Towards Interconnected Blockchains: A Comprehensive Review of the Role of Interoperability among Disparate Blockchains

ANKUR LOHACHAB, SAURABH GARG, BYEONG KANG, MUHAMMAD BILAL AMIN, and JUNMIN LEE, University of Tasmania, Australia
SHIPING CHEN and XIWEI XU, CSIRO Data61, Australia

Unprecedented attention towards blockchain technology is serving as a game-changer in fostering the development of blockchain-enabled distinctive frameworks. However, fragmentation unleashed by its underlying concepts hinders different stakeholders from effectively utilizing blockchain-supported services, resulting in the obstruction of its wide-scale adoption. To explore synergies among the isolated frameworks requires comprehensively studying inter-blockchain communication approaches. These approaches broadly come under the umbrella of Blockchain Interoperability (BI) notion, as it can facilitate a novel paradigm of an integrated blockchain ecosystem that connects state-of-the-art disparate blockchains. Currently, there is a lack of studies that comprehensively review BI, which works as a stumbling block in its development. Therefore, this article aims to articulate potential of BI by reviewing it from diverse perspectives. Beginning with a glance of blockchain architecture fundamentals, this article discusses its associated platforms, taxonomy, and consensus mechanisms. Subsequently, it argues about BI's requirement by exemplifying its potential opportunities and application areas. Concerning BI, an architecture seems to be a missing link. Hence, this article introduces a layered architecture for the effective development of protocols and methods for interoperable blockchains. Furthermore, this article proposes an in-depth BI research taxonomy and provides an insight into the state-of-the-art projects. Finally, it determines possible open challenges and future research in the domain.

CCS Concepts: • **General and Reference** → **Survey and overviews**; • **Distributed Ledger Technology** → **Blockchain**; • **Blockchain** → Blockchain Interoperability; Interoperability Taxonomy; Interoperability Reference Framework; State-of-the-Art;

Additional Key Words and Phrases: Blockchain, distributed systems, blockchain interoperability, taxonomy, consensus mechanisms, DLT

ACM Reference format:
Ankur Lohachab, Saurabh Garg, Byeong Kang, Muhammad Bilal Amin, Junmin Lee, Shiping Chen, and Xiwei Xu. 2021. Towards Interconnected Blockchains: A Comprehensive Review of the Role of Interoperability among Disparate Blockchains. *ACM Comput. Surv.* 54, 7, Article 135 (June 2021), 39 pages.
https://doi.org/10.1145/3460287

This research is supported by the Tasmanian Graduate Research Scholarship (TGRS)
Authors' addresses: A. Lohachab (corresponding author), S. Garg, B. Kang, M. B. Amin, and J. Lee, School of Information and Communication Technology (ICT), Syndicate of Technology, Environments and Design (STED), College of Sciences and Engineering, University of Tasmania, Sandy Bay, Hobart, Tasmania, Australia 7005; emails: ankur.lohachab@utas.edu.au, saurabh.garg@utas.edu.au, byeong.kang@utas.edu.au, bilal.amin@utas.edu.au, junmin.lee@utas.edu.au; S. Chen and X. Xu, Data 61 Eveleigh, Australia; emails: shiping.chen@data61.csiro.au, xiwei.xu@data61.csiro.au.

0360-0300/2021/06-ART135 $15.00
https://doi.org/10.1145/3460287

1 INTRODUCTION

The current landscape of data management and sharing is undergoing rapid development of innovative approaches triggered by the potential benefits of DLTs. Proponents of these approaches are facilitated by a range of features that primarily include immutable and transparent records, decentralization, enhanced auditability, and security [107]. Perhaps one way of looking at DLT is that it is just a hyped technology due to its overestimated effects on the financial sector. However, after taking a closer look at Amara's law [99], it can be stated that DLT will draw major transformations across information systems in the long run. Meanwhile, the past decade witnessed that organizations are limiting their dependency on intermediaries for trust establishment, and instead of third-party entities, they prefer to develop innovative projects using DLT-based approaches (e.g., smart contracts instead of lawyers, P2P currency transfer instead of using banks, and distributed ledgers instead of using central data repositories). So far, as compared to other DLTs, the continuous growth of blockchain-based projects in terms of market liquidity, operational capacity, security, and privacy concerns, has unprecedentedly gained significant interest for considering blockchain technology for global value-exchange infrastructure [65, 82, 91]. The notion of Blockchain (one of the ways to implement DLT [52]) gained attention among industry and academia due to Bitcoin [80] (being its underlying technology), and currently, it is substantially expanding its boundaries (now, its applications range from cryptocurrencies to global supply chains) by following the path of inclusive development. Put simply, in comparison to traditional databases where nodes commonly follow a client-server network architecture, nodes in blockchain-based networks operate in a decentralized manner, and the information is stored over the network on every authorized node (depends upon governing policies) in a cryptographically linked chain of blocks (i.e., organize records in blocks and blocks in a sequential ledger using cryptographic signature) [33, 46]. In fact, concerning specific applications (e.g., P2P energy trading [85]), blockchain-based network architecture can be seen as an information management paradigm shift as compared to a traditional central client-server architecture.

