Confidentiality-preserving,blockchain-based, and data sharing: a survey

Rania Znaki[1*], *Abderrahim* Maizate[1], and *Abdelaziz* Ettaoufik[2]

[1]RITM ESTC/CED ENSEM, Hassan II University, Casablanca, Morocco
[2]LTIM, FS Ben M'SIK, Hassan II University, Casablanca, Morocco

Abstract. Data sharing has gained tremendous attention in the past few years. Information being the driving power of all strategic decision-making changes as organizations aim to improve their efficiency by sharing insights within departments and collaborating with partners. However, protecting the confidentiality of sensitive information is still one of the biggest challenges when sharing these valuable assets between differ partakers. Blockchain has been one of the technologies that are being explored to solve this problem. Blockchain technology had been renowned as a means of secure asset tracking, provide immutable transaction sharing and had been proven to limit the amount of trust collaborating parties needed to exchange sensitive data. In this paper, we hover the up-to-date, relevant techniques and propositions with regards to confidential data sharing using blockchain related approaches. We will provide a comprehensive comparison between different techniques based on the widely used frameworks and technical schemes summoned and cite the challenges blockchain based applications face in the realm of confidentiality preserving data sharing.

1 Introduction

Data sharing creates functional wisdom to improve the efficiency of processes, yet challenged by lack a of trust, security of information and the ability to securely collaborate is the hot topic that transcends the concerns of pivotal organizations, to which trading confidentiality of information for any level of process improvement is inconceivable, counting healthcare institutions [1–3], transportations [2–4], smart city facilities,[5–7] Internet Of Things, eventually what applies to industry [8–10] and management policies-oriented systems, like insurance [11]. Challenges to these sensitive verticals had shifted towards creating effective and scalable data sharing models that can adapt to the stringent measures for confidentiality, for the reasons data is commended for. Thus, the provisional flood of information expected by the deployment of large scale IoT, huge data polls, big data, rises concern about the efficiency of traditional data sharing methods, either being too complex, slow, hard to scale, or need interference of a third party.

Blockchain contributes with core supporting technologies counting smart contract[12], advanced encryption and tamper resistant ledger to providing an attractive solution to secure data sharing. However, Blockchain is largely mistaken for being a confidential-by-design

* Corresponding author: rania.znaki.doc20@ensem.com

ledger. Realistically, blockchain is designed for transparency, and suffers poor ability to perform real confidentiality. In this paper, we will establish a patterned survey on the different approaches' designers have used to exploit blockchain for confidential data sharing. We will proceed to define confidentiality, break down the structural assets of the solutions represented in the literature, and share critical insights from gathered observations. The motivation behind this survey is to bring an updated, comprehensive, and cross-vertical review of the literature exclusive to the confidentiality of data sharing, complementing the existing surveys that treated privacy preserving schemes, and condensing a general review on the trends and challenges scattered amongst different databases, to assess the maturity of blockchain in concern of secure data sharing, prompting us to frame our review around the following interrogations:

Q1: What techniques are of prominent use securing the exchange of confidential data?

Q2: How do types of blockchain schemes handle confidentiality amid sharing data?

Q3: Is there common factors to evaluate the robustness of the confidentiality preserving techniques using to secure data sharing in blockchain?

To elaborate this survey, we exported different survey articles and research papers published on Science Direct, Springer, MDPI journals, IEEE Explore, Wiley and different Google Scholar cited journals, that identified the usage of blockchain related technologies for the purpose of confidential data sharing. We identified the necessary keywords to search and access the adequacy of different papers' content and topics as follows: blockchain, security, data sharing, data transfer, confidentiality, privacy. Some studies where secure data sharing had been mentioned, but no clear evidence of confidentiality assessment had been conducted, were eliminated from the pool. We used snowballing for articles mentioning definitions of concepts contained in the preliminaries.

