Global Scientific and Academic Research Journal of Multidisciplinary Studies
ISSN: 2583-4088 (Online)
Frequency: Monthly
Published By GSAR Publishers
Journal Homepage Link- https://gsarpublishers.com/journals-gsarjebm-home/

5irechain Security and Privacy beyond Technology and Crypto Currencies

BY

MD AHBAB[1], JATINDER ARORA[2*], VILMA MATTILA[3]

[1&3]5irechain, Dubai Silicon Oasis, United Arab Emirates

[2]Narre Warren South State VIC 3805, Australia

Article History

Received: 04/10/2022
Accepted: 11/10/2022
Published: 14/10/2022

Vol – 1 Issue – 7

PP: - 14-19

Abstract

The block chain is one of the most disruptive, complex, and incipient information technologies whose vertiginous growth is transversal to all sectors of activity in the public and private spheres. Beyond crypto currencies, it has enormous potential as a paradigm of decentralization and empowerment of natural and legal persons along with many regulatory, jurisdictional, and technological challenges such as scalability, interoperability, or environmental impact. That is why in the paper we tried to explain how 5ire block chain technology works with its technological challenges and technical knowledge at a general level relates to security and privacy of the 5irechain beyond technology and crypto currencies.

Keywords: *5irechain, crypto currency, technological challenges, privacy*

1. Introduction

It is not known how this new sector will affect the future, but what is known is that most of the leading companies, governments, and international monetary institutions are investing time and many resources in researching and becoming part of this new world. Perhaps, today we are not yet facing a true economic revolution. But it is undeniable that we are on the verge of a great change, especially in the financial and banking sector (Boot et al. 2021). Being able to carry out cross-border transactions almost immediately and with hardly any costs, the opportunity to finance small businesses and large projects independently and in a decentralized and transparent manner, user privacy, and the reduction of costs and greater efficiency for institutions are some of the advantages that blockchain technology offers today (Chen and Bellavitis 2020). The future depends on how those who are going to be behind the great transitions act, that is to say; banks, international financial institutions, and governments (Toufaily et al. 2021; Chen and Bellavitis 2019). They are going to be responsible for solving a very important conflict on which it will depend whether the user accepts this new emerging sector. The problem lies in how to strike a balance between consumer privacy and control of illicit activities. Blockchain technology allows value transactions to be carried out between users without the intervention of intermediaries in the process that decentralizes the management of transactions and presents all its participants with the same decentralized ledger or database (Tilooby 2018). The transactions can be monetary (cryptocurrencies) or of another nature (goods, information, services, etc.) and are carried out on platforms whose nodes communicate through networks of peers (P2P) through Internet connections (Tilooby 2018; Funk et al. 2018). The blockchain offers a dynamic and unalterable representation or record of these transactions over time that replaces intermediaries and centralized trusted authorities that support the transactions for the digital trust that users have deposited in this technology. The blockchain offers transparency, sharing and decentralization, irreversibility and disintermediation. The blockchain links the sequence of transactions and incorporates a timestamp that gives transparency and traceability to operations without violating the privacy of users a priori where the path and the content can be known, although it is not always feasible to infer the identity of the user. The actors can adopt three roles: assessors, participants and miners. All of them have a validated and unique copy of the database. Each platform establishes its rules of participation, operation and governance. Platforms can be open (public) if they are accessible without restrictions, such as the Bitcoin cryptocurrency. They are semi-public or authorized when participation. They can also be private when an actor sets the rules; in this case, the difference between a blockchain and a conventional decentralized database is blurred. The

