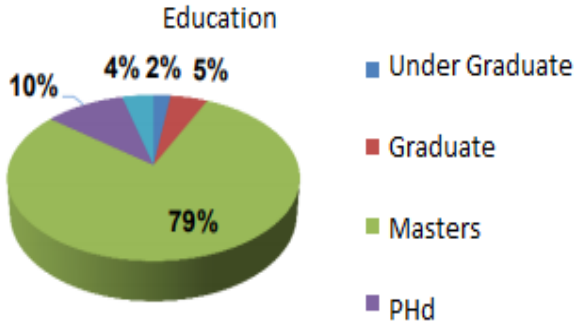

Fig 3

The survey asked participants to indicate level of knowledge about blockchain. Of all the people surveyed, 73% answered that they are aware of the existence of Blockchain, while 27% of people do not know it.

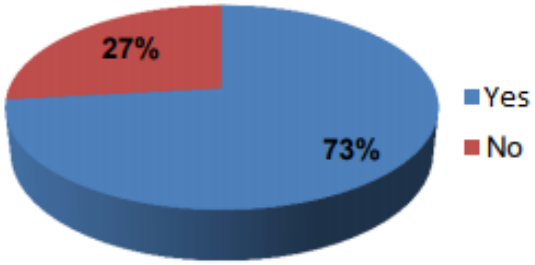

Fig 4

The researcher also asked survey participants to indicate yes if know what blockchain is about. Of the 73% of people who know about Blockchain, 63% replied that they also know what Blockchain is about. On the other hand, 37% of those who do not know are part of the 10% who claim to know the existence and 27% who know absolutely nothing about it.

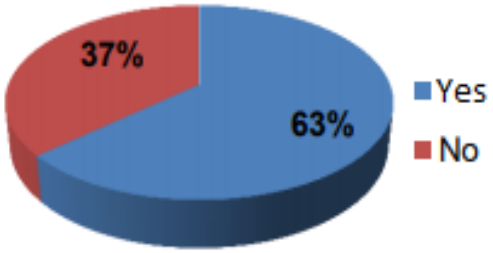

Fig 5

The questionnaire also asked to indicate which media provides knowledge and news about blockchain. Most of the participants who already knew this technology, or read it somewhere or heard about it, did it through the internet, with 37% of them, following it with 20% word of mouth, which is the equivalent of hearing about it or having someone tell it. Then, it follows them with 12% through the universities and with 11% through the traditional means of communication, such as television, magazines and newsletters. Already with a lesser proportion are talks and conferences (7%) and other media that people knew about it. These results are logical because since Blockchain is a technology based on the Internet and virtual networks, it would be logical to assume that through these the new disruptive technology is made known.

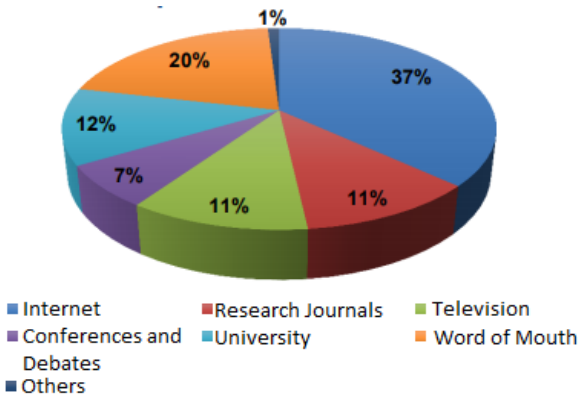

Fig 6

ISSN No:-2456-2165

Furthermore, it was also asked to indicate the following options agree with blockchain. We also consulted the participants about what they think Blockchain is, after they have read the definition we presented at the beginning of the survey about what Blockchain is. We found that 29% of people believe that Blockchain is a means of electronic payment, followed by 25% of those who think it is a new alternative currency. These two options are the ones with the highest percentage, followed by those who believe that it is a means to invest or to make transfers abroad, with 12% respectively, and others who also thought, with 10% of relevance, that it is a means to save or that Blockchain is simply a technology.