This survey is structured as follows: section 2 will treat different related works available in the literature. Section 3 will lay out the background information framing the content of the survey. In section 4, we will address a comprehensive and commented review of the literature about confidential data sharing using blockchain, with the different and most spread frameworks. In the section 5 we point the highlights of our conducted literature review, with comparisons and challenges, and finally we will sum it up with a conclusion.

2 Related works

Scraping for existing surveys, we noticed the subject of confidentiality was treated under the term of privacy. Our work makes distinction by defining confidentiality as protecting the secrecy of data, and privacy as preserving the identity of the issuers. Materials in existing surveys remain relevant to our work. Review articles of the same thematic had been issued per vertical [13] suggesting a comprehensive and detailed review around access control. Another industry where blockchain is proliferating is healthcare, around which[14] discussed the use of permissionless blockchain and pointed the importance and challenges in the segmentation of the partakers. Authors in [15] reviewed in globality the application of blockchain for secure information sharing in healthcare, its interaction with ecosystem devices, algorithms and discussed potential challenges. Supply chain exploits blockchain for its fair share of trust enhancing mechanisms. [16] reviewed the existing facilitators of information sharing, established how blockchain enables partnership by ensuring verified access information is regulated by multiple stakeholders, and brought the lack of process comprehension and conflicts of interests as cause of impediment. More general surveys had been issued, analysing the privacy protection aptitude and pertaining threats blockchain comes with [17,18]. It had also been introduced as promising to merge with IoT in articles like [19] that reviewed its applications and perspectives on data sharing. Similar view point

can be read on [20] bringing the lack of advanced and secure information management and data sharing mechanisms as a critical drawback to smart manufacturing, and blockchain as a solution. Finally, [21] reviewed in entirety smart contract data sharing, compared existing survey, and addressed blockchain as a trustworthy medium for data sharing, flagging the need for cryptographic techniques like homomorphic encryption, and clustered trusted executed environments, in contrast with the growing demand for transparency.

3 Preliminaries

3.1 Background on blockchain

Blockchain is a distributed database allowing multiple authorized parties to reliably exchange assets without resorting to trust. Blockchain was first introduced with Bitcoin [22] and assigned a set of supporting technologies counting smart contracts[12]. Each node maintains a copy of the transaction history, that is systematically updated after consensus is reached in form of attached blocks as displayed in Fig.1. The ledger's data cannot be altered or deleted. Each node receives an update from other previously authenticated nodes, allowing security and reliability for data exchanged. There had been multiples proof of concepts using and blockchain had notably been an interesting tool to secure exchanges. Blockchain became the chosen topic for collaborating entities as well, replacing records managed through consolidated repository systems or centralized databases.

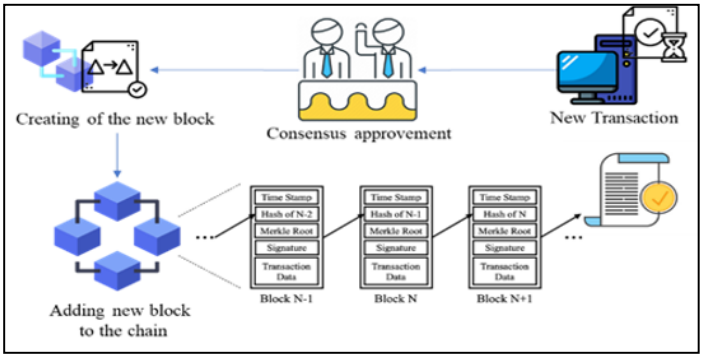

Fig. 1. New block creation and integration in blockchain workflow.

