International Journal of Social Sciences and Management Review

Volume: 05, Issue: 05 "September - October 2022"

ISSN 2582-0176

SECURITY FROM THE FIRST PHASES OF 5IRECHAIN LIFE CYCLE

[1]Md AHBAB, [2]VILMA MATTILA & [3]JATINDER ARORA

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

[2]5irechain, Dubai Silicon Oasis, United Arab Emirates

[3]Narre Warren South State VIC 3805, Australia

https://doi.org/10.37602/IJSSMR.2022.5507

ABSTRACT

The security of blockchain technology is more than ever in the point of view. Attacks on DLTs (Distributed Ledger Technology), including blockchain, which highlight the need to reinforce their security. The use of security reference architectures (SRA) has proven useful in addressing safety in the early phases of development facilitating the definition of security requirements and helping to implement security policies that allow us to protect a system throughout the life cycle. This article presents an SRA for the technology Blockchain defined through models and checking its application through an example of use.

Keywords: Blockchain, 5ire, SRA, reference architecture

1.0 INTRODUCTION

Since the appearance of Bitcoin in 2008, blockchain technology has not stopped add followers. Proof of this interest is the growing investment being made on blockchain in both industry and academia. This growing investment can be seen reflected in the MarketsandMarkets study, in which it is estimated that the use of blockchain will go from 258 million dollars in 2020 to 2,409 million dollars in 2026, with an average annual growth rate of 45.1%. In addition, the results of the 2020 global annual survey on blockchain conducted by Deloitte revealed that 53% of organizations consider blockchain to be one of its five strategic priorities. Even though blockchain technology is presented as a ledger technology of tamper-proof transactions, it is a reality that blockchain networks they are not immune to cyberattacks and fraud. In fact, it is estimated that during the first quarter of 2019 saw the loss of more than 356 million dollars in blockchain networks due to security- related issues. Some concrete examples of these actions are the loss of 13 million dollars of EOS and 6 million of dollars in Ripple only during the month of March 2019. Also, a new report from cryptocurrency forensics and blockchain threat intelligence firm Ciphertrace shows that $100 million has been stolen from distributed networks only in 2020, which reinforces the importance of security being present in any blockchain solution. There are many variables to consider when designing a security solution. In general, security threats fall into three main categories: Endpoint vulnerabilities, untested code, and risk in your own ecosystem or third parties. First of all, endpoint vulnerabilities are presented as the most direct and potentially easier to attack over any technological solution such as digital wallets, devices, or applications. If one of these points is compromised and a malicious actor gains access to an account, unless additional security protections are put in place, it is possible that a fraudulent action without producing any external alarm or behavioral abnormal signal. Second, the

untested code is a reflection of how as new technologies enter the market, developers are incentivized to be the first to submit a solution, often at the risk of deploying code insufficiently tested on active blockchains. A well-known example is an attack on the decentralized autonomous organization (DAO) of the Ethereum network in 2016, where code and smart contracts were developed in which vulnerabilities existed in the code. This led to the exploitation of a vulnerability that had the ability to manipulate smart contracts to extract money due to a mistake in a recursive call with which it was possible to divert nearly 60 million dollars. As the last threat, it highlights the risk inherent in the ecosystem of applications that use blockchain which may include association with vendors or third parties. Poor ecosystem security or flawed code can expose user credentials and blockchain data to unauthorized persons. To deal with security threats, security must be addressed from of high-level policies that can be transferred to lower levels. The Architectures Reference Models (RA) provides an abstract model that supports one or more domains and has no implementation features thus allowing them to be reusable, scalable, and configurable. Incorporating a set of elements that facilitate the definition of security requirements and allow a better understanding of security, policies, threats, and vulnerabilities, we get a Security Reference Architecture (SRA), that is, the architecture of a high level that can be used to describe a conceptual security model of a system. In this work we have defined an SRA for blockchain, based on the different proposals from the scientific community, the different proposals from the industry, and the usual implementation of multiple blockchain systems abstracting their components and based on the main attacks that make a blockchain system vulnerable to identify the elements of the architecture that are most vulnerable and on which the implementation of a security solution should be focused. Our study presents an architecture that serves as a basis for the development of a blockchain system, whether for academic purposes or in industry, considering the security from system design integrated into the technology stack blockchain to prevent it from being considered only at launch, or as something that surrounds an application once it has been developed. We organize the content of the manuscript as follows: first, existing related works are presented; Second, we present our SRA proposal for blockchain which we will use in 5irechain; Third, we compare our architecture with a real case study showing how the different components can be instantiated that are involved in their approach. Finally, we include a section in which conclusions and future work are discussed.