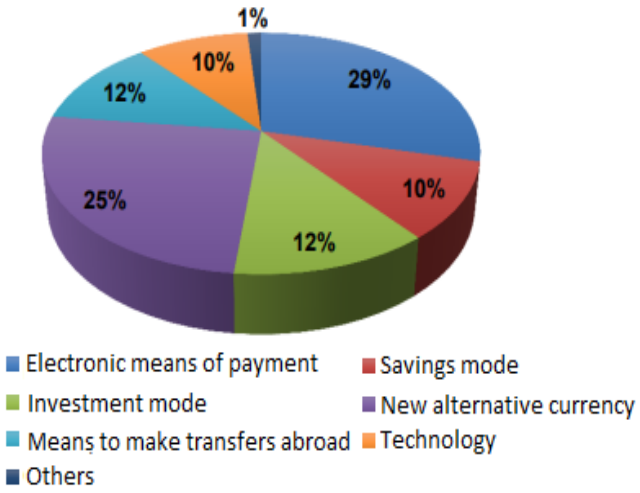

Fig 7

The survey also asked to indicate the knowledge that blockchain does not have an entity that controls it. In addition, other questions were asked, at the end of this investigation, on issues of regulation and control of Blockchain. On the one hand, we asked people if they had a notion that this technology does not have an owner or a government or private entity that controls it, and 55% answered affirmatively that they knew what was said and 45% did not know or did not know I was internalized in it.

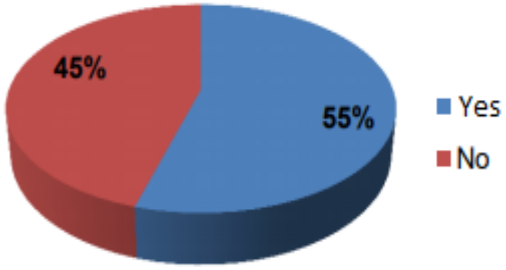

Fig 8

Then, we analyse through another question if this deregulation or independence of the Blockchain affects the reliability in the use of it by its users or acquaintances in the subject, responding 42% if it affects this, with 24% that does not affect them and with 34% that is indifferent to them or that they may not know at this time.

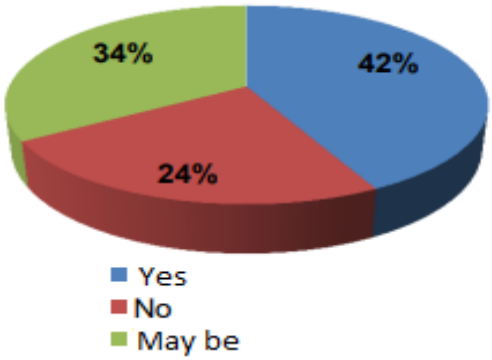

Fig 9

Finally, within this section, we allow the participants to give an opinion about whether Blockchain should be regularized or not by any entity, responding 46% that it should not be, 36% answered that it should be controlled and a 18% of people are indifferent that this technology is regularized or not.

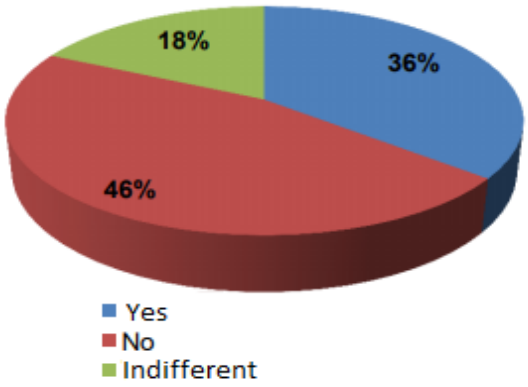

Fig 10

Another point that we analyse is the level of distrust that people in society have towards the use of Blockchain. We found that 55% of the respondents do not trust the use of this technology, while 45% do not generate this distrust.