3.2 Confidentiality in Blockchain

Confidentiality represents one of the pillars of Information Assurance according to the NIST (National Institute of Standard and Technology) of the US Department of Commerce, and one of the four pillars of IT security according to ENISA (European Union Agency for Cybersecurity). Described in ISO/IEC 13335-1:200 as "The degree to which data has attributes that ensure that it is only accessible and interpretable by authorized users in a specific context of use." Confidentiality forcibly entangles with other security aspects such as privacy, since confidentiality addresses the secrecy of the traded data, and where privacy concerns protecting the user's identity. Additionally, the more restricted the ledger, the more confidentiality it provides: Private blockchain structures such as are the most demanded for confidentiality. Two out of four categories of blockchain answer this need, permissionless private, generally used in collaboration between multiple organizations, and permissioned private, applied when access to data should be internally monitored via structured access

authorization entity or process. In public and permissionless blockchains, confidential data is usually pre-processed by encryption or access restricting the access with authentication.

4 Literature review

4.1 Smart contracts for confidential data sharing

Records on the blockchain are immutable, through consensus protocols making data resistant to tempering due to heavy computational overload [23]. However, a prominent approach the literature is creating confidentiality and privacy driven smart contracts [6]. Solutions that had been introduced in this context combine smart contracts with homomorphic encryption,[24] or zero-knowledge proof [3], [22], adjusting smart contract for secure sharing. The authors of [2] merged blockchain and AI in order to serve both purposes of secure sharing and computing, using smart contracts to automate the generation of parameters for data sharing authorization, where smart contract tracks and collects data. On the same wedge, [26] proposed a scheme based on proxy-encryption they claimed the first one able to implement efficiently a free proxy re-encryption scheme in combination with smart contracts to enable a fast and secure storage and transfer of IoT data flow, eliminating third. In other instance, [27] suggest a digital solution for outbreak containment that calls a private-permissioned blockchain based distributed application using smart contracts, the authors trigger for shortcomings such as local key storage, and lack of scalability.

4.2 Encryption, Signcryption and Proxy Re-encryption

Signcrytion enables the process of transactions to occur securely between participants over the network. It is also used as proof of identity and authority, allowing a user account to be digitally signed, including on blockchain [28,29]. The infamous symmetric key encryption is used to secure smart contract's data in various blockchain structures. However, the encryption keys are subject to numerous threats, leading to efforts targeting their enhancement, obfuscation as an example [30], the concept consists on turning the smart contract containing the private key into a black box, cancelling attempt of reverse engineering, allowing secret data inside publicly running smart contract with ease of mind.

A huge portion of the immutability of the ledger relies on the computational complexity of these cryptosystems, that comes down to the resolution of discrete logarithm problem. The use of Elliptic Curve Cryptography had also been also noticed in[31] where authors used ECC to encrypt their data to enforce confidentiality of their transaction system mitigating DDoS vulnerabilities.[32] as well-made use of ECC digital signature to provide a confidentiality-privacy centred big data scheme. [11] using attribute based centralised system with blockchain based token generation, maintaining privacy in individual patient records. Another approach is Blockchain-Based Signcryption proposed by [33] to secure data partaking from and towards the Cloud. This approached was tested to solidify access policies and enforce data unforgeability. Authors on [28] proposed a blockchain based secure data sharing platform with fine-grained access control (BSDS-FA). The approach introduces a new hierarchical attribute-based encryption algorithm (HABE), providing users with secure data sharing services, it showed progressing results in resolving leakage.

Proxy Re-Encryption and Threshold proxy re-encryption[34] are prominent in the literature. They allow stakeholders owning access to an encrypted message to share it without revealing the plaintext to any other party. The workflow of this technology allows the proxy to transform the cyphertext encrypted under a certain public key into a different cyphertext that can be decrypted by another cyphertext as illustrated in Fig.2. This technique had been

most useful to the users of public cloud services for their data storage[10,34,35]. This process is essential for companies that are reluctant to share their private keys with third-party service providers or auditors to prevent potential loss of sensitive information.

