Blockchain Interoperability: Performance and Security Trade-offs

Babu Pillai
Griffith University
Southern Cross University
Gold Coast, Australia
babu.pillai@scu.edu.au

Zhé Hóu
Griffith University
Brisbane, Australia
z.hou@griffith.edu.au

Kamanashis Biswas
Australian Catholic University
Brisbane, Australia
kamanashis.biswas@acu.edu.au

Vinh Bui
Southern Cross University
Gold Coast, Australia
vinh.bui@scu.edu.au

Vallipuram Muthukkumarasamy
Griffith University
Gold Coast, Australia
v.muthu@griffith.edu.au

Abstract

Blockchain technology is becoming a promising technological solution for enterprise applications with the rise of interoperable solutions. A cross-chain architecture facilitates interoperability, thus improves its chain efficiency, reduces fragmentation, and allows users and features to flow more freely across multiple blockchains. However, enabling interoperability in silo networks will make a significant functional trade-off on the security and performance of the system. This paper review trade-offs in blockchain technologies related to interoperability.

CCS Concepts: • **Computer systems organization → Embedded systems**; *Redundancy*; Blockchain; • **Networks →** Network security.

Keywords: Blockchain, interoperability, interoperability trade-off, decentralisation

ACM Reference Format:
Babu Pillai, Zhé Hóu, Kamanashis Biswas, Vinh Bui, and Vallipuram Muthukkumarasamy. 2018. Blockchain Interoperability: Performance and Security Trade-offs. In *Proceedings of Fourth ACM International Workshop on Blockchain-enabled Networked Sensor Systems Co-located with SenSys-2022 (BlockSyS 2022).* ACM, New York, NY, USA, 7 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

The first generation of blockchain is a stand-alone system which has a boundary of its network of nodes. Each system has its own application use case, such as Bitcoin - for currency, and name coin[1] for DNS. By design, they are not meant to be interoperable due to the trust and security model of the system. The second-generation blockchain came along with a platform approach where users can create different applications on top of a platform [3]. Different applications on the same network can interoperate with each other due to the shared trust and security model. However, putting everything into a single-threaded pipe leads to the major limitation of scalability. This technology could become a universal solution if one chain could be used everywhere. Instead, several blockchain networks and platforms emerge with different use cases that are isolated from each other and unable to interact with each other. The technology of blockchain is fundamentally designed as a stand-alone system which has a boundary of its network of nodes [16]. It is designed in a way that a network of node participants, who are the shareholders, make the decision on what the current state of the system based on the protocol. The protocol dictates the value and the built-in consensus of the system. Most importantly, the value exists only within the nodes and the system. Bitcoin was the first protocol developed to maintain a crypto-coin called BTC in the public space.

Blockchain featuring the distributed ledger technology is an emerging type of business improvement process. Decentralisation is the driving focus behind this digital technology, with fast, secure and reliable ways of storing and transferring critically important data. If we consider the blockchain-based system and its use cases, primarily, there are two types: As a holder of digital objects [10] and as a platform to run business rules/logic using smart contracts. Within these types, varying kinds of interoperability requirements exist. We believe in application-specific blockchain systems, and there

BlockSyS 2022, November 6, 2022, Boston, USA
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX

[1] https://www.namecoin.org/

will not be a perfect solution to address all needs at once. Therefore, these application requirements result in the need for many chains of different kinds [2]. One such technology that is becoming increasingly evident is the cross-chain technology.

If we consider the blockchain system as a single standalone system that corresponds to many nodes and users, then the application can operate and transact the value from one user to another easily. Here the challenge is to transact between different networks that hold their own values. As applications become more sophisticated, objects may be representations of different types of things such as tangible objects and abstract objects, which require the ability to be identifiable. In a blockchain data structure, the order of each entry that makes the current state is important [12]. Generally, interoperability focuses on systems, data, and information [15]. However, interoperability in DLTs focuses on reading, observing, and acting on states and events [13].