*Corresponding Author: **JATINDER ARORA**

blockchain uses cryptographic security mechanisms to access, sign and encrypt transactions, blocks and their chaining (Ferdous et al. 2021). Private keys can be linked to the identity of users or to intermediate elements; for example, the digital wallets with which the platform offers the anonymity of operations. The rules that execute the transactions can be established through smart contracts. For example, they ensure a common understanding of the transaction between the parties, in particular on the obligations contracted, offering limited probative visibility to the interested parties. Certain network nodes specialize in validating the transaction and writing it encrypted in the block, chaining it to the pre-existing ones once completed. Before a new block can be added to the chain, its authenticity must be verified by a consensus validation process. The consensus mechanism ensures that all copies of the distributed workbook share the same state (Si et al. 2019). Once the transaction is validated, the "mining" nodes update the distributed database by adding the transaction to the block of transactions in progress; when this block reaches a given number of validated transactions, the "miners" proceed to seal it and incorporate it into the chain, leaving these transactions permanently registered. Mining nodes use mathematical algorithms to convert a block's information into an alphanumeric or hash code that links to the previous block's hash and chain the blocks together. For each block added to the chain, the mining node receives remuneration in cryptocurrencies or a share in the business that is the object of the transaction; once a block is added, it is immutable. The participation of the mining nodes follows the rules defined by each platform regarding the consensus mechanism which largely determines the security, reliability, speed, and computational and energy cost of the process (Bhushan et al. 2021).

2. Methodology

The methodology used descriptive analysis and consists of searching information from academic journals indexed in Web of Science, Scopus, and DOAJ. Documents in physical and digital media were used. In addition, analysis of consistent strategic model is used to analyze the attractiveness of industries in the adoption of technology and thus determine through business analysis models which are the industries in which it will have the greatest impact. Besides of the analysis of internal and external documents such as strategic plan, operational planning, certification reports, list of performance indicators contributed to understanding the formal rules and aspects of the organization related to its process and decision making.

3. The Technological Challenges and BlockchainBeyond Cryptocurrencies

The complexity, the speed of growth, the proliferation of a large number of different platforms, or their high business potential make it difficult to solve significant technological challenges such as scalability, standardization, or interoperability, aspects of which have a special impact on security (Light et al. 2019). The need for scalability is accentuated by the exponential growth of major public platforms (Rodrigues et al. 2018). As the network grows, the competition to perform validations increases, it takes longer and the unit cost per transaction increases. Therefore, new consensus mechanisms are needed that reduce processing time without compromising security. The need for interoperability is accentuated given the proliferation of different solutions and the need to share data between platforms or to use common electronic wallets (Adesina and Osasona 2019). The exchange of data requires the translation between protocols and the reconciliation of different consensus mechanisms which is made difficult by the absence of standards (Noura et al. 2019). Beyond the technical aspects, interoperability between platforms will also have to respond to needs such as the ease of use of applications and the ability to transfer assets, limit the volume of transactions, prevent them or establish safeguards against fraudulent changes of ownership. A technological challenge in permanent debate is energy efficiency, given the high intrinsic consumption of the blockchain and the significant hidden cost linked to the consensus mechanisms for the validation and calculation of blocks carried out by the mining nodes. These factors are directly related to the environmental impact and determine the need for more efficient and secure validation protocols that facilitate the participation in the blockchain platform of autonomous devices with limited consumption. There are countless blockchain applications currently under development with uses other than cryptocurrencies in practically all sectors (Ku-Mahamud et al. 2019). For example, the financial sector is worth mentioning (banking transactions between entities, means of payment, insurance policies), logistics (traceability and management of merchandise), energy (integration of means of generation to the electricity grid), health and pharmaceutical (histories, medical management, drug tracing), the audiovisual industry (management of rights through the value chain of the work), tourism (management of reservations, hiring, rates, loyalty actions, identity management, baggage tracking), Industry 4.0 (building secure communications in industrial networks through real-time updated registration of reliable IoT devices integrated into the network operations) or the Public Administration (management of licenses, transactions, events, movement of resources and payments, property management, identity management). It is worth mentioning the application of the blockchain in the field of digital identity as a system to validate identities in an irrefutable, secure and immutable way, which would allow citizens to control the use of their data by third parties. In the legal and regulatory field, this technology makes it possible to trace compliance with contractual and regulatory obligations. In each sector and company, the proliferation of blockchain platforms will have important economic (investment, minimum scale, economies of scale), organizational (incorporation of cybersecurity, compliance and privacy departments into the design) and governance, as well as training implications. In this sense, the role of public authorities and public-private collaboration play a key role.