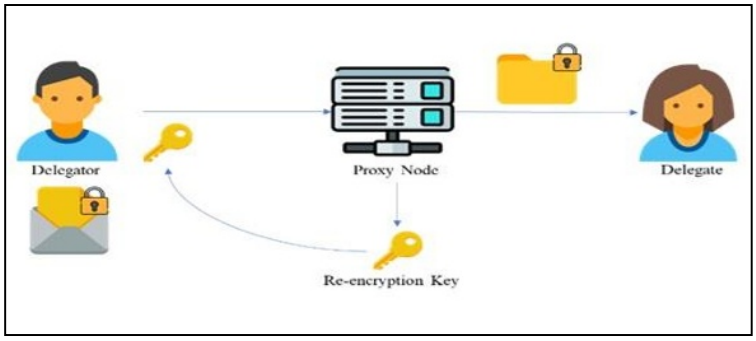

Fig. 2. Two-nodes proxy re-encryption simplified workflow.

These schemes raise however the question of trust, cost, and scalability. In their proposition, tackling these issues,[26] called for a certificate-based proxy re-encryption scheme, combined with runtime dynamic smart contracts linking sensor and data consumer, providing a secure and confidential data transfer over a third-party cloud provider in possession of the encrypted data. Blockchain takes parts mainly in securing the management of the financial transaction, executed automatically through the smart contracts, using of- the-shelf IoT sensors. IoT systems display yet another problem: open wireless transmission media being a prominent point of failure that [10] answered by creating an Ant Colony optimization improved WSN transmission method, followed by threshold proxy-re encryption. Another paper [35] targets private data sharing by combining Proxy re-encryption and identity based encryption using the edge devices as proxies. The security of the model is based on the adversary's inability to tell apart the proxy node identity.

However, [34] points out that single proxy suffer performance bottlenecks, as well as representing a serious point of failure when facing DoS attacks. Herein solution combines the threshold proxy re-encryption approach to the blockchain's consensus algorithm, for an improved ciphertext conversion security process, it splits trust by delegating re-encryption to multiple proxy nodes, therefore absorbing unauthorized conversion of ciphertexts. Authors of [36] observed the privacy of electronic health records up close and pointed the consistent problem of information leakage risks in outsourced EHRs. They introduced a proxy re-encryption management scheme consisting of an independent proxy server, associated to an access control assisted by blockchain. Another research mitigating EMR's sharing in the era of 5G is proposed by[37]. Attacking the problem of database storage by introducing consortium blockchain, attribute-based access control, and the safe transmission enabled by proxy re-encryption. Another perspective of use in [38], is denying access to the asset rights for the agent in charge of selling them unless the ciphertext access policy is fulfilled. The scheme is designed with two chains, the fair trade of decryption keys required in this scheme is performed by Ethereum smart contracts, whereas another blockchain is exploited for digital rights related information storage to overcome the overhead encountered upon storing on public blockchains [25].

4.3 Zero knowledge proofs

Using zero-knowledge proofs allow for highly sophisticated smart contracts designs that operate needless to reveal sensitive information about the contract's execution [3,25,32].These allow computation to be carried out while maintaining privacy of involved

data. There are two notable classes of zero knowledge proofs, the interactive ones, whereby the verifier challenges the prover on a mathematical puzzle, and the non-interactive. Those come in action usually to replace authentication methods, allowing more confidentiality on public blockchains. A similar solution had been the use of aggregation [8,30] allowing multiple transactions to be combined, hiding the identity of the individual transactions and limiting the scope of view of different parties. Using said techniques improves the privacy of smart contracts while maintaining integrity against malicious actors.

4.4 Decentralized storage

Storage had been a recurring hold back to adopting blockchain for data sharing, since they resort to third party storage, either by announcing the cost of in-chain storage as a constraint to creating viable scalable mechanisms, or with the useful argument of the right in the forgettability, which is the case in [39], only storing hash values on blockchain and delegating the rest to private databases, thus allowing to delete the data to comply with the right to be forgotten.

