International Journal of Social Sciences and Management Review

Volume: 05, Issue: 04 "July - August 2022"

ISSN 2582-0176

TECHNIQUES AND RESEARCH DIRECTION OF 5IRECHAIN SECURITY AND PRIVACY

VILMA MATTILA, PRATIK GAURI, PRATEEK DWIVEDI, DHANRAJ DADHICH & MD AHBAB

5ire (Sustainable Distributed Computing) Dubai Silicon Oasis,
United Arab Emirates Orcid ID: 0000-0002-1995-8185

https://doi.org/10.37602/IJSSMR.2022.5415

ABSTRACT

With the growing interest in blockchain in both academic research and industry, the security and privacy of blockchains have attracted huge interest, even though only a small part of the blockchain platforms can achieve the set of abovementioned security goals in practice. Leveraging from the state-of-the-art security paradigms, we propose 5irechain protective covering which has the ability to continuously identify, map, scan, assess, and grade the risk portfolio of all the assets, vendors, and acquisitions of a company giving a hackers perspective to the company. The dashboard gives visibility of not just only the web2 infrastructure in place, but also covers the web3 space and allows 5ire to monitor all of its nodes and their activities including historical data, tracking large wallets, monitoring bot activity, detecting transaction stats and volume along with the ability to block possible large scale attacks.

Keywords: 5irechain; Data Security; Blockchain Solutions; web3

1.0 INTRODUCTION

We argue that an in-depth understanding of the security and privacy properties of blockchain plays a critical role in enhancing the degree of trust that blockchain may provide and in developing technological innovation on robust defense techniques and countermeasures. 5ire team is always sincere regarding the security issues.

Security issues in blockchain continue to impose a significant challenge. Blockchain systems have suffered many outside attacks around the Internet. It is, therefore, necessary to study how and to what extent blockchain security issues have been addressed.

Table 1: An overview of the implementation security of a typical blockchain

Scenarios	*Goals*	*Issues*	*Countermeasures*
Internet of Things	Full autonomy capability on processing and exchanging data without human intervention	TPS, privacy violation, denial-of-service, network disruption	Robust identification and authentication of devices

Volume: 05, Issue: 04 "July - August 2022"

ISSN 2582-0176

Shared economy	Enforce the agreement between demanders and suppliers of services without any trusted party	Leak privacy of involved parties	Zero-knowledge proof
Electronic medical system	Deal with the security and privacy issue in the electronic medical system	Interconnect multi-organization	Sidechain
Smart city	Provide better services to its citizens while ensuring optimal utilization of resources	Digital disruption	Fraud detection & robust consensus
Smart grid	Solve the trustworthiness issue of decentralized energy exchanges	Privacy protection of trading data	Zero-knowledge proof
Social manufacturing	Endow intelligence to every entity on the manufacturing network	Bonding the physical and cyber world	Digital twin technology

2.0 METHODS THAT ARE LEVERAGED TO ENHANCE THE SECURITY OF 5IRECHAIN SYSTEMS

In this section, we provide a detailed discussion on a selection of techniques that can be leveraged to enhance the security and privacy of 5irechain systems.

Homomorphic Encryption (HE): Homomorphic encryption (HE) is powerful cryptography. It can perform certain types of computations directly on ciphertext, and ensure that the operations performed on the encrypted data, when decrypting the computed results, will generate identical results to those performed by the same operations on the plaintext. There are several partially homomorphic crypto- systems as well as fully homomorphic systems. One can use homomorphic encryption techniques to store data over the blockchain with no significant changes in the blockchain properties. This ensures that the data on the blockchain will be encrypted, addressing the privacy concerns associated with public blockchains. The use of the homomorphic encryption technique offers privacy protection and allows ready access to encrypted data over public blockchain for auditing and other purposes, such as managing employee expenses.

Zero-Knowledge (NIZK) Proof: Another cryptographic technology that has powerful privacy-preserving properties is zero-knowledge proofs, proposed in the early 1980s. The basic idea is that a formal proof can be formulated to verify that a program executed with some input privately known by the user can produce some publicly open output with no disclosure of any other information. In other words, a certifier can prove to a verifier that some assertion is accurate without providing any useful information to the verifier.