Perhaps there are no formally defined paradigms that holistically cover the development of the blockchain. However, motivated by its game-changer platforms and applications, this article categorizes its development journey into four major stages (i.e., Blockchain 1.0, 2.0, 3.0, and 4.0), as depicted in Figure 1. There exists literature [12, 17, 87, 104, 105] that describes similar development stages (up to 3.0), and broadly their categorization is similar to one another. Blockchain 1.0 refers to the paradigm that ranges from putting forward the notion of the blockchain-enabled P2P payment system (referred to as cryptocurrency) for the first time (i.e., Bitcoin), till now where various other cryptocurrencies get evolved in the financial sector. Therefore, applications and platforms that come under this stage often revolve around payment networks. Blockchain 2.0 introduces autonomous programmable logic (often referred to as smart contracts) to the fundamental idea of blockchain, leading to another blockchain paradigm that supports a broader spectrum of applications. These smart computer programs (programming languages can be domain-specific) get automatically triggered or enforced for performing the predefined actions (agreed mutually by the authorized nodes) on the underlying ledger. Blockchain 3.0 focuses on expanding blockchain 2.0 initiatives in terms of applications, as in this stakeholders introduce a new generation of applications (e.g., by using dApps) and explore the potential integration of blockchain-based platforms with numerous sophisticated technologies/concepts, such as Machine learning, CPSs, IIoT, AI, IoT, and so on [22, 86, 95]. While blockchain 3.0 is still in its infancy, considering the immense demand for blockchain-based solutions among stakeholders, it is significant to design and develop an interoperable blockchain ecosystem to avoid fragmentation challenges, and solutions tackling these challenges can be broadly referred to as Blockchain 4.0.

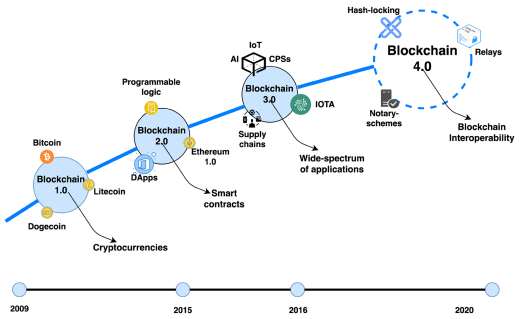

Fig. 1. Chronological flow of major paradigms depicting the developments under blockchain technology.

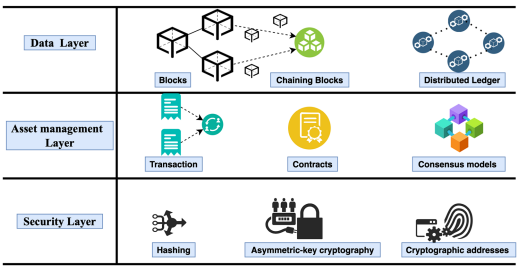

Fig. 2. The layered architecture of typical blockchain system depicting utilized component technologies.

This challenge of fragmentation is stemmed more recently when implementing different use-case scenarios stakeholders choose blockchain-based solutions that operate in silos. Thus, in a connected ecosystem scenario, these platforms may become obsolete, as they do not implicitly support interoperability and will act as a network of island archipelago having no interconnection between islands operating on separate blockchains. Therefore, this article argues that for the absolute realization of blockchain potential, there is a demand for a cornerstone architecture that can consolidate the heterogeneity of blockchain-enabled platforms, so their functionality can be represented as a single blockchain platform. This interoperability of blockchain would make the information and functionality easily accessible within disparate blockchain-based platforms.

1.1 Perception of Blockchain Interoperability

The current BI research roadmap focuses on application areas and implementation approaches resulting in no formal specifications or definitions (e.g., for enabling interoperability between two blockchains, there exist numerous BI solutions that are not interoperable in themselves). For aiming meaningful and significant research, it is critical to determine a formal theory of BI that will formulate the specifications, which will be valid in the general scenario. Therefore, this article aims to provide an initial impression of BI's formal specifications. It can assist in addressing two common challenges: (i) What is the meaning of interoperability within context to Blockchain?; (ii) What are the primary requirements for BI?

Now, before attempting to redefine BI through studying the boundaries and nature of various blockchain models (as classified in Section 2.3), it is more pertinent to understand: What does the blockchain definition exactly mean? Concerning this, this article reviews blockchain definitions given by standard-setting bodies [3, 5, 69], and it is found that even among them, the definition for blockchain varies. It creates ambiguousness among academia and organizations, resulting in no common understanding of the meaning of blockchain. However, it is also encountered that despite the divergences, these definitions reflect several similarities (e.g., both recall that blockchain is one kind of distributed ledger). Therefore for capturing these similarities, along with covering numerous blockchain-based models key aspects (e.g., tamper-resistant, successively growing, definitive blocks upon validation), this article recommends a general definition of blockchain with the help of its underlying primitive technologies, technical terms, and standards. Hence, we delineate the following definition of blockchain technology for understanding its broad outlook.