A breakthrough in the field was the creation of decentralized storage platforms. The most popular in the literature being IPFS[9] a peer-to-peer hypermedia protocol that allows users to store and share information across a decentralized network of computers commonly known as a "distributed file system". IPFS is the to-go solution for off-chain data storage for many approaches, naming [9,40] leveraging more confidentiality. The vulnerability of these systems remains the insider's attack, that was solved in some architectures with Multi-party Authorization [41] by managing the access to shared resources by inquiring multiple keys.

4.5 Identification, identity, and access management

Advanced authentication and identity management [29] is one of the historical pillars of confidentiality. Blockchain combined with AI [10] were used to prevent data leakage and reducing risks with behavioural analysis, detecting fraudulent nodes. Another paradigm is decentralized identification [42], a combination of blockchain technology with self-sovereign identity, permitting users to maintain control over their personal information without needing a central authority for verification. Unlike traditional identity management systems, it provides greater privacy and reduces risks of data breaches with identity data no longer stored in a centralized database. Another way of preventing potential unauthorised usage of confidential data is limiting unauthorised access. Numerous access control mechanisms had been implemented in connivence with smart contracts to prevent data theft, especially ciphertext based attribute-based access control, actively used in literature, where the access policy abstracts the roles and identities formulated into Boolean formulas of attributes set by regulating agencies, for a dynamic and fine-grained access control [43]. Other types of access control had been mentioned, such as role-based access control [44] and organization-based access control [45]. The main drawback to this technique is the non-flexibility of the granted access, usually raised by attribute change. Some such in [46] propose timely revocable access to data in the cloud with a changeable update factor to the cipher.

4.6 Blockchain frameworks for data sharing

4.6.1 Hyperledger fabric

Hyperledger Fabric is an open-source framework that was created in 2015 by members of the Linux Foundation and the IBM Watson group for the development of enterprise-grade

blockchain technology operable by different companies in the supply chain and financial services industry[47]. Organizations use Hyperledger Fabric to build secure blockchain-based networks through which they share information in a secure and encrypted manner and make decisions without risking sharing data with their competitors. Another benefit Hyperledger Fabric is the easy integration with existing IT operation [49]. Hyperledger Fabric supports multiple versions of consensus algorithms, each use different voting mechanisms to ensure that no single entity can cheat the other nodes[47].

4.6.2 Ethereum

Ethereum is an open-source software based distributed system that supports smart contracts, being conditional, automatically executable digital agreements that can be used to process payments, execute compromises, and manage assets. This feature is used to create decentralized applications (DApps) that can interact and operate without the involvement of a central authority or third party. When an organization desires to share information with another business or entity, it could establish an Ethereum-based smart contract for the two parties to mutually transfer sensitive data in a secure manner [38,50]. However, smart contracts are vulnerable, entailed by coding irregularities that had been detailed by authors of [51].

4.6.3 Consortium blockchain

To reduce the cost of sharing data between enterprises, groups of companies can set up a consortium blockchain, upholding a record of every transaction and sharing without the need of a third party auditor.[4,53]. Running on a consortium blockchain can provide a high level of security for the users compared to DApps running on public blockchains. As an example [52] proposed a scheme to overcome the need of third-party auditors. Many secure and efficient data sharing schemes based on consortium blockchain had been proposed for smart industrial environments,[3] where the goal was to create a comprehensive and efficient sharing scheme that relay on Hyperledger Fabric for an efficient data sharing. On another hand [4] proposes an algorithm that can effectively control access permission and secure the exchanges in the vehicular ad-hoc network, with consortium blockchain and ciphertext-policy attribute-based proxy re-encryption, exhibiting great improvement in data sharing confidentiality, alongside optimal computing overhead and a reasonable resistance to collision attacks. Another approach of using consortium in the medical field is presented in [1], suggesting a design for secure medical data sharing scheme, that is based on blockchain and cloud computing where key management is insured by consortium. To prove the security of this architecture, authors applied the BAN logic analysis.