2.0 RELATED WORKS

The standardization of blockchain technology is an important step toward a concept common, interoperability, scaling, auditing, and possible subsequent regulation of technology. Although there are several initiatives to define norms and standards for the development and maintenance of the blockchain, they are in a very preliminary phase, this being an obstacle to the settlement of the technology. There are multiple initiatives of organizations that are working on documents of standardization. NIST (National Institute of Standards and Technology which is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce) published in 2018 NISTIR 8202 - Blockchain Technology Overview. The document addresses the functionalities and fundamental components of a system blockchain as well as cybersecurity concerns and the general applicability of blockchain in organizations. The purpose of this document is solely to serve as an entry point to blockchain technology, as it explains the structure and models, consensus

mechanisms, and known examples of it, as well as a series of questions and considerations specific to the blockchain without going into depth in the technical elements. ANSI SCX9 (American National Standards Institute is a private non-profit organization that oversees the development of voluntary consensus standards) also published in 2018 the report of its study group on DLT and blockchain. In this study, they worked together with experts from various fields and evaluated what types of standardization efforts would be both necessary and beneficial especially for the financial sector, but also for other industries, as well as to increase the adoption of DLT. The biggest part of the document focuses on blockchain security needs and issues which he deals with mainly by focusing on the financial field. To facilitate understanding of the key components of blockchain systems, the high-level reference architecture is included in the appendix to provide an overview of the operation of a DLT system. The UNE 71307-1 standard defines a generic reference framework for the management of identities of individuals or organizations, allowing control of your own digital identity in a self-managed way in a blockchain system. ISO/TR 23455:2019 offers an extensive discussion of smart contracts within a blockchain system/DTL and its operation. It is also possible to appreciate the interest in addressing security by design, the standard DIN SPEC 4997 Privacy by Blockchain Design describes a standardized model for the processing of personal data through blockchain taking into account the Regulation General Data Protection (GDPR) of the EU. The document presents an overview of the risks and mitigations of data protection principles with a clear focus on privacy by design, as well as a privacy architecture project by the design of blockchain. Homoliak proposes a specific version-based architecture for the blockchain of the ISO/IEC 15408 threat risk assessment standard by adaptation of a customized version of the presented four-layer stacked model in the work of Wang et al. This proposal differs from this work, which focuses solely on risk without considering business objectives or orchestration of security policies. Despite the growing interest in the standardization of blockchain systems, it is not Studies have been carried out that have defined security architectures in which address the implementation of its different components. In this article, we studied an SRA sketch for 5irechain where the components of the blockchain are specified technology as well as the relationships between the different components and subcomponents. Different security concepts are also integrated to ensure the protection of these types of systems.

3.0 SECURITY REFERENCE ARCHITECTURE FOR BLOCKCHAIN

In this work we have analyzed the functionalities and fundamental components of a blockchain system that have been proposed by NIST (National Institute of Standards and Technology), as well as the concerns of cybersecurity and the general applicability of blockchain. Also they have been considered the main implementations of blockchain in the market focusing on in Bitcoin, Ethereum, and Hyperledger for being the most consolidated technologies today and its main components have been abstracted to create our architecture.

We have defined our SRA through UML diagrams as we found a lack of proposals that precisely define the relationships between the different components and subcomponents. Likewise, it is a language widely accepted that facilitates the understanding of the relationships between the different components. A layered model has been used since it offers us simplicity in the implementation and maintenance, flexibility and scalability.

The architecture is divided into six different components that interact with each other with different objectives: business layer, orchestration layer, application layer, service layer, platform layer, and network layer.

3.1. Business layer

The purpose of the business layer is to define the business rules that collect the functionalities that the blockchain network must offer. Due to the characteristics of this layer, related security activities are generally focused on defining of security policies from the orchestration layer, described in the next section, and how to implement and monitor them. The blockchain system must satisfy the objective for which it has been created by fulfilling with the objectives while staying aligned with the different objectives business and company policies. In this sense, the role of the manager security is crucial to ensure compliance with security requirements. These safety requirements must comply with the regulations that affect each context of the ecosystem and will be defined in the next layer.