The Trusted Execution Environment (TEE) Based Smart Contracts: An execution environment is called TEE if it provides a completely isolated environment for application

execution, which effectively prevents other software applications and operating system(s) from tampering with and learning the state of the application running in it. 5irechain can utilize TEE in its current version to allow users to create privacy-preserving smart contracts using a decentralized credit scoring algorithm. Multiple factors are weighted for credit scoring, such as the number and types of accounts, payment history, and credit utilization.

Attribute-Based Encryption (ABE): Attribute-based encryption (ABE) is a cryptographic method, in which attributes are the defining and regulating factors for the ciphertext encrypted using the secret key of a user. One can decrypt the encrypted data using the user's secrete key if her attributes are agreed with the attributes of the ciphertext. The collision resistance is an important security property of ABE. It ensures that when a malicious user colludes with other users, he cannot access other data except the data that he can decrypt with his private key. The concept of attribute-based encryption was proposed in 2005 by a single authority. Since then, a number of extensions have been proposed to the baseline ABE, including ABE with multiple authorities to generate users’ private keys jointly, and ABE schemes that support arbitrary predicates.

Secure Multi-Party Computation: The multi-party computation (MPC) model defines a multi-party protocol to allow them to carry out some computation jointly over their private data inputs without violating their input privacy, such that an adversary learns nothing about the input of an authentic party but the output of the joint computation. In recent years, MPC has been used in blockchain systems to protect users’ privacy.

Anonymous Signatures: Digital signature technology was developed in several variants. Some signature schemes themselves have the ability to provide anonymity for the signer. We call this kind of signature scheme an anonymous signature. Among the anonymous signature schemes, group signature and ring signature were proposed earlier and are the two most important and typical anonymous signature schemes.

Group Signature: Group signature is a cryptography scheme proposed initially in 1991. Given a group, any of its members can sign a message for the entire group anonymously by using her personal secret key, and any member with the group’s public key can check and validate the generated signature and confirm that the signature of some group member is used to sign the message. The process of signature verification reveals nothing about the true identity of the signer except the membership of the group. Group signature has a group manager who manages adding group members, handling the event of disputes, including revealing the original signer.

Ring Signature: A ring signature also can achieve anonymity through signing by any member of a group of users. The term “ring signature" originates from the signature algorithm that uses the ring-like structure. The ring signature is anonymous if it is difficult to determine which member of the group uses his/her key to sign the message. Ring signatures differ from group signatures in two principal ways: First, in a ring signature scheme, the real identity of the signer cannot be revealed in the event of a dispute, since there is no group manager in the ring signature. Second, any users can group a “ring" by themselves without additional setup. Thus, the ring signature is applicable to the public blockchain.

Mixing: Bitcoin's blockchain does not guarantee anonymity for users: transactions use pseudonymous addresses and can be verified publicly, thus anyone can relate a user's transaction to her other transactions by a simple analysis of addresses she used in making bitcoin exchanges. More seriously, when the address of the transaction is linked to the real-world identity of a user, it may cause the leakage of all her transactions. Thus, mixing services (or tumblers) were designed to prevent users' addresses from being linked. Mixing, literally, it's a random exchange of users' coins with other users' coins, as a result, for the observer; their ownership of coins is obfuscated. However, these mixing services do not provide protection from coin theft. In this section, we describe two such mixing services and analyze their security and privacy properties.

Mixcoin: Mixcoin was proposed by Bonneau et al. in 2014, which provides anonymous payment in Bitcoin and bitcoin-like cryptocurrencies. To defend against passive adversaries, Mixcoin extends the anonymity set to allow all users to mix coins simultaneously. To defend against active adversaries, Mixcoin provides anonymity similar to traditional communication mixes. In addition, Mixcoin uses an accountability mechanism to detect stealing, and it shows that users will use Mixcoin rationally without stealing bitcoins by aligning incentives.

CoinJoin: CoinJoin is proposed in 2013 as an alternative anonymization method for bitcoin transactions. It is motivated by the idea of joint payment. Suppose a user wants to make a payment, he will find another user who also wants to make a payment, and they make a joint payment together in one transaction by negotiation. By the joint payment, it significantly reduces the probability of linking inputs and outputs in one transaction and tracing the exact direction of money movement of a specific user. CoinShuffle was proposed by Tim Ruffing et al. in 2014, which further extends the CoinJoin concept and increases privacy by avoiding the necessity of a trusted third party for mixing transactions. CoinShuffe is claimed as a completely decentralized coin-mixing protocol and has the ability to ensure security against theft. To ensure anonymity, CoinShuffle uses a novel accountable anonymous group communication protocol, which is called Dissent.