Despite its importance, interoperability concepts are not fully understood, and this is vital for the future growth of this industry. However, with the current architecture, it may not be entirely possible. When transferring assets between networks, the systems involved need to ensure the safety of the network and its process. For this, the network involved needs to identify the appropriate middleware mechanism and process to integrate the networks. While these choices introduce interoperability, they result in trade-offs which are defined as *a compromise between two desirable but incompatible features.* For example, a trade-off has been made in the design of a consortium blockchain model, where there is a limitation on participants operating on the network to improve performance. Understanding the potential trade-offs in integrating blockchains is important, as it better informs the development of blockchain integration networks. Since this interoperability approach relies on the middleware mechanism, the primary challenges lie in securing the integration process. The integration process and its security aspects have been underexplored; therefore, how interoperability trade-offs affect the suitability of a blockchain should be investigated.

This research makes an original contribution on the review of decentralization and its trade-offs. First, we formulate security properties of the distributed system in relation to decentralization. Secondly, we discuss interoperability trade-offs on decentralization and present a trade-off equilibrium that measures the extent of a given system's decentralization. And finally, security concerns of the interoperability integration modes are discussed.

2 Interoperability trade-offs

Interoperability solutions lead to a specific set of node(s), integrate through interfaces and communicate with the networks. While these choices introduce interoperability, they violate the principle of decentralization, resulting in trade-offs on the security of the system against its performance.

2.1 Security

In the context of this paper, security refers to the processes and methodologies involved in protecting a blockchain system and assuring its integrity [5, 7]. This includes the security of the network itself, as well as the security of the data and the information that is stored on the blockchain. This can include data such as transaction histories, financial records, and identifiable personal information. Blockchain security aims to protect this information from unauthorized access and tampering. It is a relatively new field that is constantly evolving, as new threats and vulnerabilities are discovered. The most common threats to blockchain security are 51% attacks, sybil attacks, and double spending. There are a number of different approaches to blockchain security, including cryptographic techniques, access control mechanisms, and decentralized consensus protocols. When designing a system, the two main considerations are performance and security. Performance must be considered, as well as the security of the system. We consider that security and performance are two sides of the same coin and are contradictory goals to achieve. They are directly related and dependent on each other [7] and the goal is to have the right balance between them.

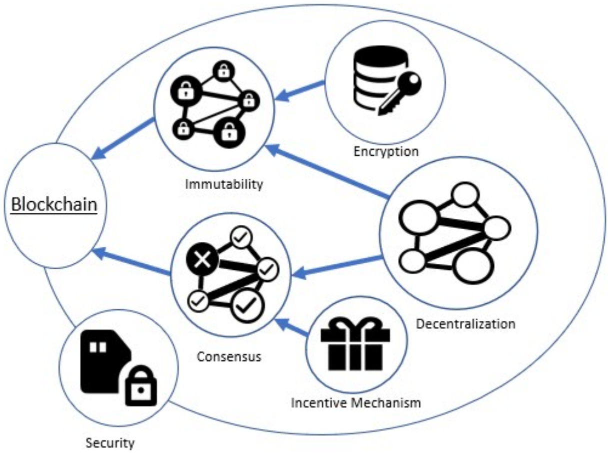

Figure 1. Blockchain security architecture.

A permissionless blockchain system is more secure because it is transparent. All transactions that take place on the blockchain are visible to everyone on the network. This transparency makes it very difficult for anyone to tamper with the blockchain. Therefore, the security in a blockchain technology-based system is concerned with preventing centralized control of the system [7]. We argue that decentralization, which is, defined as *not controlled by a single entity* or *distributed among many nodes*, is the key to maintaining this security. For example, the high performance of a DLT design mostly comes at the cost of its level of security [8, 9]. Figure 1 illustrates a blockchain security architecture. The main characteristic of blockchain technology is defined as its *ability to operate in distributed environments without relying on a trusted third party*. There are two main features that make up these characteristics. Firstly, compared to a distributed ledger system which updates its ledger, in the blockchain technology, individual ledger transactions are segmented and cryptographically combined to form a chain of blocks. Thus, it creates an immutable cryptographical secure record of all transactions that ever happened across the network. Secondly, instead of updating the ledger, new records can only be appended to the chain once the network reaches consensus. Here, this consensus process is embedded with processes and techniques that allow participants on a distributed network to reach consensus.

These unique characteristics of blockchain offer new infrastructure for business applications, but they carry some unique security challenges. Technically, the protocol[2] is proved to be tamper-resistant; however, vulnerabilities are found in the components of its applications. The components such as the smart contract and wallet have been exploited with some significant consequences of DAO [18], wallet and exchange attacks [6]. However, the usability of a large number of blockchain-based business solutions is to deal with the storage and transportation of data. In that context, security focuses on ensuring integrity (referring to the risk of unauthorised modification of data), consistency (referring to the possibility of inconsistencies of data held by different entities) and availability (referring to the access of the data and the system) of data [17]. These basic security properties stem from the cryptographical features along with the distributed nature of its database and consensus process. Therefore, the security of blockchain-based distributed ledger systems very much relies on the property of decentralisation.