4. The Security of The Blockchain and Design of 5irechain Privacy

The blockchain is a conceptually secure technology. Vulnerabilities usually arise as a result of the implementation of platforms and applications that are linked to the development of computer code, communication protocols, or the simplification of block validation and consensus mechanisms (Kumar and Goyal 2019). The blockchain is a recent and complex technology. Despite thorough code design and review, vulnerabilities due to programming errors cannot be excluded. Once these have been identified, they are especially complicated to patch without affecting the service due to the distributed architecture and the immutability of the blockchain. The vulnerabilities are accentuated by the multiplicity of programming languages and protocols by the absence of technological standards (Brent et al. 2020). This fragmentation slows down the maturity curve of this technology, reduces the chances of detecting errors and implementing controls over the code, and disperses the experience of developers, who are under constant pressure to shorten delivery times. Likewise, the integration of blockchain platforms with the information systems that support the company's business processes or the interoperability between different blockchain platforms is still very incipient which limits efficiency and increases cyber-security risks. It can take years to reach a degree of maturity and technical consensus that facilitates the convergence of security standards and interoperability between platforms. Therefore, developers and companies must unavoidably incorporate security-by-design methodologies from the early stages of development, with the participation of information systems and cybersecurity departments. Platforms, services, and networks share security risks with information technologies, such as confidentiality, privacy, key management, cryptography, identification and patching of vulnerabilities, or awareness of social engineering threats. But they also offer specific risks:

- Distributed denial of service attacks by injecting a high number of spam transactions
- Attacks focused on the capabilities of the managing entity of an authorized blockchain.
- Hijacking of the consensus mechanism through the coalition of users (51% attack) or one-off acquisition of large cloud computing capacity
- Sidechain or parallel mining due to less mining capacity or the possibility of attacks that can block a sidechain and reverse the transactional load by overloading the root blockchain;

As the number of blocks in a chain increases mining nodes that tend to pool as the chance of an individual node stamping a block and getting the reward decreases. This concentration can pose vulnerabilities in obtaining a reliable consensus if the preponderance of a few pools is dominant on the platform. In relation to the widespread use of smart contracts to carry out transactions, they are exposed to errors and vulnerabilities – more likely to the extent that smart contracts are more complex – derived from their coding. In addition to programming errors, blockchain technologies face risks that have to do with cryptographic techniques that ensure the confidentiality and integrity of the transaction records. Therefore, it should be assumed that blockchain platforms are exposed to cybersecurity and operational risks similar to those of any information system, as evidenced by numerous cyber incidents of great impact for clients, such as those contained in the "McAfee BlockchainThreat Report 2018" or the CipherTrace report that analyzes criminal activity in the cryptocurrency market. Examples of incidents are referenced below:

- In August 2010, a hacker generated 184.467 million bitcoins in one transaction using a code vulnerability known as a "value overflow incident," which was fixed within hours.
- In January 2018, Coincheck, one of the most popular exchanges in Japan, lost $532 million worth of NEM coins, affecting 260,000 investors. A cybercriminal had accessed an employee's computer and installed malware to obtain keys for the digital wallets used in immediate online transactions (hot wallet) and empty the accounts.
- In March 2018, Schneier on Security echoed the vulnerabilities of smart contracts on blockchain platforms such as Ethereum.
- In May 2019, the Binance platform suffered the theft of 41 million dollars in bitcoins. The hackers used various techniques, from viruses to phishing, to break into the system and access a company's bitcoin wallet from which its customers were making transactions.
- In 2019, the death of the CEO of a crypto asset management fund caused the disappearance of the credentials to access the cryptocurrencies it managed, worth more than 150 million dollars, which became unrecoverable.