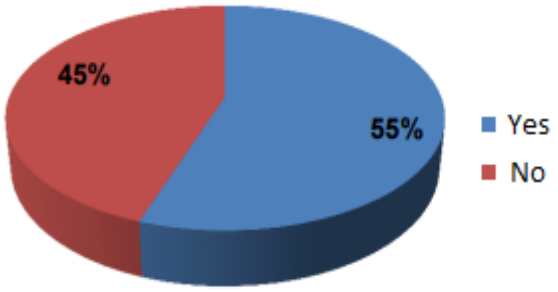

Fig 11

On the other hand, we made a survey of why the use of Blockchain generates some kind of mistrust, and we find that, on the one hand, 22% are afraid of not returning the money if something happens to Blockchain, the 20 % have insecurity to the theft of money from their account, 16% generate insecurity due to fear of theft of personal data online and illegal transactions anonymously, 14% generate distrust for fear of money laundering by of users in

ISSN No:-2456-2165

Blockchain, 10% would not use it for reasons of tax evasion or the promulgation of the same and, finally, 2% for other reasons that each participant added to the question. It should be noted that people had the possibility to choose between several options because they are distrustful of the use or possession of Blockchain.

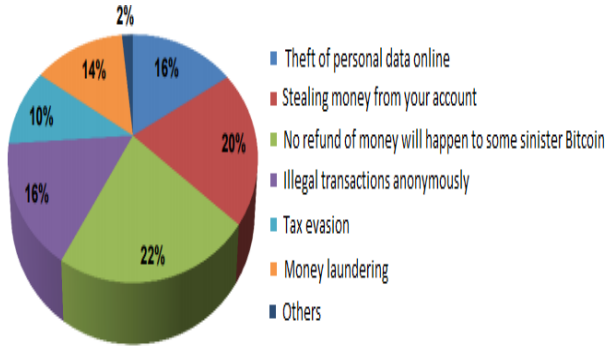

Fig 12

We also had the intention to find out if the company had a notion of the Blockchain price value of today. We can see that, on the one hand, 38% of people believe that the value of Blockchain is less than US $ 100 (dollars) and 33% believe that the value is between 101 US $ and 500 US $, while 16% believe that the value is between US $ 500 and US $ 1000 and 13% think that Blockchain value is greater than 1000.

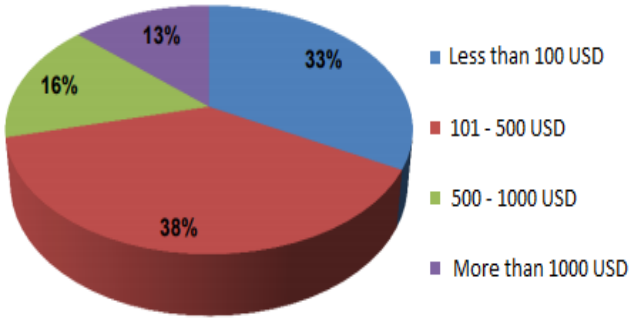

Fig 13

Another of the studies we did was to investigate if people had knowledge of a local, business or company that accepts Blockchain as a means of payment. We observe that 79% of respondents do not know any place that accepts them, while only 21% know places that accept blockchains as a means of payment. Of those who knew, they mentioned the following companies or businesses: Subway, Nick-Hard, The Historic, ROT Bar, Fukuro Noodle Bar, Dell, The pirate bay, avalancha.com, Antidomingo (restaurant), 3d lab Bar, Amazon, PayPal , Newegg, Tigerdirect, Blockchain store, Trifl, Overstock, Greenpeace NY, Gyft, Bitpagos, Porto Pirata Restó, royalqueenseeds.com, Ripio, Third South, Mustaine Taxi, also mentioned tourism agencies, such as Destinia, as well as hotels, restaurants , various bars, video game sites, among others.