Blockchain can be defined as a conditionally growing decentralized and distributed digital ledger comprising cryptographically signed records of assets that are grouped in a chain of blocks upon validation.

The recommended definition represents a consistent approach within the scope of identified gaps and overlaps from the standard-setting bodies. But it may be possible that this not be able to highlight all of the distinctive blockchain perspectives. Considering this definition as symbolic of the fundamental blockchain (as depicted in Figure 2), we recommend the following BI definition, which can serve as a cornerstone for future research efforts:

An interoperable blockchain infrastructure can be considered as a composition of autonomous blockchain networks, where each network can be depicted as a distributed ledger of data, in which data can be operated among heterogeneous unconnected blockchain networks, and where data ledger can be accessed by validated foreign data.

Table 1 provides a high-level formalization of the BI concept under the recommended definition. To date, there are many practices done in implementing BI in various contexts, but this article identifies that there is one work [38] that is similar to the recommended definition and the TAST project [25–27] provides formalization to address the cross-blockchain challenge (somewhat similar to the mentioned formalization).

From the discussion in Table 1, it will be possible to articulate the BI concept in a more precise way. Moreover, in literature, there exist various methods for achieving swapping and transferring interoperability. However, despite several initial attempts, lack of formal specifications along with several other challenges (as mentioned in Section 5) serves as a bottleneck in the BI research roadmap. Concerning this, this article also believes that trustless interoperability will serve as a cornerstone for BI development journey. Therefore, accordingly, it presents a layered reference BI architecture in Section 3.1. Besides, this article does not assert that BI is the sole factor for Blockchain adoption, but still, it suggests a proactive approach in which academia and organizations should focus more on the development of BI solutions along the sidelines of performance-related solutions. Since, nowadays, most of the research works are focusing on the scalability of blockchain, and some of them can achieve the performance up to 40,000 TPS [49]. This performance is better than the initial platforms; even than the approximate VISA network TPS. However, there is still a lack of interest among industries in adopting blockchain as their primary infrastructure. This is probably because of the fact that blockchain infrastructure is still more isolated as compared to the global payment methods (e.g., MasterCard, VISA, American Express) [1]. These global methods are interoperable across Internet, merchants, and ATM. Interoperability plays an imperative role in the growing demand for these methods. Therefore, to increase the acceptability of blockchain among corporations, there is a need for the universal applicable standards or protocols that can support BI. More recently, WEF published a series of white papers [55, 56], which significantly highlights the importance of interoperability among blockchains and how it can assist in bridging the existing gap in governance. In Reference [56], the authors argued about how BI can improve the supply chain systems, especially in the ongoing coronavirus pandemic situation. Moreover, to our understanding, there are various potential benefits that can be achieved through the idea of interoperable blockchains. A few of them are listed below.

- Uninterrupted communication can be established to carry out frictionless information sharing among heterogeneous blockchains.
- Fungible and non-fungible assets can be exchanged regardless of the source and target blockchain.
- No single blockchain network will have the monopoly in the blockchain ecosystem, which will provide even more reliability in blockchain.
- Multiple opportunities can be practically possible even in a heterogeneous blockchain ecosystem, where users do not have to worry about their platform, as enabling interoperability can seamlessly transverse their independent blockchain boundaries.

Table 1. Formal Specification to Determine Fundamental Properties for Blockchain Interoperability