2.2 Performance

Similar to security, there are many different situations in which various performance measures are needed to understand the usability[3] of a system. From an application perspective, one of the performance measures is *How fast a blockchain-based system performs for a given operation?*, for example, confirmation of a transaction. However, due to the distributed nature of the system, the performance measures resemble the collective nodes' response time and decision, not simply based on an individual node. On top of such design constraints, we should also consider some other parameters that inherently belong to distributed and decentralized systems such as network propagation time, which is dependent on the network topology and hardware configuration of the participating nodes.

While many parameters determine the performance of a blockchain system, evaluating the performance based on a single parameter is not possible [11]. When compared to the decentralized system, a centralized system has a higher performance rate typically in terms of throughput. However, a blockchain-based decentralized and distributed consensus system offers a higher level of trust and security. So, the performance comparisons between centralized and decentralized systems do not just measure the performance of the system, but also include how secure the system is. The decentralized consensus nature of the blockchain system makes it challenging to break the system as an attacker has to compromise the majority of mining nodes to falsify any data. Decentralization is a fundamental concept of a blockchain-based system. However, the current performance metric of transaction per second completely ignores the feature of decentralization.

2.3 The interoperability equilibrium

Motivated by the property of decentralization, we present a concept of an interoperability equilibrium that measures the extent of a given system's decentralization. Further, the trade-off equilibrium also determines how much a given usability modification improves or reduces the degree of decentralization. On the given equilibrium in Figure 2, security and performance are two ends of a spectrum. For any given usability scenario, the equilibrium indicates the balance between security and performance. As a result, the Y axis shows the degree of decentralization. Our approach to measure decentralization beginning with determining the elements that impact the system's decentralization.

To apply this concept in a public blockchain-based system, we need to make the distinction between security and performance. Here security refers to the decentralized safety of the systems, and performance refers to the application output based on its specification. A decentralized system of is composed of a set of decentralized subsystems such as consensus process, data storage, and mining process. A usability situation that modifies any of these subsystems results in the system making a trade-off. Note that these challenges are not specific to information systems, instead they are inherent challenges of blockchain technologies. For instance, 51% of attacks are theoretically possible, but with the right amount of decentralization, it is challenging to do in practice for most of today's major blockchains [5].

On the X axis is the application usability, defined as the degree to which that application is fit for the purpose within the constraint of the technology framework. Based on the application requirement, the usability will move along the X axis, making the trade-off choice between security and performance. Respectively, the degree of decentralization will

[2] We refer to the Bitcoin or Etherium

[3] https://hackernoon.com/blockchain-usability-checklist-5c5e1409183d

be indicated on the Y axis. If the usability choice is of performance, then the usability will move towards performance and security will decrease. Similarly, if the usability choice is of security, the performance will decrease and result in a higher degree of decentralization.

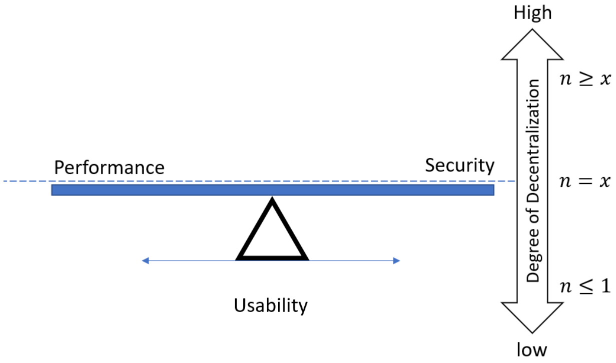

Figure 2. Blockchain trade-off equilibrium.