3.2. Orchestration layer

The orchestration layer aims to address the different requirements that must be fulfilling the blockchain ecosystem. According to Biktimirov, technology requirements blockchain can be divided into the following groups:

- Structural requirements on the availability of certain types of data in blockchain links to ensure the technology works.
- Business requirements related to enforced policies, such as standards of international cryptography, as well as national or institutional standards in the areas of application: taxation, voting technologies, the workflow of internal documents, etc. These requirements must be aligned with the objectives of the business process to fulfill the function for which they have been defined.
- Technological requirements on the reliability of block storage, using the technology proposed by Zitsev to maintain the parameters of reliability and availability of link storage.
- Reliability requirements with a clear blockchain structure, technologies regulated link processing and an interface for link operations. All applied interfaces must be available with source code to ensure a high level of trust.

Security requirements can be satisfied by different security solutions that follow the company's security policies and aim to address threats to control vulnerabilities. The definition of these security solutions can be guided by the use of security patterns, which can be defined as a solution to recurring problems that indicate how to defend against a threat, or a set of threats, concisely and reusable.

3.3. Application Layer

The application layer contains solutions for the end user and applications that are built on the blockchain network; therefore, security threats are specific for each application. This layer may exist totally or partially outside the network [19]. One of the core elements of the application layer are Applications. Decentralized or DApps. These are software applications

Volume: 05, Issue: 05 “September - October 2022”

ISSN 2582-0176

that run on a network. A decentralized peer-to-peer network is usually a blockchain network. DApps usually include a user interface running on another system (centralized or decentralized). DApps also include blockchain explorers, monitoring tools, and other business intelligence tools. Browsers implemented on a blockchain network are the most common way of retrieving information, the trusted parties usually being centralized. In the case of monitoring tools, they facilitate the management of multiple networks, the identification of problems and the general maintenance of the health of the network of the block chain. Business intelligence tools also provide a platform for tracking records held in your database encrypted ledger-based.

Since developers are allowed to develop their own DApps with contracts custom smart apps are highly vulnerable to attack. In some cases, it is common for an attack to occur in the information transfer phase of the node. Apply a specific security solution based on how the application works will reduce their impact.

3.4. Service layer

The service layer makes it possible to make the blockchain more accessible, in particular for businesses, reducing the costs and overhead of technology adoption. The precise nature of a SaaS (Software as a Service) implementation will depend on the service provider, application specifications and objectives of the client. This layer integrates asset managers, blockchain events. Asset management aims to ensure the management of the assets of the platform layer, with assets stored on the blockchain being the reason principal of the chain's existence. The digital asset can be monetary units or of another type, on which an organization wants to interact. Asset management can be integrated with business management systems through external interfaces using APIs, libraries and common techniques. A connection directly with the blockchain core allows the correct functioning of these tools. In addition to deployment and configuration capabilities, it is important that there are possibilities to manage events such as failure notification of software, performance management, security management, integration with other business software and historical analysis tools. These events can be generated through these common APIs, libraries and techniques.

In the case of blockchain, the use of offchains and oracles stands out for the management of events. Offchain transactions, which occur outside the chain, are won popularity due to its zero/low cost. Off-chain transactions offer many advantages: they can be executed instantly, they do not usually have a commission per transaction, since nothing happens within the blockchain, and they offer more security and anonymity to the participants, since the details are not transmitted publicly, which makes it impossible to partially ascertain the identity of a participant by studying the transaction patterns. Oracles offer an external service to the chain that is called to provide information from an external source, for example, a rate of change or the result of a mathematical calculation. Oracles are a safe bridge between smart contracts and real-world information sources.

Identity management is essential for the management of cryptographic private keys that are associated with a user's account. Blockchain clients often choose to offer local management of user credentials, such as system and wallet keys. These facilities can also be applied outside the scope of a client.

The security solution in this layer acquires relevance as it is composed of sensitive items. Policies should be implemented to prevent improper exploitation protecting that all transactions are legitimate and that asset management and identities is not exploited by adulterating assets.

3.5. Platform Layer

It is the core of the architecture and is responsible for the execution of the network logic; it contains the necessary elements for the publication of each block. In function of the implementation of this component, there is the possibility of creating and managing third-party part of cloud-based networks for construction companies of blockchain. The platform layer security solution aims to mitigate the damage that can be caused to a blockchain network by exploiting vulnerabilities identified, and protecting the digital assets contained in the chain. All the infrastructure of the blockchain platform can be understood as a Blockchain-as-a-Service (BaaS) that allows the creation and management by third parties of networks cloud-based for companies dedicated to building blockchain applications.

This is beginning to be a growing trend and is one of the main reasons to separate the platform layer from the service layer. The underlying idea is to get a function similar to that of a web host. That is, run the operation from the backend of an application.