Formal specifications
BC Blockchain. We assume that each blockchain will abide by the fundamentals of the blockchain definition (given in Section 1.1).
B Block. It is a structured data defined as a two tuple structure, $B = (B_H, B_D)$, where B_H is the block header and B_D is the block data.
B_H Block Header. It is a structured data defined as B_H= (CL, T, N, HV), where cryptographic link (CL) : $B_{H_i} \mapsto B_{H_{i-1}}$ is the reference constructed using a CHF that point to previous B_H, T is the timestamp, N is the Nonce, and HV is the hash value (e.g., Merkle root).
B_D Block Data. Let T_R be the transaction records and ${}^*T_R$ be the reference to the transaction records. Then, B_D is a structured data comprising T_R or ${}^*T_R$, where $T_R = \{t_r \mid t_r \in \mathbb{N}^+ \cup \{0\}\}$ and ${}^*T_R = \{{}^*t_r \mid {}^*t_r \in \mathbb{N}^+\}$.
T Transaction. In the context of blockchain interactions, a transaction T can be referred as the smallest unit (i.e., in terms of transformation) of a system state (S). More precisely, $T(S_I, AC_J) = S_O$, where S_I, S_O are input and output states, respectively, and S_I, $S_O \subset S$. Moreover, AC_J represents a sequence of actions that are responsible for consistent system state transformation. In this, a system state can be described in terms of state of the assets, which generally includes assertions (e.g., governing rules) and allowed transformations for any particular state. The assets can be denoted as $a_i \in \mathbb{A}$, where $i \in \mathbb{N}^+$, and $\mathbb{A} = \mathbb{A}_T \cup \mathbb{A}_I$, where $\mathbb{A}_T$ and $\mathbb{A}_I$ represent tangible assets and intangible assets, respectively. (It is to be noted that here the complexity of the asset life cycle has not been considered.) Besides, within the BC context by claiming a transaction that happened does not make it a valid transaction. Since in BC, validity depicts the status when checking of integrity conditions (such as cryptographic primitives (e.g., generally digital signature) of the transaction initiator) by authorized entities have been already performed. This also determines that if a transaction is considered as a part of a specific transaction record, then $t_{r_i} \in T_R$, *where* $t_{r_i} \iff$ *valid*(T_i). (It is to be noted that this assumption depicts the uncomplicated version in the hierarchy of validation. E.g., block, ledger record, can also be validated.)
T_R Transaction Record. It is a data structure used to document the result of T. Moreover, we assume that $T_R \mapsto B$ *iff* $\exists\ t_{r_i} \in T_R$ (*valid* $(T_i) \wedge$ *confirm* (T_i)), which simply means T_R will only be referred to or included, in a specific block (for simplicity, we mention block rather than block data), if and only if it consists of valid and confirmed T. Here, we are assuming that the confirmation process for block and transaction will be determined distinguishably.
C(B) Configuration Block. It is a first block that stores various functionalities of a particular blockchain, such as governing procedures, and it is the only block that is not cryptographically linked to any previous block, which means $\nexists\ C(B) \prec B \wedge C(B)_H \mapsto B_H$.
B_T Block Trail. The block trail of block B, denoted as $B_T(B)$, refers to the direct chain of preceding blocks (D) of B from the Configuration block C(B), i.e., $B_T(B) = B_T(D(B)) \cup B$, where $B_T(C(B)) = C(B)$. Moreover, $B_T(B)$ will always be a non-empty finite set represented as $B_T(B) = \{b_{t_i} \mid i \in \mathbb{N}^+\}$, and $B_T(B)$ will always be unique and immutable.

(Continued)

Table 1. Continued

M, A Consensus Mechanism. There are different consensus mechanisms that are adopted by various blockchains, and for simplicity, two fundamental properties should be persuaded while establishing consensus. These two properties are as follows:
We define the decidable function M that decides (i.e., Boolean decision value) whether an arbitrary block B is a valid successor of the block trail $B_T(B)$ in a bounded time interval ΔT (here, ΔT can vary based on the requirement of the Blockchains). Hence, M can be depicted as $M : \mathbb{B} \times \mathbb{B}^* \rightarrow \{0, 1\}$ (where $\mathbb{B}$ is the finite set of predecessor blocks before this consensus mechanism, and $\mathbb{B}^*$ is the set of all possible arbitrary blocks that are to be appended in the chain of predecessor blocks).

$$\mathrm{M}\left(B_T(\mathrm{B}), B_{new}\right) = \begin{cases} 1, & \textit{if } B_{new} \textit{ is a valid descendent of } B_T(\mathrm{B}) \\ 0, & \textit{Otherwise} \end{cases}$$

We define another decidable function A, which takes a finite set of arbitrary leaf blocks (i.e, those data blocks that are yet to be appended in the main blockchain) as input and returns one distinctive leaf block. Hence, A can be represented as, $A : \mathbb{B}^* \rightarrow \mathbb{B} | \mathbb{B} \subseteq \mathbb{B}^*$ (where $\mathbb{B}^*$ is the finite set of arbitrary leaf blocks and $\mathbb{B}$ is the resultant preferred blocks). The function A decides what are the preferred leaf blocks among a finite set of arbitrary leaf blocks based on the specified chain rule. The objective of this property is that all the blocks have a common prefix chain. From the above-discussed specifications, we can introduce the two propositions for interoperability among unconnected heterogeneous blockchains that are not limited to a set of specific blockchains.

Proposition 1 (Swapping Interoperability)—*For any asset $a_1 \in BC_1$ and $a_2 \in BC_2$ in a particular system state, the existence of a transaction record T_R^{Swap} such that $T_R^{Swap} \mapsto BC_1 \Leftrightarrow T_R^{Swap} \mapsto BC_2$ implies (i) there exists a transaction T_{Swap} that is able to transform the current system states of both BC_1 and BC_2 into a new consistent system state (i.e., $a_1 \in BC_2 \wedge a_2 \in BC_1$) in the bounded time interval ΔT; (ii) T_{Swap} should be considered as final when it can be be ensured that both desired system states gets achieved. It is interpreted as $(T_{Swap}^{final}) \implies ((S(BC_1) \mapsto (S(BC_1))') \wedge (S(BC_2) \mapsto (S(BC_2))'))$; (iii) there exists consensus mechanism that can successfully ensure that integrity conditions of $T_{Swap} \in T_R^{Swap}$ have been checked on the respective blockchains (i.e, in this case BC_1 and BC_2) simultaneously; (iv) B_{Swap} has the access to the block trail as an arbitrary block on both BC_1 and BC_2, where in this case $B_{new} == B_{Swap}$.*