In a blockchain-based system, the security and integrity of data and its transfer is achieved using mathematically designed cryptosystems and processes. Interoperability infrastructure acts as a framework that allows blockchain networks to connect, thereby benefitting from operating in a more comprehensive scalable network. However, the ability to integrate value and assets has significant implications on the process. Blockchain's characteristics are dependent on its features, therefore improving such features affect the characteristics. For instance, Bitcoin offers security through a higher number of participating nodes which results in low performance. However, Hyperledger[1] Fabric offers higher performance compared to security, with a fixed set of participating nodes. In the interoperability context, to succeed in integration, blockchain systems must make trade-offs in function efficiency. Meanwhile, these networks also ensure their own safety and prevent attacks, leading these systems to have a distinct combination of design which offer differences in security and performance. The networks must choose a trade-off based on which of them provides the best protection for the key capabilities offered by the network. Therefore, the solutions are making their way to a mix of centralized and decentralized methods for the next generation of the blockchain network.

2.4 Interoperability concerns and trade-offs

Interoperability processes take place at various levels [4]. This section defines the interoperability concerns and trade-off derived from the various tasks performed at a different level of an interoperability process. These given concerns are defined based on the point of view of a blockchain-based system. The objective is to capture the interoperability concerns at a varying level. The concerns are coupled, such that one might contribute to or detract from another.

Table 1. Interoperability concerns

levels	Interoperability concerns
Application level	Defined access permission/ role to participates in the network.
Consensus level	Special privilege on data validation.
Database level	Cross-chain data validate through witnessing.

The current blockchain architecture can be roughly divided into the **application layer** – *who has got access to the network*, the **consensus layer** -*who controls the network* and the **database layer** – *is the database distributed*. In an interoperability scenario, each layer has trade-offs based on its objectives. As shown in Table 1, the interoperability trade-off at the application layer is *role-based access control* which determines who could view, add and update information in the network; at consensus level, the trade-off involves *selected validation*, which involves nodes that are given special privilege to perform validation or delegate to produce a block on the network; and at the database level, the trade-off involves nodes only witnessing data based on the proof from another chain. While these trade-offs offer interoperability, security of the system is compromised.

Currently, cross-chain technology and its mechanics are in an exploratory stage. Existing research on blockchain interoperability has mainly focused on platform and application-specific solutions. Within these projects, solutions are tailored to specific contexts and employ a particular blockchain design to meet the requirement in the close context. Trade-offs resulting from the integration between blockchains are often neglected and not further investigated. Consequently, interoperability and resulting trade-offs between blockchains are not quantified. Therefore, we use our blockchain trade-off equilibrium to calculate the trade-offs shown in Figure 3 against the benefits.

We assume *minimum decentralization* a satisfactory node threshold[4] as x, therefore, the number of nodes $n = x$; the upper bound of n is $n \geq x$; and the lower bound of n is $n \leq 1$. Figure 3 illustrates the given interoperability scenario, the application and consensus level trade-off directly affect the features of immutability, and distributed consensus results in the security of the system decreasing. Being in a controlled environment of access, validation, and verification increases the system's performance accordingly. Therefore, introducing interoperability to improve or add new capability will affect the degree-of-decentralization of the system. However,

[4] which is a minimal requirement to deal with Byzantine behaviour

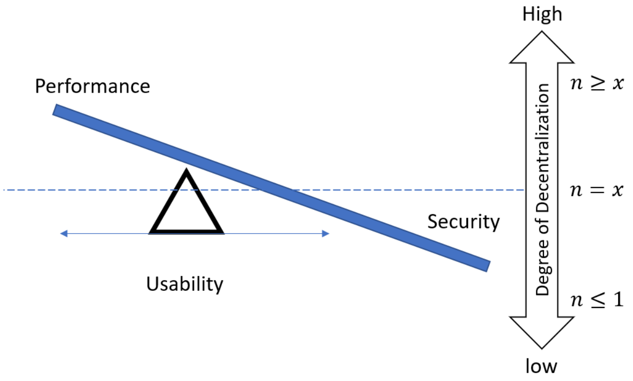

Figure 3. Blockchain interoperability trade-off equilibrium.

it will be waived against the benefits offered by the integration of networks. Refer to Table 2 for a brief description of trade-off consequences.

The primary advantage of blockchain over other DLT systems is its distributed consensus ability deriving from its property of decentralization. Interoperability in blockchains consists of a group of technologies and services that enable the distribution of digitization processes across multiple enterprises. For this, careful considerations are given to decentralization, it's trade-off, and the usability of the applications and processes that represent them are highly recommended.