The wide variety of incidents unrelated to the conceptual design of the blockchain is significant, as is the strong growth in reported crimes: cryptocurrencies stolen from exchanges and swindled from investors increased by more than 400% in 2018, reaching around 1,700 million dollars (Reddy, Minnaar, and Victimology 2018). To the change of the $1.7 billion, $950 million was stolen from cryptocurrency exchanges and infrastructure, an increase of nearly 260% from the $266 million stolen in 2017. At this point, it is important to reiterate the importance of taking care of the non-technological aspects derived from incorporating a blockchain platform into business processes or operations, in particular those related to organizational and business process impacts. For example, the company's information security department will have to be involved in the design of the solution from its inception, as well as in its implementation, as with any other technology platform. In a different area, the growing acceptance and anonymity that characterize the transactions of the new cryptocurrencies have led to crypto-jacking or illegitimate use by cyber criminals of the processing capacity of non-blockchain computer equipment to fraudulently obtain

cryptocurrencies. Crypto-jacking subtracts resources (computer, memory, energy) from the affected user's computer to appropriate assets from a blockchain platform. It is estimated that in January 2018 the number of samples of this type of malicious code was around 94,000, while only three months later this figure increased by 74% (Seligman 2022). The blockchain raises new and complex questions regarding the protection of privacy rights in the use of personal data and in particular when the transactions manage personal data or the information of the blocks does reference to personal data of the participants.

In this sense, 5ire indicates four generally applicable guidelines and strategies to its developers:

- Start the design at a high level avoiding that the blockchain becomes an innovative solution in search of a problem (e.g. what is the value contribution of the solution for the user? How to manage the data?)
- Avoid storing personal data; use obfuscation, encryption, and aggregation techniques to anonymize this data.
- Keep personal data out of blocks whenever possible; analyze the transfer of personal data by connecting private and public blockchains.
- Offer full transparency to users about data processing.

5. Security and Privacy Beyond Technology and Cryptocurrencies and 5ire Solution

5.1. ARCO Rights (Access, Rectification, Cancellation, Opposition) and 5irechain

ARCO rights are the rights of access, rectification, cancellation, and opposition (Nieves-Lahaba and Ponjuan-Dante 2021). However, regarding the rights of rectification, cancellation, and opposition we could find conflicts by not being able to modify or delete network information. Having said the above, then we may address some possible solutions to the intersection of this blockchain technology and the protection of personal data.

Solution #1: Change data and have branch

In a broad sense, data is not totally immutable, there is the possibility of change since nodes control all copies of the network, and the moment the stored data was changed, it would give as result in new versions, called forks. That is, it could also be the case of modifying the chain of blocks, but this would create a Fork where there would be a split in the blockchain, where two different branches exist for a period of time. The first is the Hard Fork because after the fork the network is not reconverted into a single chain, the two chains evolve independently (Webb and Technology 2018). Hard forks happen when part of the network is operating under a different set of rules consensus than the rest of the network. This may occur due to an error or due to a deliberate change in the implementation of the consensus rules.

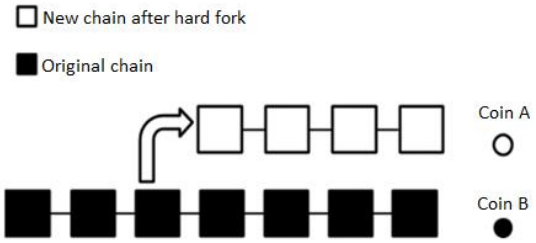

Fig.1. Hard Fork

The second is the Soft Fork and it is a change compatible with the advancement of the consensus rules that allows clients not updated continue to operate in consensus with the new rules. An aspect of soft forks, which is not so obvious, is that soft fork updates can only be used to restrict consensus rules, not to expand those (Antonopoulos 2017). That is, the Soft Fork is a temporary divergence where the nodes that have not been updated will break some of the new rules. Therefore most of the mining nodes are required to upgrade towards the new rules.