Table 2: Summary of existing and upcoming security and privacy techniques of 5ire

Techniques	Advantages
Homomorphic Encryption (HE)	It can achieve privacy-preserving computation by performing computations directly on ciphertext.
Zero-Knowledge Proof (ZKP)	User can easily prove that he has sufficient balance for the transfer with ZKP, while without revealing the account balance.
The Trusted Execution Environment (TEE) based solutions	It can protect the privacy of smart contracts by running them in TEE.
Attribute-Based Encryption (ABE)	It can simultaneously achieve data confidentiality and fine-grained access control
Secure Multi-Party Computation (SMPC)	It allows multi-party to carry out some computation jointly over their private data inputs without violating their input privacy

Volume: 05, Issue: 04 "July - August 2022"

ISSN 2582-0176

Group signature	The identity of signer can be hidden among a group of users. In the event of a dispute, the identity of the signer can be revealed.
Ring signature	The identity of signer can be hidden among a group of users. No need for the participation of any trusted third party
Mixing	It can prevent users' addresses from being linked.

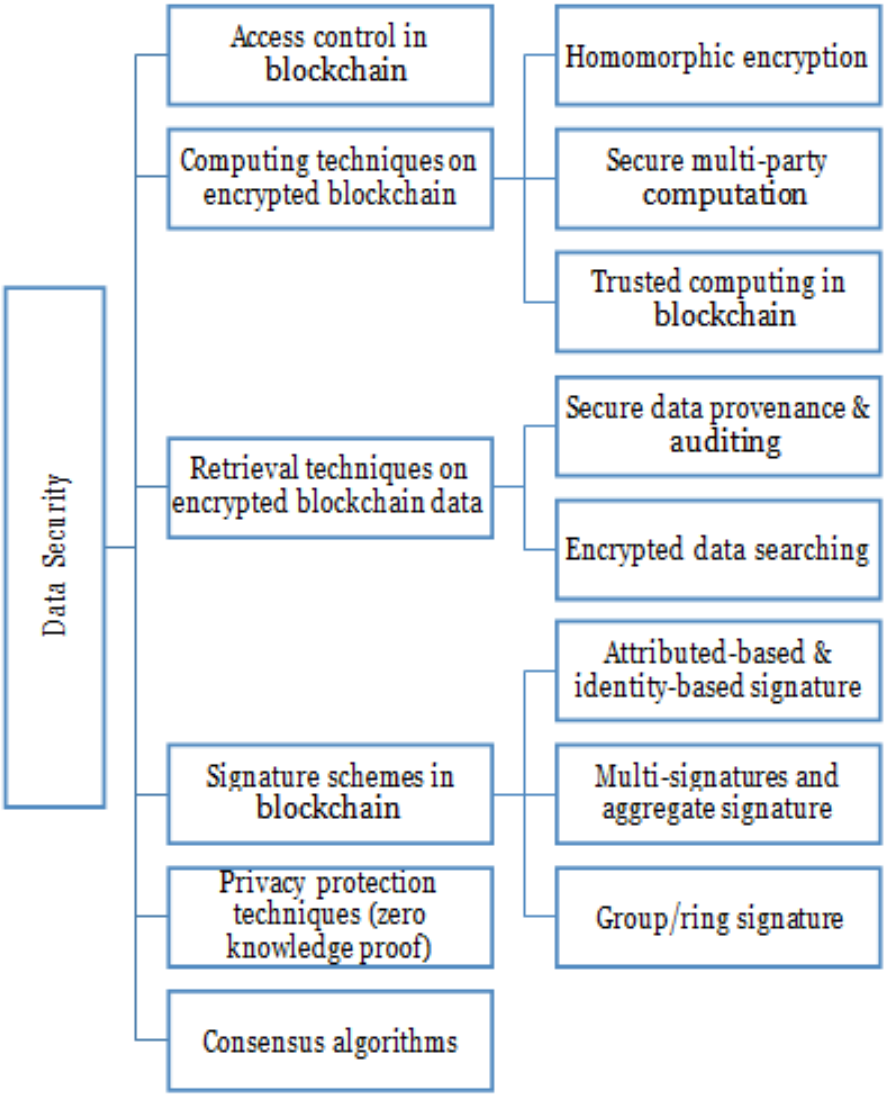

Figure 1: Major aspects of Data Security in the 5irechain

Blockchain infrastructure becomes more exposed to vulnerabilities than ever before. Generally, infrastructure security contains three aspects: private key management, terminal and networking vulnerability, and compliance enablement.