3 Discussion and conclusion

Interoperability is a broad problem in the domain of information systems. The scope of the work described here is focused around interoperability for blockchain-based technology. In this digital age, information systems must communicate outside of its organizational boundary, which allows more integrated services and improves efficiency. Current research on interoperability in blockchain technology addresses the challenges of interpreting and exchanging values through solutions of a middleware system. However, the trade-off and security concerns of the middleware solutions have not been identified and discussed.

In this research, we analyse the current state and the future of interoperability and decentralization in a blockchain ecosystem. We explore and examine the dimensions and importance of decentralization. Decentralization is the key property that maintains the security of a blockchain system; therefore, the degree of decentralization is a fact to measure. The settlement layer of different interoperability modes can measure the degree of decentralization against the trade-off. However, despite its importance, we are unable to calculate decentralization. If we could, it would allow us to measure the extent of a given system's decentralization and determine how much a given system's modification improves or reduces decentralization.

Decentralization is defined as distributed among or controlled by a number of entities. However, the number of entities is not fixed; it could range between 2 to n, therefore, it is hard to determine a quantitative minimum or maximum value of decentralization unless a fixed number is given. The mining process of public blockchains such as Bitcoin and Etherium is somewhat decentralized. However, we do not have a quantitative measure of a minimum or maximum value of decentralization. Quantifying blockchain's decentralization using metrics that are not objective may not be ideal. Instead, an alternative strategy is to identify the known cause of centralization.

In an interoperable ecosystem, a variety of blockchain networks operate in cooperation with each other to suit the needs for varying types of use cases. A defined integration process will address all cross-chain settlement. The settlement mechanism and process will vary based on the mode of integration. The key to the settlement is that integration services will serve as the global trust layer for all those connected networks. The settlement layer provides security and

Table 2. Interoperability trade-off consequences

Value	Security	Performance
Application level	Access restriction could lead to centralization of participants in the cross-chain process; therefore, the network must adopt security parameters of permission models to secure the cross-chain process.	This could result in high performance by processing cross-chain transactions through a set of authorised nodes. However, depending upon the number of participant nodes, the system could face a centralization risk.
Consensus level	Selected validation could lead to centralization of consensus in the cross-chain process; therefore, the network must adopt adequate consensus mechanisms to secure the cross-chain process.	Cross-chain consensus processes through selected nodes increases performance. However, depending on the number of participant nodes, the system could be under the control of those selected nodes.
Database level	Data witnessing through middleware entity leads to centralization of data verification; therefore, the network must adopt adequate middleware mechanisms for cross-chain data verification and validation.	Cross-chain data are witnessed through a middleware process that fills the gap of cross-chain settlement. However, connected systems must choose the right middleware mechanism.

Table 3. Security concerns of integration modes

Integration mode	Security concerns
Third-party[14]	A Third-party integration mode consist of mechanisms that interconnect the independent network of blockchain systems through third-party services. Therefore, the security of the cross-chain process is dependent on the credibility of the third-party services provider. The system must choose an appropriate middleware mechanism of third-party services that satisfies the requirements of the application.
Bridge[14]	Bridges are an intermediate mechanism that aims to provide interoperability between two networks. A possible bridge mechanism is composed of special nodes which act as gateway nodes that process a cross-chain settlement. Each network will have its own set of gateway nodes that are trusted by the network. We assume a gateway selection algorithm is employed by the network; therefore, the gateway way will be selected randomly or by the protocol. Therefore the decentralization security guarantee of the bridge mode depends on the gateway node and its selection process. Depending on the application's usability requirement, the network can choose the degree of decentralization to increase the performance.
Connector[14]	In the concept of the connector mode, a possible integration mechanism can be a distributed network which acts as a mother blockchain for the connected networks. The mother blockchain acts as a trust layer where the settlement takes place and provides security and finality for the connected blockchain. Therefore, the decentralization security guarantee of the connector integration process largely depends on the characteristics of the decentralization of the mother blockchain.

objective finality of transactions that happen on the connected networks. It is important to note that the security guarantee of the integration process at the settlement layer is dependent on the choice of integration mode. Therefore, choosing the right integration mode for an interoperable ecosystem is important. In reality, not every integration process needs to prioritize absolute decentralization; rather, it can prioritize the application's usability with varying degrees of decentralization that trade-off security. However, despite the widely acknowledged importance of this property, most discussions on the topic of interoperability lack the understanding of decentralization security concerns. In Table 3, we present possible security concerns introduced by the mechanisms of the surveyed integration modes.