5 Comparisons, pitfalls, and security challenges

Throughout our review of literature, we noticed a patterned use of Ethereum and Hyperledger Fabric for data sharing schemes, mainly for being manoeuvrable along with the powerful smart contract/chain code engine, making a generic platform for a wide range of applications.

However, in the case of Ethereum, the consensus mechanism consumes a lot of energy, reducing the efficiency of data sharing. In Ethereum, miners use the algorithm of Ethash to generate their hashes whilst Hyperledger Fabric uses SHA-3, both are resource intensive, but it takes longer to mine a block in Ethereum than it does in Hyperledger, proving its efficiency when challenged in the same environment.

Most of the studies we reviewed above, experienced drop in performance and enlarged delays as the number of collaborative pears increases. Solutions that involve multiple chains tended to have a similar behaviour but with slightly more performance[5].

Blockchain solutions that are enhanced with complex access control mechanisms experience significant delay increase, especially the ones that are Attribute Based, Proxy re-encryption also increases the average time to share encrypted data, and is reported in some cases to increases delay by 60% due to mining of re-encryption keys [38]. Storage overhead is a problem that must be considered in any distrusted computing scheme[1].

Therefore, in the expense of efficiency, blockchain risk vectors are sometimes overlooked. Blockchain is suffering the rise of computational costs contiguous with the level of required security. This encourages more research work upon new cryptographic schemes that may combine effectiveness and lightweight. Many flaws still compromise the confidentiality of users' private data transitioning thought the chain, and some of notable confidentiality vulnerabilities in blockchain are identity theft via Man-In-The-Middle, widespread endpoint attacks, sybil attacks and 51% attack, consensus hijacking, DDoS attacks and forking. Although private chains offer the advantage of higher transaction speeds and greater security compared to public blockchains, they are unsustainable for large scaling, and vulnerable to Sybil attacks (where multiple fake identities are created on the network to carry out fraudulent activities). Forking attacks are also a threat to public blockchains and can lead to the loss of millions of dollars in funds if the coin of the forked chain spreads [51].

A source of scepticism in the literature are proposals that relayed upon encryption schemes, not detailing the process of securing digital assets of private keys. Physical separation of the file is a necessity to avoid Certificate Authority from provide adversaries with forged usable public keys. Re-encryption and identity-based authentication reduce these risks, but do not eliminate the threat completely. Data forgery attacks are also difficult to track, with a few studies focusing on detecting fraudulent nodes, tackling the issue with behavioural analysis upon the advances of artificial intelligence [54]. However, no definitive way ensures data has not been falsified beforehand based on the history of the hash.

A crucial limitation had been raised by [55] debating the confidentiality provided by schemes that relay on cloud storage. Since part of valuable data are stored off-chain within the total control of a third party, whereas users often only keep their metadata or hash of data in chain, while the rest is delegated, including sometimes passwords and encryption keys.

The proliferation of quantum computing is also an alarming countdown to the efficiency of great numbers of powerful cryptosystems, since their resiliency had been tested against attack conducted by classical computers [56], compromising the security level of most common symmetric and asymmetric cryptosystems [57]. In parallel, blockchain is pushing in the way of using quantum computing attributes to solidify blockchain-based security solutions by the means of Quantum inspired blockchain frameworks[58].

Finally, the lack of a framework or regulatory rules for blockchain that are centred around data confidentiality preserving data sharing leaves room for research, where novel architectures like Hybridchain[59] built and tested to fit confidential data sharing, but also take in consideration computational complexity, are rare in the literature.

6 Conclusion and perspectives

This study aimed to investigate research advent concerning blockchain based solutions for secure sharing of confidential data, by exploring the different solutions and challenges that these approaches stumble upon. A major challenge to this review was the lack of a unified testing process in the literature: the different solutions are tested according to different parameters and applying different criteria, thus the need of creating a framework or protocol that could be able to assess the capacity of blockchain based models to handle confidential

data sharing. We can add that new advances and horizons are currently explored with the rise of quantum computing, thus the need of experimenting tailored, up to date cryptosystems that could adapt blockchain to confidential data sharing, in perspective of IoT democratization.