Blockchain technology works in such a way that each block stores a number of valid registrations or transactions, information related to that block its link with the previous and next block through the hash of each block. Each block is linked to the previous block by means of a cryptographic hash. All transactions must be encrypted with public-key infrastructure (PKI) to prevent it from being compromised by unwanted parties. The multi-signature function will be available for sensitive transactions on the blockchain. The blocks also contain information regarding the smart contracts in which the clauses are collected and information about any physical contract in the form of a code and that must be fulfilled to publish a new block.

3.6. Network layer

The network layer is the foundation on which blockchain technology is built. Basically, blockchain networks are networks that overlay other networks; therefore they inherit the security and privacy issues of the underlying networks. The network layer is therefore, one of the bases on which this architecture is based, being crucial to have with security solutions that can cover network problems. The main services provided by the network layer in blockchain technology are peer-to-peer management and discovery, which are based on the operation of the underlying network, such as domain name resolution (DNS) or network routing (for example, LAN routing for IP, routing WAN as BGP). Network layer security issues are one of the research topics most popular in the field of blockchain security. Between the different attacks, Distributed Denial of Service (DDoS) attacks. Likewise, the attacks eclipses are also very popular. These attacks disable the connection of a network node with the rest of the nodes that are used by the attacker.

4.0 APPLICATION OF THE SRA

Volume: 05, Issue: 05 "September - October 2022"

ISSN 2582-0176

A real case has been used to analyze the applicability of the proposed architecture. We have used the case proposed by Sladic et al. where they present the implementation of a notary on the blockchain network that supports the transactions carried out in the Serbian cadastre. The system stores the legal link between the properties and their owners, as well as the cadastral map containing the geometric data and the topographic attributes of the soil. Figure below details the correlation of the case of study with the proposed architecture. For a better understanding of the proposed case, the elements that correlate with our architecture have been highlighted, leaving in gray those that are not used in the proposal. In the business layer, it is proposed to use a hybrid block chain that allows consultation of the cadastre by the population, but that guarantees that the property registries are always carried out by a notary. In this case, the business layer fully maps with the architecture proposed in this study.