Proposition 2 (Transferring Interoperability)–*For any asset $a \in BC_1$, the existence of $a_{Proof} \in BC_2 \Leftrightarrow a \in BC_1$ implies (i) access to the block trail of the block encompassing a on BC_2; (ii) $\exists$ Consensus C_2 ($C_2 \in BC_2$) that can mimic consensus (C_1) $\in BC_1$. Moreover, for any asset $a \in BC_1$ in a particular system state, the existence of transaction record T_R^{Trans} such that $T_R^{Tran} \mapsto BC_1 \Leftrightarrow T_R^{Tran} \mapsto BC_2$ implies (i) there exists a transaction T_{Tran} that is able to transform the current system states of both BC_1 and BC_2 into a new consistent system state (i.e., where $\exists$ a ($a \in BC_2 \wedge a \notin BC_1$)) in the bounded time interval ΔT; (ii) T_{Tran} should be considered as final when it can be be ensured that both desired system states are achieved. It is interpreted as $(T_{Tran}^{final}) \implies ((S(BC_1) \mapsto (S(BC_1))') \wedge (S(BC_2) \mapsto (S(BC_2))'))$.*

1.2 Our Contribution

To the best of our knowledge, this article is the first attempt that comprehensively and systematically reviews blockchain interoperability aspects, where systematic review means that it begins

by highlighting various blockchain aspects and, thenceforth, explores the importance of implementing blockchain interoperability by describing its potential applications, taxonomy, and state-of-the-art solutions. Comprehensive review means that it will cover blockchain and blockchain interoperability according to varying degrees of scope and depth to fill the research gaps in the literature. The highlights of the various aspects covered in literature and the broad perspectives that readers can find in this survey are summarized in Table 1 of the online appendix (Appendix A). Based on the highlighted comparisons (Appendix A), the contributions of this article are manifold and are listed below.

- This article comprehensively discusses the need and concept of BI in a delineate manner as compared to existing survey papers (see Appendix A).
- This article systematically discusses the principles behind blockchain, with an emphasis on generic blockchain structure instead of typical bitcoin ledgers (see Appendices B and C).
- Compared to the literature, it provides an in-depth comparison of how existing blockchain-based platforms have different requirements, which potentially limits the communication among these distinguished platforms (Section 2.2).
- It proposes a more comprehensive research taxonomy of blockchain by considering variations in its standard working principles and approaches (Section 2.3).
- It contemplates a comprehensive possibility of different applications and pinpoints several use cases ranging from governance to smart cities (see Appendix D).
- It proposes an abstract reference multi-layer architecture for enabling interoperability among incompatible heterogeneous blockchains by using similar design principles that are used as the basis in the OSI model (Section 3).
- It proposes an in-depth taxonomy of BI based on the empirical approach leveraging state-of-the-art approaches and other possible solutions (Section 3.2).
- It provides a comprehensive discussion on the implemented state-of-the-art BI research and also highlights comparison among them (Section 4).
- Finally, it untangles the challenges and future research directions associated with achieving interoperability among blockchains (Section 5).

Although the originality of this survey is multi-fold as highlighted above, the ultimate goal is to familiarize readers with the requirement of the interoperable blockchains to make an understanding for investigating and developing solutions for integrating heterogeneous blockchains. Moreover, with these contributions, our survey will try to provide clarity on the following research questions:

- Why is there an imperative need for carrying out research in the field of BI?
- What benefits could come up with the evolution of BI?
- Which potential applications will be feasible due to the concept of BI?
- What are the challenges in the way of accommodating interoperability in blockchain technology?

1.3 Organization of the Article

We organize this survey in a systematic and top-down manner, beginning with an overview of the generalized concepts associated with blockchain and pin-pointing our emphasis on BI. In the online appendix (Appendix A), we begin by pointing out the aspects covered in existing survey papers and highlight those aspects that readers will find in this article and how this survey bridges the research gap in the area of BI. Section 2 presents the working principles of blockchain technology and proposes a research taxonomy. This section also provides an outline of its underlying

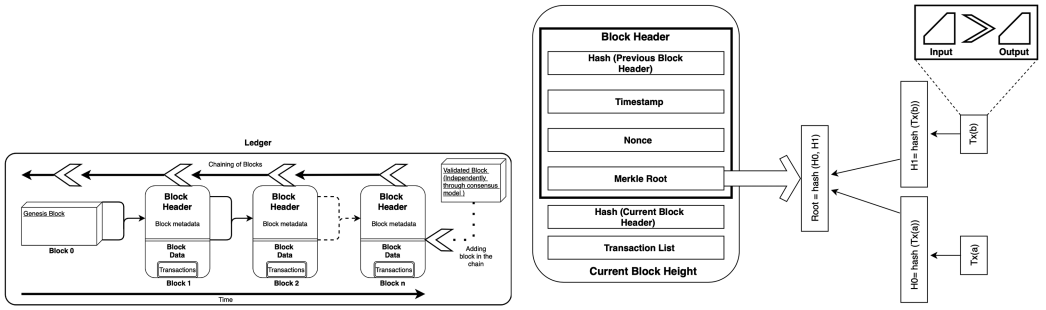

Fig. 3. Simplified representation of logical structure of a typical blockchain and high-level representation of the generic block structure.