References

1. X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, J Med Syst **44**, 52 (2020)
2. R. Kumar, W. Wang, J. Kumar, T. Yang, A. Khan, W. Ali, and I. Ali, Computerized Medical Imaging and Graphics **87**, 101812 (2021)
3. H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, Computers & Security **99**, 102010 (2020)
4. D. Wang and X. Zhang, IEEE Access **8**, 56045 (2020)
5. I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, Computers & Security **88**, 101653 (2020)
6. A. Qashlan, P. Nanda, X. He, and M. Mohanty, IEEE Access **9**, 103651 (2021)
7. N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, and P. N. Pathirana, Future Generation Computer Systems **131**, 209 (2022)
8. A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, and Z. Mushtaq, IEEE Access **10**, 11404 (2022)
9. S. Muralidharan and H. Ko, in *2019 IEEE International Conference on Consumer Electronics (ICCE)* (IEEE, Las Vegas, NV, USA, 2019), pp. 1–2
10. J. Liu, Z. Liu, C. Sun, and J. Zhuang, Journal of Artificial Intelligence and Technology **2**, 23 (2022)
11. A. Mubarakali, Mobile Netw Appl **25**, 1330 (2020)
12. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, IEEE Transactions on Systems, Man, and Cybernetics: Systems **49**, 2266 (2019)
13. L. Golightly, P. Modesti, R. Garcia, and V. Chang, Cyber Security and Applications 100015 (2023)
14. H. Jin, Y. Luo, P. Li, and J. Mathew, IEEE Access **7**, 61656 (2019)
15. P. Xi, X. Zhang, L. Wang, W. Liu, and S. Peng, Applied Sciences **12**, 7912 (2022)
16. P. K. Wan, L. Huang, and H. Holtskog, IEEE Access **8**, 49645 (2020)
17. Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, Journal of Network and Computer Applications **126**, 45 (2019)
18. L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, Digital Communications and Networks **7**, 295 (2021)
19. S. Mathur, A. Kalla, G. Gür, M. K. Bohra, and M. Liyanage, Computer Networks **227**, 109726 (2023)
20. X. Guo, G. Zhang, and Y. Zhang, Sensors **23**, 155 (2023)
21. L. T. Nguyen, L. D. Nguyen, T. Hoang, D. Bandara, Q. Wang, Q. Lu, X. Xu, L. Zhu, P. Popovski, and S. Chen, (2023)
22. S. Nakamoto, (n.d.)
23. M. Shen, L. Zhu, and K. Xu, in *Blockchain: Empowering Secure Data Sharing*, edited by M. Shen, L. Zhu, and K. Xu (Springer, Singapore, 2020), pp. 15–27
24. D. P. Hellwig and A. Huchzermeier, in *Innovative Technology at the Interface of Finance and Operations: Volume II*, edited by V. Babich, J. R. Birge, and G. Hilary (Springer International Publishing, Cham, 2022), pp. 31–49
25. B. Sharma, R. Halder, and J. Singh, in *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)* (2020), pp. 1–6