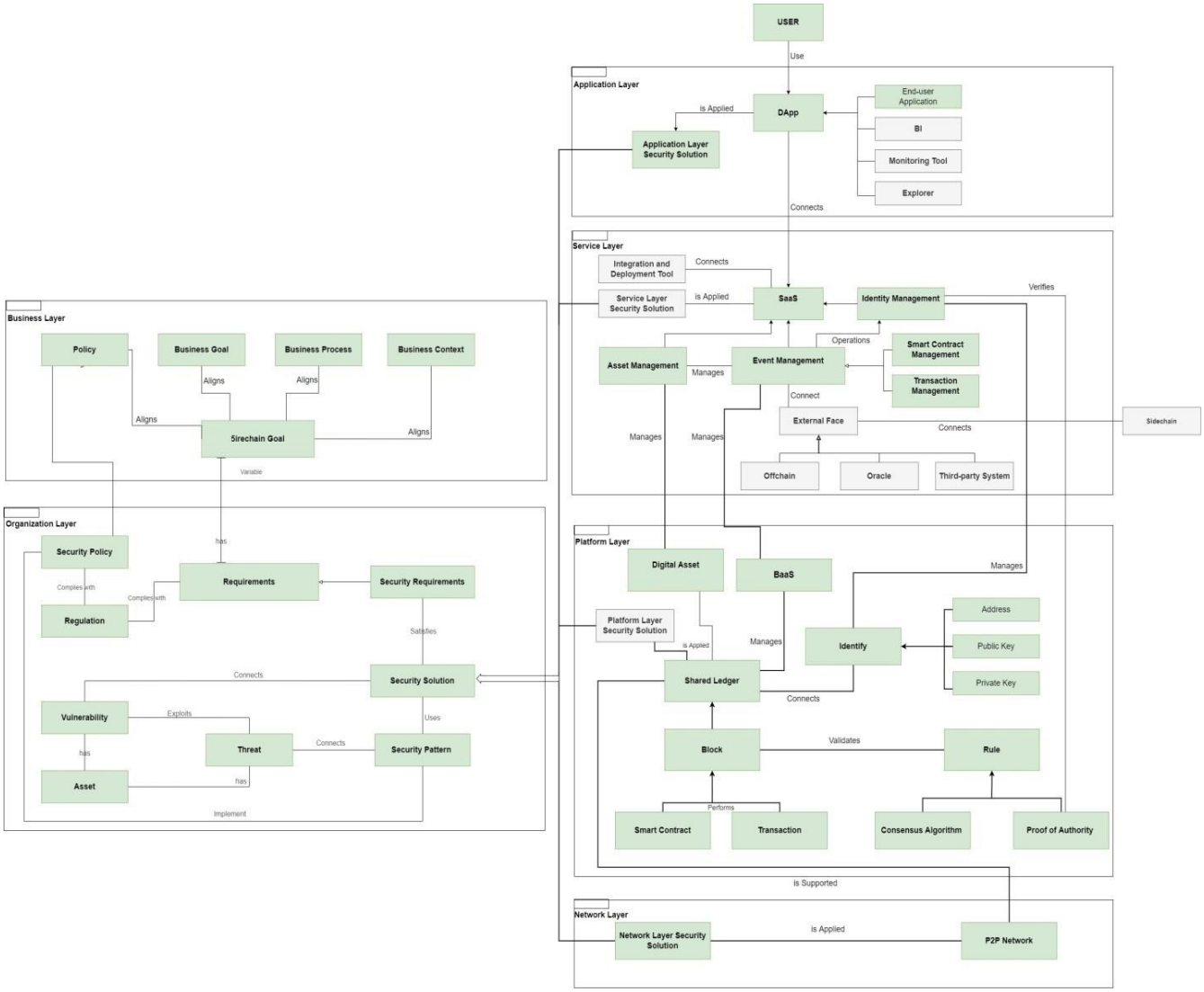

Figure: Architecture of the case proposed by Sladic et al.

Through the orchestration layer, we ensure compliance with one of the main system security requirements that all users are able to consult the data of the cadastre, but they can only be modified by the figure of a notary. To this end, it is proposed that users can only access using

Volume: 05, Issue: 05 "September - October 2022"

ISSN 2582-0176

their digital certificates, digital documents that link the key public of the user with the identity of this, and the certification authority that verified the content of the certificate. The use of digital certificates allows for controlling the risks of unwanted access is a widely used identification security pattern extended. On the other hand, the requirements of the chain must comply with the regulation that exists. In this sense, it must be governed by the Electronic Document Law, electronic identification, and trust services in electronic commerce.

Likewise, in the application layer, the cadastre information remains accessible for all users through a DApp consisting of a web front end that allows access to data stored on the chain. The DApp frontend uses a standard web for frontend development, i.e. HTML, CSS, and JavaScript to render a page and retrieve details directly from the backend. On the other hand, a second DApp is presented that allows notaries to store the keys hashes of documents during rights transfer activities. Despite that security measures are not specified for both DApps, they must be considered taking into account the technology used. The service layer is aimed at making the blockchain more accessible than it differs with the objective of the proposed architecture. The incorporation of elements of this layer will depend on whether it is intended to carry out an implementation-oriented to obtain multi- user shared services that save social resources and achieve a larger scale. The identity management component offers the possibility to centralize identity management since it is not expected that just anyone can generate transactions, but only a selected group of users. The identity manager contains the information related to the user since in the access controls they include the verification that the user can make changes.

The platform of the proposed system comprises alphanumeric data on rights of property, the holders of the rights and the attributes of the properties, like the surface; and geospatial data (cadastral map) as a result of the activities topographical. These data comprise our assets and may be subject to a transaction on the blockchain. The transaction constitutes an input of data that is stored in a block, belonging to the distributed ledger, and containing the transaction information, i.e. user ID, unique ID of a property, change number, type of change, and description of the change.

In addition, the transaction is completed with transaction details about the change that has occurred (change number, type of change, description, date, etc). The result of the execution is also stored in the block when performing a transaction. Finally, the chain of blocks contains the information of the users who have made the transaction. Users have two keys: a private key that only the user knows and a public key shared with the entire network. The user who made the change digitally signs the transaction with your private key. Once created, the transaction is inserted into a newly created block and after being verified by the network, the block is added to the chain. The architecture of this case study makes use of the P2P network to support the rest of the layers of architecture. At this point, there is no difference between the components of architecture and our MRS. As mentioned above, an SRA aims to offer architecture with a high level of abstraction that allows covering any implementation scenario in a blockchain system, applying the implementation of some or other components depending on the need of the blockchain chain itself. If we look at the ingredients proposed by Sladic it can therefore be concluded that the case is aligned with the SRA proposed in this document, allowing us to validate the applicability of the proposal.