Volume: 05, Issue: 04 "July - August 2022"

ISSN 2582-0176

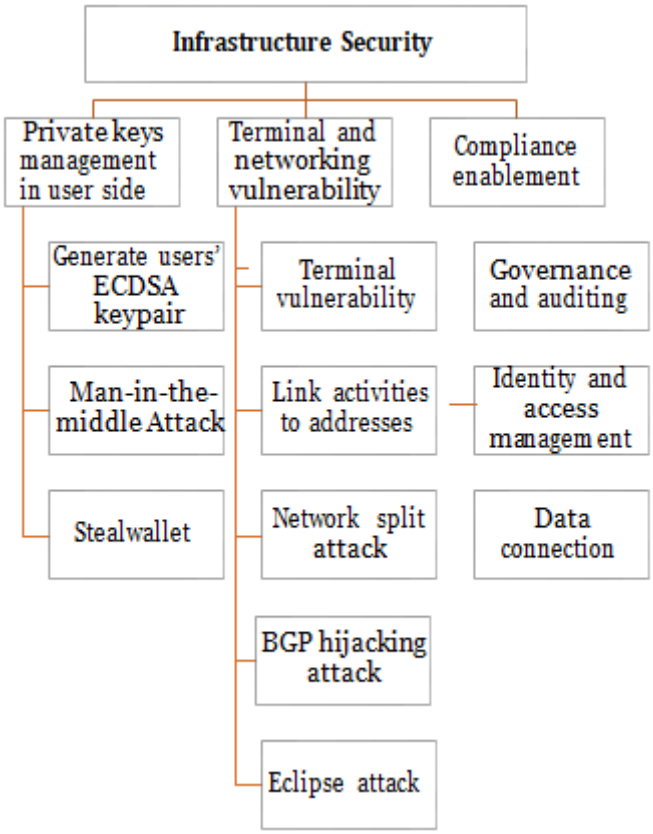

Figure 2: Major aspects of the Infrastructure Security in the blockchain

3.0 SECURITY ENDORSEMENTS, FUTURE DIRECTION, AND CONCLUSION

Based on the increasing use of blockchain technologies and the incidents reviewed, 5irechain's best practices framework can reduce the chance of cyber security vulnerabilities.

Regulatory Compliance: Blockchain solutions are often implemented on cloud platforms, and we have already seen hacks due to the cloud infrastructure. 5ire team carefully investigates the risks of the cloud platform itself and ensures to choose an appropriate platform to host permissioned blockchains, especially within a regulated industry. We ensure our cloud infrastructures are at least compliant with ISO 27001 and ISO 270017. The 5ire team also considers industrial-specific compliance requirements.

Blockchain Providers Selection: Blockchain consumers carefully consider platforms available when choosing a third-party provider. The question they may ask is: will this provider help me to be compliant with the needs of my industry? 5ire team always has the consumer in mind by ensuring that 5irechain frameworks contain detailed guidance on how we can help consumers to satisfy their industrial needs. In essence, the 5irechain framework meets all needs of the consumer as a provider.

Routine Audits: Mistakes can compromise the entire system as seen with The DAO incident. The 5irechain framework contains the detail of how an internal formal code review should be

carried out, who should carry out the review, what experience is required to undertake the review, and what seniority level is required for sign-off. It is unrealistic for all smart code contracts to be externally audited, however, all will go through detailed internal reviews. The framework states that if a code has been audited for a specific purpose, it should not be used for other purposes.

Automation of Blockchain Incident Response: In the root cause analysis, it was noted that in many cases the root causes of hacks were not discussed or recorded. This results in a lack of ability for the wider blockchain community to learn from security breaches. Companies can therefore fall victim to the same attacks that could otherwise have been prevented. Therefore, 5ire provides necessary public information at the earliest opportunity. This allows other organizations adopting our technology to learn although their purpose in using the blockchain may be different, the vulnerabilities remain the same.