26. A. Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila, and M. Liyanage, Journal of Network and Computer Applications **176**, 102917 (2021)
27. S. Saleh and F. Shayor, Frontiers in Blockchain **3**, (2020)
28. H. Xu, Q. He, X. Li, B. Jiang, and K. Qin, IEEE Access **8**, 87552 (2020)
29. S. Wang, H. Li, J. Chen, J. Wang, and Y. Deng, Journal of Information Security and Applications **66**, 103134 (2022)
30. M. Raikwar, D. Gligoroski, and K. Kralevska, IEEE Access **7**, 148550 (2019)
31. J. R. Shaikh and G. Iliev, in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)* (2018), pp. 155–158
32. H. Ghayvat, S. Pandya, P. Bhattacharya, M. Zuhair, M. Rashid, S. Hakak, and K. Dev, IEEE Journal of Biomedical and Health Informatics **26**, 1937 (2022)
33. N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, Journal of Systems Architecture **102**, 101653 (2020)
34. Y. Chen, B. Hu, H. Yu, Z. Duan, and J. Huang, Electronics **10**, 2359 (2021)
35. K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, IEEE Systems Journal **16**, 1685 (2022)
36. Y.-H. Park, Y. Kim, S.-O. Lee, and K. Ko, Applied Sciences **11**, 9422 (2021)
37. W. Chen, S. Zhu, J. Li, J. Wu, C.-L. Chen, and Y.-Y. Deng, Sensors **21**, 7765 (2021)
38. J. Gao, H. Yu, X. Zhu, and X. Li, IEEE Systems Journal **15**, 5233 (2021)
39. E. Balistri, F. Casellato, C. Giannelli, and C. Stefanelli, ICT Express **7**, 308 (2021)
40. S. Athanere and R. Thakur, Journal of King Saud University - Computer and Information Sciences **34**, 1523 (2022)
41. A. A. Battah, M. M. Madine, H. Alzaabi, I. Yaqoob, K. Salah, and R. Jayaraman, IEEE Access **8**, 196813 (2020)
42. E. S. Babu, A. Barthwal, and R. Kaluri, Computer Communications **199**, 10 (2023)
43. S. Ding, J. Cao, C. Li, K. Fan, and H. Li, IEEE Access **7**, 38431 (2019)
44. J. P. Cruz, Y. Kaji, and N. Yanai, IEEE Access **6**, 12240 (2018)
45. R. Saha, G. Kumar, M. Conti, T. Devgun, T. Kim, M. Alazab, and R. Thomas, IEEE Transactions on Industrial Informatics **18**, 3452 (2022)
46. Z. Zhang, J. Zhang, S. Kang, and Z. Li, in *Communications, Signal Processing, and Systems*, edited by Q. Liang, W. Wang, X. Liu, Z. Na, and B. Zhang (Springer Nature, Singapore, 2023), pp. 190–197
47. E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, in *Proceedings of the Thirteenth EuroSys Conference* (2018), pp. 1–15
48. J. Song, Y. Yang, J. Mei, G. Zhou, W. Qiu, Y. Wang, L. Xu, Y. Liu, J. Jiang, Z. Chu, W. Tan, and Z. Lin, Energies **15**, 2570 (2022)
49. G. Al-Sumaidaee, R. Alkhudary, Z. Zilic, and A. Swidan, Information Processing & Management **60**, 103160 (2023)
50. D. Lee and M. Song, IEEE Access **9**, 158122 (2021)
51. Z. A. Khan and A. S. Namin, (2020)
52. H. Huang, X. Chen, and J. Wang, Sci. China Inf. Sci. **63**, 130101 (2019)
53. M. Firdaus and K.-H. Rhee, Applied Sciences **11**, 414 (2021)
54. M. Gawas, H. Patil, and S. S. Govekar, Peer-to-Peer Netw. Appl. **14**, 2840 (2021)
55. X. Li, L. Ge, J. Chen, and Z. Peng, Journal of Systems Architecture **131**, 102702 (2022)
56. C. Easttom, in *Modern Cryptography: Applied Mathematics for Encryption and Information Security*, edited by W. Easttom (Springer International Publishing, Cham, 2022), pp. 397–407

57. T. M. Fernández-Caramès and P. Fraga-Lamas, IEEE Access **8**, 21091 (2020)
58. A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, Information Processing & Management **58**, 102549 (2021)
59. Y. Wang, J. Li, S. Zhao, and F. Yu, IEEE Access **8**, 190652 (2020)