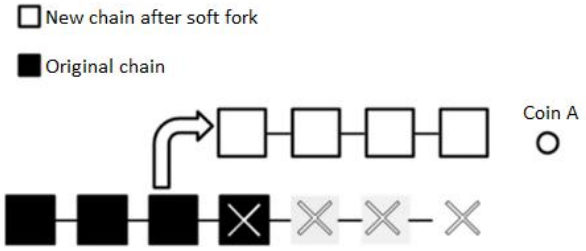

Fig. 2. *Soft Fork*

With these Forks, which are updates to the protocol, would lead to the modification of rules to a lesser or greater degree. Which will cause, depending on the type of modification that is added, the nodes whether or not they will continue to accept the new blocks that are generated and added to the Blockchain. The result will be new and diverse blockchains, every time you need to modify information.

***Solution #2:* Store the personal data off-chain and hash on-chain**

There is a structure outside the chain, merely adding references; identifiers, or rather encrypted data, hashed, in order to verify the integrity of the personal data, when they are compared to those of the Blockchain network.

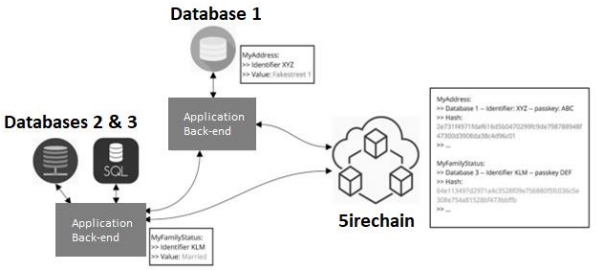

Fig. 3. *Information storage solution offline and on-chain hashes*

Above graph, we can see how two different entities process data on the Blockchain network; conversely, it only stores in the network the hash, or encrypted chain to "verify if this data has not been influenced by calculating the hash of the

retrieved data and comparing them with the hash provided by the Blockchain. If they counterpart, the data is not they have been manipulated"(Humbeeck and Privacy 2019).

Solution #3: private communication channel and hashes

Another solution (Humbeeck and Privacy 2019) is the one proposed by the company Grant Thornton which consists of private channels with encrypted data, and whose operation would be:

1) Nodes A and B create a private channel on the Blockchain.
2) Encrypted personal data is shared in the private channel between A and B.
3) The encrypted data hash is stored on the "common" Blockchain, that is, the rest of the nodes (C, D, E, F, G, H, and I) know that A and B have shared information at a specific time, but not they can view the content: they only see the hash

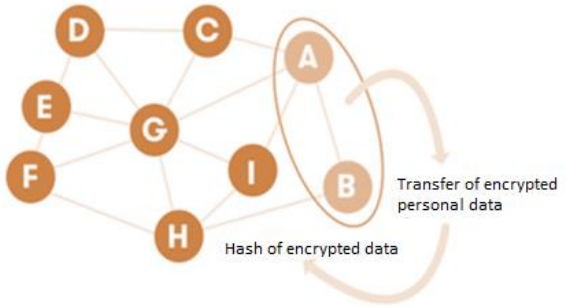

Fig. 4. ***Data transfer between private channel and the encrypted data to the rest of the network***

By means of this mechanism, it could be classified as elimination of the data, although firmly speaking; they are simply anonymized because they are not eliminated; only the hashes remain as random anonymous data so that they become intelligible and irrelevant.

Solution 4: Delete encryption keys

The solution of destroying the encryption keys means that when intends to modify the blockchain, the data becomes unusable or unintelligible: "removing the key is an effective way to put to zero the protected data without actually modifying the database. The encrypted data cannot be recovered if the key is no longer available. It is not elimination, and it would have to be considered the legislative technique of legal systems to know if this fulfills as suppression. A possible exception to this erasure technique is the one contemplated by the Information Commissioner's Office in the United Kingdom when mentioning that it is satisfied that the information has been put out of use, if not actually deleted, provided that the data controller cannot, attempts or uses the personal data, as well as does not give access to the information to another organization, and surround the personal data with measures technical and security as well as the commitment to the permanent elimination of information when this is possible.