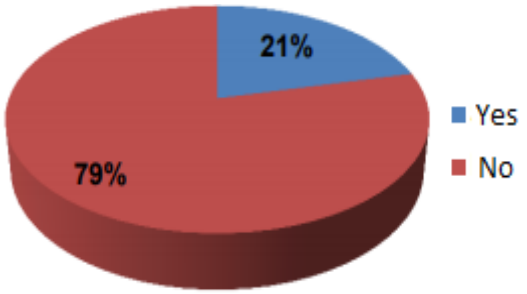

Fig 14

In another question, we mentioned to respondents whether they would be willing to use Blockchain to buy and / or sell goods and / or services, that is, to use it as a means of payment for different purposes. We discovered that 48% of the people, that is, almost half of the respondents, are not sure of using it. This is because this is a recent technology that brings many confusions to society, so much so that Blockchain catches their attention but still, as new as it is, they are not sure whether to adopt it or not. On the other hand, 29% of the respondents answered that if they would use it, and 23%, instead, they would not use it as a means to buy or sell services or diverse goods.

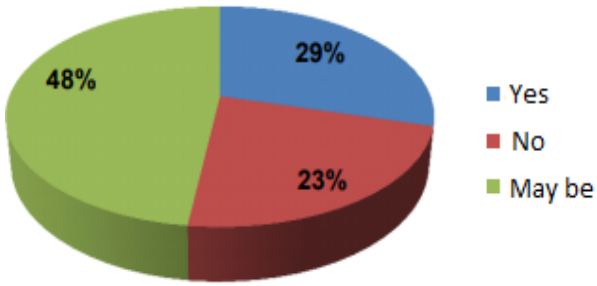

Fig 15

Another point to analyse in our survey is about the impact that Blockchain could have on society, like other technologies that have appeared over time. 42% of people agree that Blockchain will have a significant impact on society, while 30% of respondents fully agree with the aforementioned statement. On the other hand, 17% of the respondents are indifferent or irrelevant the fact that Blockchain can generate an impact at a social level, while 12% disagree with it (9% of people) or that absolutely do not produce anything (2%).

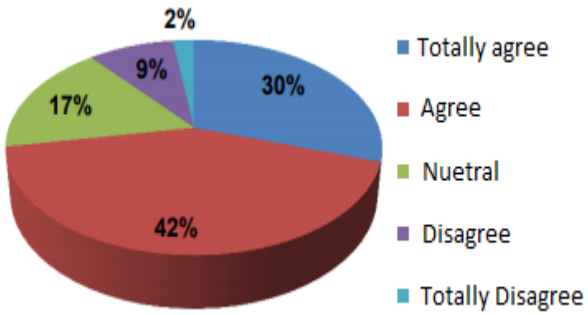

Fig 16

ISSN No:-2456-2165

As one of the objectives of our research is to find out if the company would adopt Blockchain as a digital currency, we ask a question that solves this question. Given this situation, we find that 56% of people, that is, more than half of respondents, might be willing to adopt Blockchain, but are not completely sure of it. This we believe is due to the same reasons already discussed above, that is, that Blockchain is a novel technology, of which people did not develop a complete opinion on it to be safe when adopting it or not. We also saw that 22% of the respondents are totally sure of the adoption of blockchains, while 14% might not adopt it and 8% are definitely sure of not wanting to adopt them.

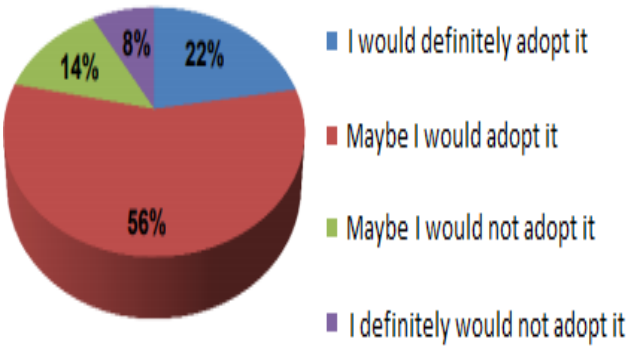

Fig 17

Of the people who might adopt or who are totally sure of adopting Blockchain, 33% would use it as a means of payment and 20% would use it to make an investment, either in the short or long term. Others, with 17%, would use it as a means to make transfers, both locally and abroad, and would also be a means to save or preserve the value of holding their money, with 16%. Finally, we saw that 14% would use it for the purpose of traveling abroad and making their payments or purchases outside the country with blockchains, and the rest (1%) would use it for other personal reasons of each user.