Use of Hot Wallets and Cold Wallets: Hot wallets were identified earlier as a key risk, with some incidents being the result of hackers gaining access to hot wallets. Although the vulnerability may have been elsewhere, if cold storage had been used, the attack could have been mitigated. This is not to say that cold storage is completely secure, but we have seen many more hot wallet breaches in comparison to cold storage. Therefore, the keys of value are stored using cold storage methods.

End-to-end Product Life Cycle Reviews: Detailed end-to-end reviews is 5ire's part of the business process to try and identify vulnerabilities through risk-based scenarios. This will aid proactive identification of risks rather than waiting until they materialize. Experience is borrowed from the cyber security risk assessment that key blockchain risk factors throughout the product life cycle should be identified, measured, prioritized, and mitigated to an acceptable level that is benchmarked or predefined.

Automated Checks: Automated checks should be in place to ensure the systems and processes are working as expected. In this respect, 5ire designed 'Automated Management Information Reports' to check such totals and send an alert when a mismatch is detected.

"A blockchain is as secure as its underlying code"… Therefore, before going public with our blockchain, we run thorough tests and audits for any blockchain security issues. As the financial value of our blockchain increases, so does the attacks on it. While a blockchain security audit may seem costly, it's nothing compared to the losses we may face if an unfortunate attack happens on your blockchain-based app. We do regular in-depth security audits and pentesting will prevent our blockchain from going defunct in the future. To prevent 5irechain from being well-secured, we use Proof of 5ire that can help prevent the 51% attacks. As the decision will be made by users who are already in control of the majority of coins. We ensure any pool that breaches a limit of 40%, gets some of its miners diverted to other pools. To prevent routing attacks on us. we use secure routing protocols (one with certificates) which can help We build a robust community of our blockchain users and update them via phone numbers, emails, newsletters, etc. regarding safe private key storage practices.

Volume: 05, Issue: 04 “July - August 2022”

ISSN 2582-0176

5irechain implementations and solutions have considered security embedded in the technology stack. 5irechain security measures are implemented at each layer with a risk-based approach. This strengthens the defense and builds up the cyber resilience of the platform against attacks from foreseeable vectors. As implementations mature and the risks evolve, 5irechain considers reviewing the risks at each layer and strengthening its security measures appropriately.