Volume: 05, Issue: 05 "September - October 2022"

ISSN 2582-0176

5.0 CONCLUSION

In this work, an SRA has been presented that serves as a basis for the development of blockchain systems and integration security from the first phases of the life cycle of this technology. We have defined our SRA through UML diagrams, a widely accepted language that facilitates the understanding of the relationships between the different components. In addition, the use of UML has allowed us to precisely define the relationships between the different components and subcomponents. In this article, we studied an SRA sketch for 5irechain where the components of the blockchain are specified technology as well as the relationships between the different components and subcomponents. Finally, the applicability of our outline has been shown through the realization of a real example demonstrating how to fit effectively and incorporate all the necessary elements for the implementation of the system. In future work intends to carry out a complete case study that allows us to validate and refine our proposal.

5.1 Acknowledgment

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

REFERENCES

Abdallah, R., & Abdallah, R. (2022). A Blockchain-Based Methodology for Power Grid Control Systems. In The International Conference on Innovations in Computing Research (pp. 431- 443). Springer, Cham.

Avgeriou, P. (2003). Describing, instantiating and evaluating reference architecture: A case study. Enterprise Architecture Journal, 342, 1-24.

Biktimirov, M. R., Domashev, A. V., Cherkashin, P. A., & Shcherbakov, A. Y. (2017). Blockchain technology: Universal structure and requirements. Automatic Documentation and Mathematical Linguistics, 51(6), 235-238.

Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. Overview report The British Standards Institution (BSI), 40, 40.

Dumortier, J. (2017). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). In EU Regulation of E-Commerce. Edward Elgar Publishing.

Fernandez, E. B., Monge, R., & Hashizume, K. (2016). Building security reference architecture for cloud systems. Requirements Engineering, 21(2), 225-249.

Fernandez, E. B., Yoshioka, N., Washizaki, H., & Syed, M. H. (2016). Modeling and security in cloud ecosystems. Future Internet, 8(2), 13.

Haffke, L., Fromberger, M., & Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them. Journal of Banking Regulation, 21(2), 125-138.

Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29(2), e2060.

Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., & Szalachowski, P. (2020). The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. IEEE Communications Surveys & Tutorials, 23(1), 341-390.

Lie, X., Jiang, P., Chen, T., Xiapu, L., & Qiaoyan, W. (2017). A Survey on the Security of Blockchain Systems Future Generation Computer Systems.

Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: a review. Ieee Access, 6, 10179-10188.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

Nwaiwu, F. (2021). Digitalisation and sustainable energy transitions in Africa: assessing the impact of policy and regulatory environments on the energy sector in Nigeria and South Africa. Energy, Sustainability and Society, 11(1), 1-16.

Pankov, K. N. (2020, March). Testing, verification and validation of distributed ledger systems. In 2020 Systems of Signals Generating and Processing in the Field of on Board Communications (pp. 1-9). IEEE.

Pržulj, Đ., Radaković, N., Sladić, D., Radulović, A., & Govedarica, M. (2019). Domain model for cadastral systems with land use component. Survey review, 51(365), 135-146.

Raj, P. (2021). Industrial use cases at the cusp of the IoT and blockchain paradigms. In Advances in Computers (Vol. 121, pp. 355-385). Elsevier.

Ray, P. P., Das, B., & Das, A. (2021). IoT-Blockchain Integration: The Way Ahead. In Proceedings of International Conference on Computational Intelligence, Data Science and Cloud Computing (pp. 749-763). Springer, Singapore.

Schwalm, S., & Alamillo-Domingo, I. (2021). Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0. Wirtschaftsinformatik, 58, 247-270.

Sladić, G., Milosavljević, B., Nikolić, S., Sladić, D., & Radulović, A. (2021). A blockchain solution for securing real property transactions: a case study for Serbia. ISPRS International Journal of Geo-Information, 10(1), 35.

Sladić, G., Milosavljević, B., Nikolić, S., Sladić, D., & Radulović, A. (2021). A blockchain solution for securing real property transactions: a case study for Serbia. ISPRS International Journal of Geo-Information, 10(1), 35.

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. Ieee Access, 7, 22328-22370.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Nistir 8202 blockchain technology overview. National Institute of Standards and Technology, US Department of Commerce, Washington, USA.

Zaitsev, A. V., Gostev, S. S., Cherkashin, P. A., & Shcherbakov, A. Y. (2017). Regarding the technology of distributed storage of confidential information in centers of general-purpose data processing. Automatic Documentation and Mathematical Linguistics, 51(3), 117-119.