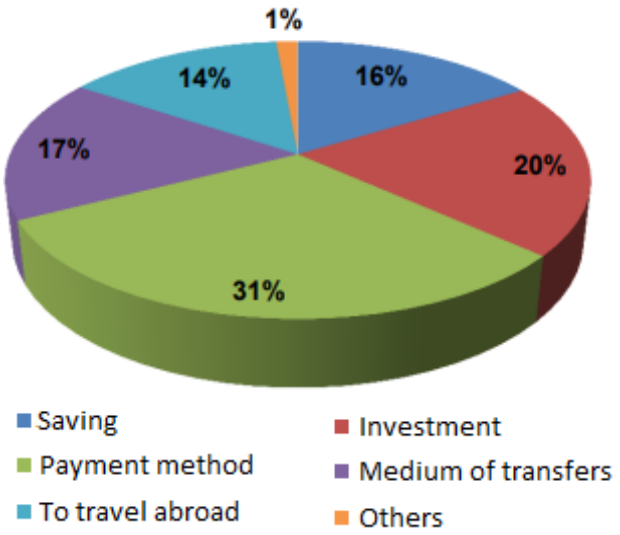

Fig 18

V. CONCLUSIONS

This position paper examines blockchain technology from all the relevant technical aspects and the associated with security of information and data from different sources. It shows that the still young technology still has significant potential to contribute towards security of personal data and information. Various elements such as cryptography, consistency and scaling, P2P network, consensus and validity, smart contracts, and trustworthiness increases the security of data and information. A major challenge will be the modularisation of individual blockchain concepts and their combination and integration for an application-specific blockchain solution. Investigating fields of application and industries that are most likely to benefit from the new technology shows that different properties of the blockchain are relevant to an application field. While for the Internet of Things, the automation potential associated with smart contracts is key, it is the irreversibility of managed transactions for supply chain or proof of origin applications. Central to this, however, is the fact that the blockchain has great relevance for many different areas of application outside the financial sector and, above all, independent of cryptocurrencies. The breadth of blockchain technologies, as well as their applications, requires a multidisciplinary approach to both basic technology development, application development, economics calculation, and the design of new governance models.

REFERENCES

[1]. Belle I. The architecture, engineering and construction industry and blockchain technology. Digital Culture. 2017:279-84.
[2]. MICHAEL J, COHN A, BUTCHER JR. BlockChain technology. The Journal. 2018 Feb.
[3]. Buchanan B, Naqvi N. Building the Future of EU: Moving forward with International Collaboration on Blockchain. The JBBA. 2018 Apr 27;1(1):3579.
[4]. Pilkington M. 11 Blockchain technology: principles and applications. Research handbook on digital transformations. 2016 Sep 30:225.
[5]. O'Leary K, O'Reilly P, Feller J, Gleasure R, Li S, Cristoforo J. Exploring the Application of Blockchain Technology to Combat the Effects of Social Loafing in Cross Functional Group Projects. InProceedings of the 13th International Symposium on Open Collaboration 2017 Aug 23 (p. 13). ACM.
[6]. Wright A, De Filippi P. Decentralized blockchain technology and the rise of lex cryptographia.
[7]. Till BM, Peters AW, Afshar S, Meara JG. From blockchain technology to global health equity: can cryptocurrencies finance universal health coverage?. BMJ global health. 2017 Dec 1;2(4):e000570.
[8]. Sikorski JJ, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Applied Energy. 2017 Jun 1;195:234-46.
[9]. Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology.