fundamentals, features, along with highlighting and comparing its popular platforms and consensus algorithms. In the online appendix (Appendix D), we briefly discuss the potential opportunities for BI and blockchain, and by enabling BI, what are the key possible applications area that can be implemented using blockchain technology. Section 3 discusses the proposed layered meta-architecture for BI and, thenceforth, presents a research taxonomy for BI based on the empirical approach. Section 4 presents an in-depth discussion and comparison of various state-of-the-art approaches, which implement interoperability from different perspectives. Section 5 presents open research issues and challenges that will be faced in BI and highlights future research directions that can foster the solutions at various levels to connect the current paradigm of disparate blockchains. Section 6 concludes this survey article. For assistance regarding the acronyms that appeared throughout this article, readers can refer to the electronic appendix (see Appendix A).

2 BLOCKCHAIN WORKING PRINCIPLES AND TAXONOMY

For understanding the potential of interoperable blockchains, it is important to comprehend the functioning of blockchains and how blockchain features help in achieving security, transparency, immutability, and integrity. Therefore, this section presents a preliminary analysis of blockchain, which contributes to the background for further consideration on the potential of interoperability in blockchain scenario. In this section, we summarize the features and prominent platforms of blockchain, and the blockchain working mechanism is discussed in the electronic appendix (see Appendix B and Appendix C). Subsequently, we propose an in-depth research taxonomy for blockchain that provides a hierarchical classification across various blockchain configurations. Thereafter, we succinctly describe the contribution of consensus mechanism through epitomizing various consensus algorithms according to their working mechanism.

2.1 Overview of Blockchain Fundamentals

In general, blockchain is considered as a complex technology; however, it can be easily understood by analyzing every component independently. At the conceptual level, blockchains make use of computer science mechanisms (i.e., distributed networking, hashing, data structure, digital signature, and cryptography) and incorporate these concepts with financial primitives (i.e., ledgers and transactions). Put simply, Blockchain is composed of distinguished technologies/concepts that are integrated into a specific fashion to provide effective functioning required by the blockchain systems, as depicted in Figure 3 and discussed in detail in the online appendix (see Appendix B).

2.2 Platforms and Principles of Blockchain

The potential of blockchain can transform the industries/digital wave globally, which makes it more than just a technology for cryptocurrencies. What makes blockchain a disruptive technology? The oversimplified answer is its unique and innovative features. Some of the identified features are highlighted in the online appendix (see Appendix C). Besides, for addressing the interoperability issue, there is also a need to understand the working mechanism of individual blockchain platforms. There were more than 1,500 active cryptocurrencies in the year 2018 and among them, around 500 had more than 10M dollars of market capitalization [84]. In addition, there are more than a dozen of blockchain platforms that are being used for various decentralized use-cases [4]. For the scope and domain of this article, well-known and relevant platforms from each year based on the blockchain evolution are identified and reviewed. Accordingly, Table 2 summarizes a systematic comparison of these platforms according to their capabilities and characteristics. The objective of this table is to compare these blockchain platforms by considering features that are appropriate to provide a reference for specific requirements coming across while designing interoperability applications. Hence, this systematic comparison can provide a reference to researchers for developing specific novel solutions for fostering the concept of blockchain interoperability. In addition, these platforms are the ultimate guide to address constraints and challenges raised by individual blockchain platforms, including different ledger accessibility, block time, consensus mechanisms, and hash techniques. We also analyze this comparison in a way, which leads towards proposing a detailed taxonomy for blockchain technology that will be discussed in the next sub-section.

2.3 Taxonomy of Blockchain

The proposed research taxonomy of blockchain, as shown in Figure 4, is intended to help in understanding the concept of blockchain systematically. Our approach for classifying blockchain fits better in the current state-of-the-art related to blockchain technology. Therefore, considering heterogeneity in the blockchain, we begin with the coarse-grained classification and present an in-depth analysis based on its governing mechanisms and chain structure. The detailed analysis of this classification is discussed as follows:

2.3.1 Based on Governance Model for Consensus Mechanism. The notion of "Governance" can have various perspectives, but primarily it is described as governance "of" or "to" the infrastructure [96]. Both provide a road-map to the software, organizations, and projects, for determining the procedure to compose decisions. Based on the practical cooperation perspective, the governance model can range from centralized to decentralized, with both having their heterogeneous structures. Decentralized transparent governance is a paramount aspect for the successful implementation of blockchain technology. Although blockchain technology is based on decentralized or partially centralized mechanisms, its way of governance is different from conventional approaches [81]. Moreover, the scope of the notion of "blockchain governance" is very vast, but concerning BI perspective, this article limits the meaning of blockchain governance based on three access control decisions: (1) which nodes have reachability to the ledger?; (2) what permissions are granted to the participating nodes?; and, most importantly, (3) is the consensus mechanism accessible to the nodes, who are willing to participate? The first rule typically determines that the ledger construct adheres to governance rules that are enforced to the participating nodes and often decides which nodes have the permission to access the ledger. Followed by this rule, the second rule describes a set of permissions provided to the nodes for access and control to the data. These granted permissions may differ based on the role of the node in the blockchain. Last, consensus mechanism is an inherent issue to blockchain governance, as it is an alternative for trust by providing methods for effective decentralized governance. In other words, it can be understood as the

Table 2. Comparison of Blockchain-based Platforms Based on Their Capabilities and Characteristics

Platform Year [Ref.]	Brief summary	Capabilities and characteristics					
		Ledger accessibility	Block-time (per min)	Consensus	Hash algorithm	Native symbol	Applications
Bitcoin 2009 [90]	Decentralized digital cryptocurrency that uses public distributed ledger.	Public	10	PoW	SHA-256 double iterations	BTC	Financial institutions, and digital market
Name coin 2011 [30]	Cryptocurrency, which was originally forked from bitcoin, and stores data within its own blockchain database.	Public	10	PoW	SHA-256 double iterations	NMC	
Litecoin 2011 [98]	It is an open-source decentralized network that provides faster transaction confirmation than Bitcoin.	Public	2.5	PoW	Scrypt	LTC	Financial institutions, digital market, and transportation
Peercoin 2012 [79]	It was the first cryptocurrency that used both PoW and PoS consensus algorithms, and also referred as PPcoin.	Public	8.5	PoW and PoS	SHA-256 double iterations	PPCoin	Financial institutions, and digital market
Ripple 2012 [77]	It is a gross settlement system that supports real-time transfer of various values, such as fiat currency, mobile minutes, commodities, etc.	Private	NA	RPCA	ECDSA	XRP	
Primecoin 2013 [72]	It introduces a unique form of PoW-based system, (i.e., search chains of prime numbers), and these chains are also known as the bi-twin chains and Cunningham chains.	Public	Approx. 1	PoW	Cunningham chain-based	XPM	
Nxt 2013 [59]	It is a flexible open source payment network that uses PoS as its consensus algorithm.	Public	1	PoS	SHA-256 double iterations	NXT	
Dogecoin 2013 [32]	It is a flexible open source payment network that uses PoS as its consensus algorithm; during its launch, it was funded with around one billion coins.	Public	1	PoW	Scrypt	XDG	
Counterparty 2014 [37] [48]	It is a peer-to-peer platform that has a native currency, referred as XCP; it uses proof-of-burn as its consensus protocol.	Public	10	PoB	SHA-256	XCP	Financial institutions, digital market, and transportation
Dash 2014 [19]	This cryptocurrency is a form of decentralized autonomous organization that is run by master nodes (i.e., subset users). It generally permits transactions that are untraceable, and it is forked from the bitcoin.	Private	2.5	PoW and Proof of Service	X11	Dash	
Monero 2014 [43]	The primary focus of this cryptocurrency is on privacy, which means that this cryptocurrency provides a platform in which anybody can send or broadcast transactions, but no outside entity will able to trace the origin of transaction.	Private	2	PoW	CryptoNight	XMR	
Monax 2014 [20]	It provides an open-source platform for developing smart contract-based applications, and it is considered as the first client that uses permissioned blockchain. Currently, it is contributing in the Hyperledger burrow framework.	NA	NA	NA	NA	NA	Supports various private and public use-cases
Stellar 2014 [41]	It is an open source protocol that is supported by non-profit organization, which is developed for allowing cross-border transactions.	Private	0.06	SCP	SCP	XLM	Banking institutions
Ethereum 2015 [16]	It is an open source blockchain platform, which provides an EVM for running smart contracts. Instruction set on the virtual machine is Turing complete as compared to the Bitcoin script.	Public, but can be used as a private	0.16-0.31	PoS	Ethash	ETH	Supports various private and public use-cases
Enigma 2015 [89]	This is an off-chain network protocol, which maintains distributed hash table for storing data references instead of the data itself. This protocol is fundamentally aiming to increase blockchain scalability and providing privacy in the blockchain.	Private	NA	Enigma	NA	ENG	Privacy concerned use-cases

(Continued)