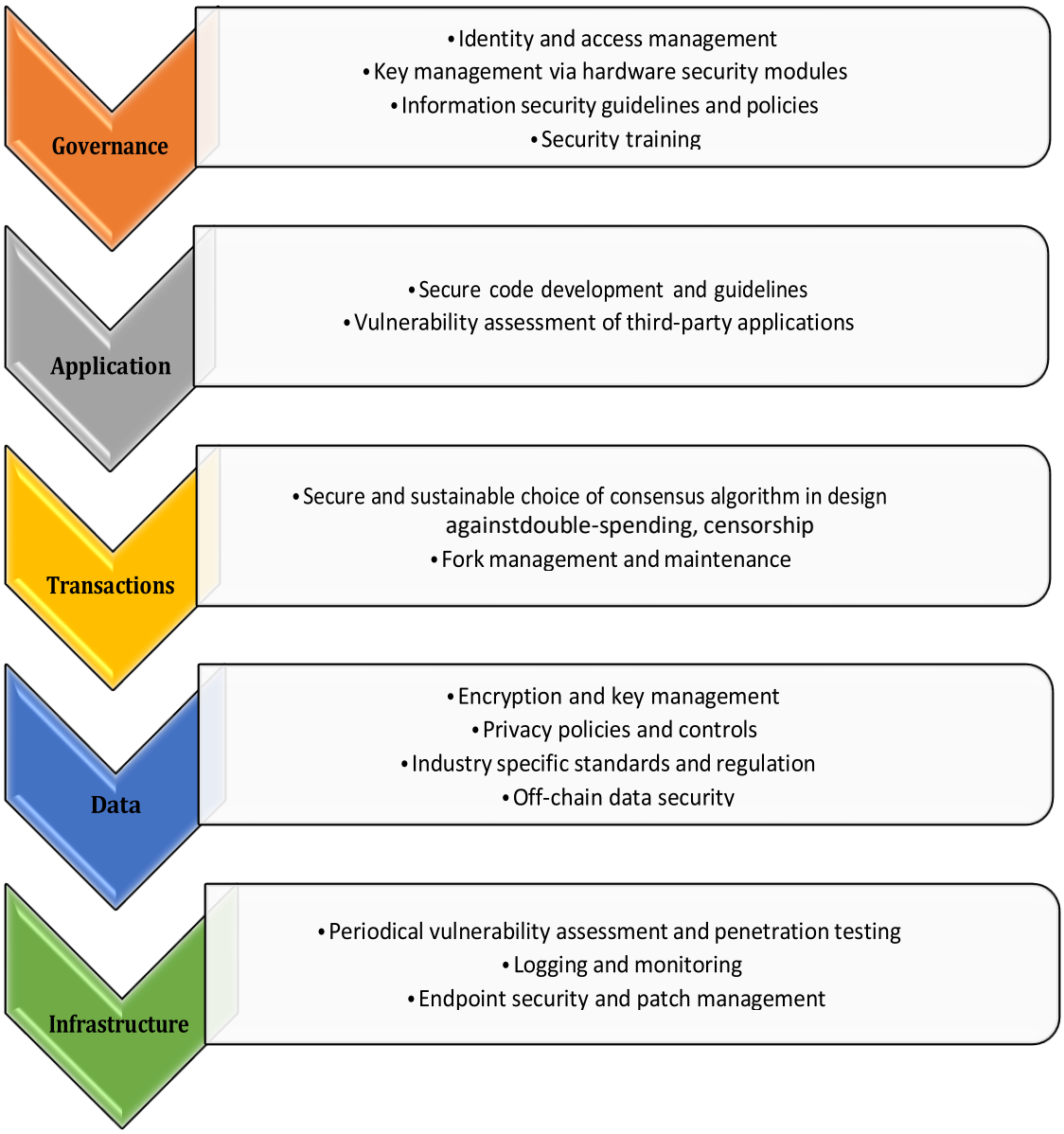

Figure 3: 5irechain security measures for different areas

REFERENCES

Benet, Juan. "IPFS-content addressed, versioned, P2P file system (DRAFT 3)." arXiv preprint arXiv: 1407.3561, 2014.

Berkowsky, Jake A., and Thaier Hayajneh. "Security issues with certificate authorities." In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pp. 449-455. IEEE, 2017.

Chung, Christina Yip, Michael Gertz, and Karl Levitt. "Demids: A misuse detection system for database systems." In Working Conference on Integrity and Internal Control in Information Systems, pp. 159-178. Springer, Boston, MA, 1999.

Datta, Sreemana, Ayan Kumar Das, Abhijeet Kumar, and Ditipriya Sinha. "Authentication and privacy preservation in IoT based forest fire detection by using blockchain–a review." In International Conference on Internet of Things and Connected Technologies, pp. 133-143. Springer, Cham, 2019.

Dib, Omar, Clément Huyart, and Khalifa Toumi. "A novel data exploitation framework based on blockchain." Pervasive and Mobile Computing, 2020.

J. F. Barrera, C. Vargas, M. Tebaldi and R. Torroba, "Chosen-plaintext attack on a joint transform correlator encrypting system", Opt. Commun., vol. 283, no. 20, pp. 3917-3921, Oct. 2010.

Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future generation computer systems 82, 395-411. 2018.

Lee, Wenke, and Dong Xiang. "Information-theoretic measures for anomaly detection." In Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001, pp. 130-143. IEEE, 2000.

Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. On security analysis of proof-of-elapsedtime (PoET). In Stabilization, Safety, and Security of Distributed Systems. 282–297, 2017.

Peng, L.: DAIS: A real-time data attack isolation system for commercial database applications. In: 17th Annual Computer Security Applications Conference (ACSAC 2001), pp. 219–229. IEEE Press, New Orleans, 2001.

Peter Bogetoft et al., Secure multiparty computation goes live. In FC, 325–343, 2009.

Saad, Muhammad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and Aziz Mohaisen. "Exploring the attack surface of blockchain: A systematic overview." arXiv preprint arXiv. 2019.

Saleh, Fahad. "Blockchain without waste: Proof-of-stake." The Review of financial studies 34, 1156-1190, no. 3, 2021.