InService Systems and Service Management (ICSSSM), 2016 13th International Conference on 2016 Jun 24 (pp. 1-6). IEEE.
[10]. Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. InService Systems and Service Management (ICSSSM), 2016 13th International Conference on 2016 Jun 24 (pp. 1-6). IEEE.
[11]. Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. InService Systems and Service Management (ICSSSM), 2016 13th International Conference on 2016 Jun 24 (pp. 1-6). IEEE.
[12]. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. InBig Data (BigData Congress), 2017 IEEE International Congress on 2017 Jun 25 (pp. 557-564). IEEE.
[13]. Mattingly T, High DR, Wilkinson B, McHale B, Cantrell R, John JO, Jurich J, inventors; Walmart Apollo LLC, assignee. Managing smart appliances using blockchain technology. United States patent application US 15/881,705. 2018 Aug 2.
[14]. Chanson M, Bogner A, Bilgeri D, Wortmann F. Privacy preserving data certification in the Internet of Things: Leveraging blockchain technology to secure sensor data. InJournal of the Association for Information Systems (JAIS) Theory Development Workshop Associated with Thirty-eighth International Conference on Information Systems (ICIS 2017), December 10-13, 2017, Seoul, South Korea 2017.
[15]. Ølnes S, Ubacht J, Janssen M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing.
[16]. Lemieux VL. Trusting records: is Blockchain technology the answer?. Records Management Journal. 2016 Jul 18;26(2):110-39.
[17]. Cohen LR, Samuelson L, Katz H. How Securitisation Can Benefit from Blockchain Technology. The Journal of Structured Finance. 2017 Jul 31;23(2):51-4.
[18]. Zhang Y, Wen J. The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications. 2017 Jul 1;10(4):983-94.
[19]. Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. InHigh Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on 2016 Dec 12 (pp. 1392-1393). IEEE.
[20]. Sun J, Yan J, Zhang KZ. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation. 2016 Dec 1;2(1):26.
[21]. Atzori M. Blockchain technology and decentralized governance: Is the state still necessary?.
[22]. Ølnes S. Beyond bitcoin enabling smart government using blockchain technology. InInternational Conference on Electronic Government and the Information Systems Perspective 2016 Sep 5 (pp. 253-264). Springer, Cham.
[23]. Tanner H, Valtanen K. Blockchain technology in the manufacturing industry. InTowards a new era in manufacturing: Final report of VTT's For Industry spearhead programme 2017 (pp. 149-153). VTT.
[24]. Saberi S, Kouhizadeh M, Sarkis J, Shen L. Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research. 2018 Oct 17:1-9.
[25]. Alsadi A, Boodoo R, Taylor J, Diaz M, Singh M, Patel T. A Future for" BitBiopsy" and" CryptoSpecimen"? Proposed Use Cases of Blockchain Technology in Anatomical and Clinical Pathology. InMODERN PATHOLOGY 2018 Mar 1 (Vol. 31, pp. 583-583). 75 VARICK ST, 9TH FLR, NEW YORK, NY 10013-1917 USA: NATURE PUBLISHING GROUP.
[26]. Ver R, Antonopoulos AM. Blockchain Revolution How the Technology Behind Bitcoin Is Changing Money. ADC Publishing Book; 2018 Jan 25.
[27]. Hawlitschek F, Notheisen B, Teubner T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electronic commerce research and applications. 2018 May 1;29:50-63.
[28]. Jain A, Jain A, Chauhan N, Singh V, Thakur N. Seguro Digital storage of documents using Blockchain.
[29]. Mattila J. The blockchain phenomenon–the disruptive potential of distributed consensus architectures. The Research Institute of the Finnish Economy; 2016 May 10.
[30]. Lee JH, Pilkington M. How the Blockchain Revolution Will Reshape the Consumer Electronics Industry [Future Directions]. IEEE Consumer Electronics Magazine. 2017 Jul;6(3):19-23.
[31]. Pilkington M, Lee JH. How the Blockchain Revolution Will Reshape the Consumer Electronics Industry.
[32]. Scott B. How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?. UNRISD Working Paper; 2016.
[33]. Trautman LJ. Is disruptive blockchain technology the future of financial services?.
[34]. Casey M, Crane J, Gensler G, Johnson S, Narula N. The Impact of Blockchain Technology on Finance: A Catalyst for Change. Geneva Report on the World Economy. 2018(21).
[35]. Pilkington M. Blockchain technology: principles and applications. research handbook on digital transformations, edited by f. xavier olleros and majlinda zhegu.
[36]. Malinova K, Park A. Market Design with Blockchain Technology.
[37]. Saberi S, Kouhizadeh M, Sarkis J. Blockchain technology: A panacea or pariah for resources