Fig. 5. ***Elimination of the private key, to convert the data in illegible and anonymized information, and comply with the rights of cancellation and opposition***

5.2. Data transmission in blockchain networks

Before thinking about data transmission, it is necessary to clarify something about the controller of the data for its treatment. In the case of Blockchain, there are miners who have multiple functions of validating the transactions. This is how the obligatory question arises about whether the nodes are data controllers? To understand the nature of miners, it is important to make a classification link. Three types of nodes could be defined as actors in the field of personal data protection, which are:

- "Accessories", who have the right to read and keep a copy of the string
- "Participants", who have the right to make entries
- "Miners", who validate a transaction, and create blocks where apply the rules of the blockchain so that the community "accept" them.

Another fundamental problem is the consent part since each transmission is considered as treatment. In the case of private blockchains, it could be guaranteed but in the case of public ones, it is complex and debatable especially if the data transmission takes place outside the country. For such case, the solution can be the following: Users responsible for their own information personal where no one controls or owns it. In the case of a DLT, being a consortium that decides to share a distributed registry, the controller of the data must be defined from a beginning. In the event that there are several controllers, it will be necessary to reach an agreement. On the other hand, in public blockchains, the participant can be considered a data controller, since the participant determines the purpose and means of data processing.

6. Conclusion

The blockchain is one of the most disruptive, complex, and emerging information technologies whose vertiginous growth is transversal to all sectors of activity in the public and private spheres. Beyond cryptocurrencies, it has enormous potential as a paradigm of decentralization along with many regulatory, jurisdictional, and technological challenges such as scalability, interoperability, or environmental impact. Consequently, the application of the principles of security and privacy by design are inescapable from the initial phases of the design together with considerations resulting from integrating the blockchain platform to business processes or

operations. Facing these challenges requires the creation of multidisciplinary teams that 5ire already belongs which have the participation from the beginning of the legal/regulatory area, cyber-security, and company information systems. During this study, we address various points of view regarding blockchain and its intersection with the transparency and protection of personal information. We address various tangible approaches and questions, in relation to whether the data processed by this technology is considered as personal data, being encrypted under a hash function as a result of pseudonymization or anonymization/dissociation. Likewise, the teleological attribute of transparency in blockchain networks was addressed if raised the controversy between the rights of rectification, cancellation, and opposition, right to be forgotten, deletion, or deletion of information against the primordial and original characteristic of blockchain. In the case of the controllers or those responsible for the treatment of the personal data, it is necessary to previously identify them. If there are several subjects, we recommend forming a legal entity.

Acknowledgment

The authors would like to acknowledge a research grant from "Innovation and Research of 5irechain"