Ideally, interoperability is made possible through the middleware integration settlement layer on top of which different networks of blockchains can integrate. However, the integration solutions that lead to a specific set of node(s) that integrate through interfaces for cross-chain settlement violate the principle of decentralization, resulting in trade-offs. The networks must choose a trade-off based on which of them provides the best protection for the key capabilities offered by the network. Thus, the solutions are making their way towards a mix of centralized and decentralized methods of integration solutions for the next generation of the blockchain network. The application's usability can prioritize the trade-off with varying degrees of decentralization. The decentralization guarantee will vary depending on the protocol, the type of network and the consensus algorithm. Minimum decentralization for a public PoW blockchain looks very different to how a private PoS blockchain would. Therefore, the future work that identifies interoperability trade-off metrics that measure decentralization should identify objective data depending on the protocol, the type of network and the consensus algorithm. We conclude that, although interoperability offers a different set of functionalities, there are trade-offs at the cost of security or performance. This is useful when deciding which integration mode to choose and to become aware of the trade-off that comes with each solution.

References

[1] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*. 1–15.

[2] Gray block. 2018. Interoperability — The Holy Grail of Blockchain. *https://medium.com/coinmonks/interoperability-the-holy-grail-of-blockchain-eb078e1a29cc, accessed date: 10 June 2019* (2018).

[3] Richard Brown. 2018. The interoperability challenge will make or break enterprise blockchain platforms. *https://medium.com/corda/the-interoperability-challenge-will-make-or-break-enterprise-blockchain-platforms-4016518e333d, accessed date: 2 March 2019* (2018).

[4] David Chen, Nicolas Daclin, et al. 2006. Framework for enterprise interoperability. In *Proc. of IFAC Workshop EI2N*. Bordeaux, 77–88.

[5] Amir Dembo, Sreeram Kannan, Ertem Nusret Tas, David Tse, Pramod Viswanath, Xuechao Wang, and Ofer Zeitouni. 2020. Everything is a race and nakamoto always wins. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 859–878.

[6] Giuseppe Destefanis, Michele Marchesi, Marco Ortu, Roberto Tonelli, Andrea Bracciali, and Robert Hierons. 2018. Smart contracts vulnerabilities: a call for blockchain software engineering?. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 19–25.

[7] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. 2015. The bitcoin backbone protocol: Analysis and applications. In *Annual international conference on the theory and applications of cryptographic techniques*.

Springer, 281–310.

[8] Johannes Göbel, Holger Paul Keeler, Anthony E Krzesinski, and Peter G Taylor. 2016. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation* 104 (2016), 23–41.

[9] Johannes Göbel and Anthony E Krzesinski. 2017. Increased block size and Bitcoin blockchain dynamics. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, 1–6.

[10] William J Gordon and Christian Catalini. 2018. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal* 16 (2018), 224–230.

[11] Garrick Hileman and Michel Rauchs. 2017. Global blockchain benchmarking study. *Rochester, NY: Social Science Research Network* (2017).

[12] Tommy Koens and Erik Poll. 2018. What blockchain alternative do you need? In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 113–129.

[13] Tommy Koens and Erik Poll. 2019. Assessing interoperability solutions for distributed ledgers. *Pervasive and Mobile Computing* 59 (2019), 101079.

[14] Babu Pillai, Kamanashis Biswas, Zhé Hóu, and Vallipuram Muthukkumarasamy. 2022. Cross-blockchain technology: integration framework and security assumptions. *IEEE Access* (2022), 1–1. https://doi.org/10.1109/ACCESS.2022.3167172

[15] Amit P Sheth. 1999. Changing focus on interoperability in information systems: from system, syntax, structure to semantics. In *Interoperating geographic information systems*. Springer, 5–29.

[16] Jack Thomas. 2019. Blockchain Interoperability Remains a Critical Missing Puzzle Piece. *https://journal.binarydistrict.com/blockchain-interoperability-remains-a-critical-missing-puzzle-piece/, accessed date: 10 October 2019* (2019).

[17] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)* 52, 3 (2019), 1–34.

[18] Xiangfu Zhao, Zhongyu Chen, Xin Chen, Yanxia Wang, and Changbing Tang. 2017. The DAO attack paradoxes in propositional logic. In *2017 4th International Conference on Systems and Informatics (ICSAI)*. IEEE, 1743–1746.