conservation and recycling?. Resources, Conservation and Recycling. 2018 Mar 31;130:80-1.
[38]. Chatterjee R, Chatterjee R. An Overview of the Emerging Technology: Blockchain. InComputational Intelligence and Networks (CINE), 2017 3rd International Conference on 2017 Oct 28 (pp. 126-127). IEEE.
[39]. Zheng Z, Xie S, Dai HN, Wang H. Blockchain challenges and opportunities: A survey. Work Pap.–2016. 2016.
[40]. Pilkington M. Blockchain Technology: Principles and Applications (September 18, 2015). Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu.
[41]. Pilkington M. Can Blockchain Technology Help Promote New Tourism Destinations? The Example of Medical Tourism in Moldova.
[42]. Cheung AS. Data Privacy Considerations for Blockchain Technology. InTrade Law Forum–Incheon 2018 2018. United Nations Commission on International Trade Law..
[43]. Wang B, Zhu X, He Q, Gu G. The forecast on the customers of the member point platform built on the blockchain technology by ARIMA and LSTM. In2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA) 2018 Apr 20 (pp. 589-593). IEEE.
[44]. Nguyen QK. Blockchain-a financial technology for future sustainable development. InGreen Technology and Sustainable Development (GTSD), International Conference on 2016 Nov 24 (pp. 51-54). IEEE.
[45]. Ouaddah A, Elkalam AA, Ouahman AA. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. InEurope and MENA Cooperation Advances in Information and Communication Technologies 2017 (pp. 523-533). Springer, Cham.
[46]. Treleaven P, Brown RG, Yang D. Blockchain Technology in Finance. Computer. 2017 Sep 1(9):14-7.
[47]. Angraal S, Krumholz HM, Schulz WL. Blockchain technology: applications in health care. Circulation: Cardiovascular Quality and Outcomes. 2017 Sep 1;10(9):e003800.
[48]. Raval S. Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. " O'Reilly Media, Inc."; 2016 Jul 18.
[49]. Kennedy ZC, Stephenson DE, Christ JF, Pope TR, Arey BW, Barrett CA, Warner MG. Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology. Journal of Materials Chemistry C. 2017;5(37):9570-8.
[50]. Pilkington M. Can Blockchain Improve Healthcare Management? Consumer Medical Electronics and the IoMT.
[51]. Strobel V, Castelló Ferrer E, Dorigo M. Managing byzantine robots via blockchain technology in a swarm robotics collective decision making scenario. InProceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems 2018 Jul 9 (pp. 541-549). International Foundation for Autonomous Agents and Multiagent Systems.
[52]. Eyal I. Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. Computer. 2017;50(9):38-49.
[53]. Wright A, De Filippi P. Decentralized blockchain technology and the rise of lex cryptographia, 2015. Retrieved August. 2015;1:2017.
[54]. Adams M. Blockchain: The History, Mechanics, Technical Implementation And Powerful Uses of Blockchain Technology. CreateSpace Independent Publishing Platform; 2016 Oct 20.
[55]. Zhu H, Zhou ZZ. Analysis and outlook of applications of blockchain technology to equity crowdfunding in China. Financial innovation. 2016 Dec;2(1):29.
[56]. Oketch ML. Govt to Use Blockchain Technology to Improve Service Delivery. Friday May 4, 2018.
[57]. Randall D, Goel P, Abujamra R. Blockchain applications and use cases in health information technology. Journal of Health & Medical Informatics. 2017;8(3).
[58]. Wong MC, Yee KC, Nohr C. Socio-technical consideration for blockchain technology in healthcare: the technological innovation needs clinical transformation to achieve the outcome of improving quality and safety of patient care. Studies in health technology and informatics. 2018;247:636-40.
[59]. Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for IoT data access protection. InUbiquitous Wireless Broadband (ICUWB), 2017 IEEE 17th International Conference on 2017 Sep 12 (pp. 1-5). IEEE.