References

1. Adesina, Tolulope, and Oladiipo Osasona. 2019. "A novel cognitive IoT gateway framework: Towards a holistic approach to IoT interoperability." In *2019 IEEE 5th world forum on internet of things (WF-IoT)*, 53-58. IEEE.
2. Antonopoulos, Andreas M. 2017. *Mastering Bitcoin: Programming the open blockchain* (" O'Reilly Media, Inc.").
3. Bhushan, Bharat, Preeti Sinha, K Martin Sagayam, J %J Computers Andrew, and Electrical Engineering. 2021. 'Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications, and future research directions, 90: 106897.
4. Boot, Arnoud, Peter Hoffmann, Luc Laeven, and Lev %J Journal of Financial Stability Ratnovski. 2021. 'Fintech: what's old, what's new?', 53: 100836.
5. Brent, Lexi, Neville Grech, Sifis Lagouvardos, Bernhard Scholz, and Yannis Smaragdakis. 2020. "Ethainter: a smart contract security analyzer for composite vulnerabilities." In *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation*, 454-69.
6. Chen, Yan, and Cristiano %J Journal of Business Venturing Insights Bellavitis. 2020. 'Blockchain disruption and decentralized finance: The rise of decentralized business models, 13: e00151.
7. Chen, Yan, and Cristiano %J Stevens Institute of Technology School of Business Research Paper Bellavitis. 2019. 'Decentralized finance: Blockchain technology and the quest for an open financial system'.
8. Ferdous, Md Sadek, Mohammad Jabed Morshed Chowdhury, Mohammad A %J Journal of Network Hoque, and Computer Applications. 2021. 'A survey of consensus algorithms in public blockchain systems for crypto-currencies, 182: 103035.
9. Funk, Eric, Jeff Riddell, Felix Ankel, and Daniel %J Academic Medicine Cabrera. 2018. 'Blockchain technology: a data framework to improve validity, trust, and accountability of information exchange in health professions education, 93: 1791-94.
10. Humbeeck, Andries Van %J Journal of Data Protection, and Privacy. 2019. 'The blockchain-GDPR paradox'.
11. Ku-Mahamud, Ku Ruhana, Mazni Omar, Nur Azzah Abu Bakar, Ishola Dada %J International Journal on Advanced Science Muraina, Engineering, and Information Technology. 2019. 'Awareness, trust, and adoption of blockchain technology and cryptocurrency among blockchain communities in Malaysia', 9: 1217-22.
12. Kumar, Rakesh, and Rinkaj %J Computer Science Review Goyal. 2019. 'On cloud security requirements, threats, vulnerabilities, and countermeasures: A survey, 33: 1-48.
13. Light, Janice, David McNaughton, David Beukelman, Susan Koch Fager, Melanie Fried-Oken, Thomas Jakobs, Erik %J Augmentative Jakobs, and Alternative Communication. 2019. 'Challenges and opportunities in augmentative and alternative communication: Research and technology development to enhance communication and participation for individuals with complex communication needs, 35: 1-12.
14. Nieves-Lahaba, Yadira Rosario, and Gloria %J Universitas-XXI Ponjuan-Dante, Revista de Ciencias Sociales y Humanas. 2021. 'Access to information and processing of personal data. Visions from the academy': 167-85.
15. Noura, Mahda, Mohammed Atiquzzaman, Martin %J Mobile networks Gaedke, and applications. 2019. 'Interoperability in internet of things: Taxonomies and open challenges', 24: 796-809.
16. Reddy, Eveshnie, Anthony %J Acta Criminologica: African Journal of Criminology Minnaar, and Victimology. 2018. 'Cryptocurrency: A tool and target for cybercrime', 31: 71-92.
17. Rodrigues, Tiago Gama, Katsuya Suto, Hiroki Nishiyama, Nei Kato, and Katsuhiro %J IEEE Transactions on Computers Temma. 2018. 'Cloudlets activation scheme for scalable mobile edge computing with transmission power control and virtual machine migration', 67: 1287-300.
18. Seligman, Joel %J Washington University in St. Louis Legal Studies Research Paper. 2022. 'The Rise and Fall of Cryptocurrency: The Three Paths Forward': 01.
19. Si, Haiping, Changxia Sun, Yanling Li, Hongbo Qiao, and Lei %J Future Generation Computer

Systems Shi. 2019. 'IoT information sharing security mechanism based on blockchain technology, 101: 1028-40.

20. Tilooby, Al. 2018. 'The impact of blockchain technology on financial transactions.
21. Toufaily, Elissar, Tatiana Zalan, Soumaya Ben %J Information Dhaou, and Management. 2021. 'A framework of blockchain technology adoption: An investigation of challenges and expected value', 58: 103444.
22. Webb, Nick %J North Carolina Journal of Law, and Technology. 2018. 'A fork in the blockchain: income tax and the bitcoin/bitcoin cash hard fork', 19: 283.