Table 2. Continued

Platform Year [Ref.]	Brief summary	Capabilities and characteristics					
		Ledger accessibility	Block-time (per min)	Consensus	Hash algorithm	Native symbol	Applications
PotCoin 2015 [13]	It was originally considered as the fork of Litecoin, the goal of which is to provide standard form for the payment in the cannabis industry. It uses PoS-Velocity as its consensus algorithm.	Private	0.67	PoS	Scrypt	POT	Cannabis industry
Hyperledger 2015 [9]	Hyperledger project is open-source project that aims to contribute by providing various kinds of blockchain frameworks and tools. It has obtained contributions from Intel, IBM, and SAP Ariba, for its collaborative development.	Pluggable	NA	Pluggable	NA	NA	Supports various private and public use-cases
Zcash 2016 [71]	It is a cryptocurrency with a total number of 21M units, and transactions are controlled by a t-addr or zk-SNARKs.	Public	1.25	PoW	Equihash	ZEC	Financial institutions, and digital market
Corda 2016 [29]	It is based on DLT, and it maintains shared ledgers for eliminating the need of constantly maintaining the ledgers after every new transaction.	Private	NA	Pluggable	NA	NA	Supports various private and public use-cases

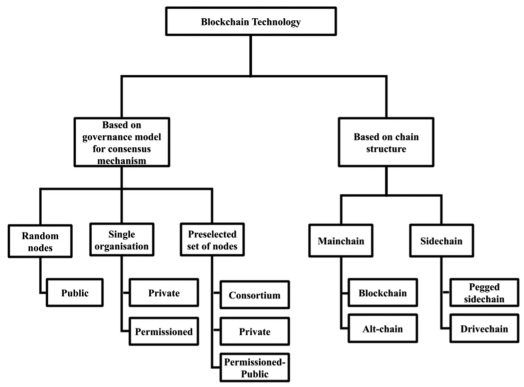

Fig. 4. Blockchain taxonomy–A typical representation of classification of blockchain.

backbone of the blockchain governance, since blockchain will able to function only if there is a valid consensus. Moreover, proof of liveness, synchronization, consistency, safety, and security are some of the prominent features that are ensured by the consensus mechanism. Concerning distinctive requirements, blockchain-based platforms use different consensus algorithms. Table 3 summarizes the popular ways of establishing consensus in the blockchain. Although the scope of utilization of these algorithms is limited to a siloed blockchain-based network, their underlying concepts can be used to develop consensus mechanisms for an interoperable blockchain-based network. Based on the above-discussed blockchain governance scope, this article broadly considers three aspects that can come under this category, as shown in Figure 4, and are discussed as follows:

- **Random nodes**–In this aspect, no node has specific privilege over other nodes in access control for ledge construct or managing the consensus, as the network is open for random node contribution in the blockchain. It only requires that participating nodes adhere to the underlying consensus mechanism for their active involvement in the decision-making process. In simpler terms, random public nodes can send and receive transactions; however, in the process of considering the transaction valid, it must be validated by each of the authorized nodes. Anyone can submit their intention for participation as an authorized node; however, in the process of considering them as authorized nodes, it must follow or implement the

Table 3. Comparison of Various Consensus Algorithms in Blockchain Technology

Algorithm	Brief description	Principle of agreement on information	Tolerated power of the adversary nodes	Applications (Preferably)
Vote-based				
RPCA [10]	It works by trusting subnetworks within the networks. This trust model can further be miniaturized by trusting on member nodes. This algorithm is robust and fast in nature, and also once consensus is closed, the current ledger known as the last-closed ledger.	By using Unique Node List	79% of the nodes or 20% of Unique Node List	Cryptocurrency
SCP [45]	This protocol is constructed for the federated byzantine algorithm, and it also supports open membership model.	By using Federated Voting	$T > N/2$, where T is quorum size and n is number of nodes that shows fail-stop behavior	Financial transactions
pBFT [109]	It handles Byzantine faults by considering that manipulated data is proliferated by autonomous nodes, and failure also happen in autonomous nodes. It is useful for those consortium blockchains where nodes are partially trusted.	By performing mathematical operations	Less than 33.3% replicas	Digital assets, financial services, trade finance, healthcare, and insurance
Raft [70]	It implements a substantial amount of coherence for scale down the number of states that must be acknowledged, and it also distinguishes between features, including safety, log replication, and leader election.	By using randomized timers	t < n/2, i.e., 49% of the nodes	IoT, financial and smart contracts
Quorum-Chain [36]	It uses the trust model to define a set of voter nodes and specifies random number of block-maker nodes that are well-known among all nodes.	By using smart contracts	t < n/2, i.e., 49% of the nodes	Financial use-cases
YAC [53]	It is a novel BFT consensus algorithm that uses voting for proposing block.	By using peer nodes	$FP < 3P + 1$, means faulty peer (FP) should be less than 3P+1 peer nodes	IoT and Infrastructure projects
Proof-based				
PoW [51]	In this algorithm, the node can be chosen as a leader if it will be able to solve a particular problem.	By solving difficulty of hash	Less than 25% computing power	Cryptocurrency and Financial Transactions
PoL [50]	It utilizes two functions that include PoLMine and PoL-Round for the purpose of mining the new block, and new chain, respectively.	Depends upon the luck value	Less than 50% processing power	Cryptocurrency
PoET [15]	This is considered as the effective form of PoW that gets rid from mining-intensive process and re-instantiate it with the randomized timer system.	Depends upon the shortest time	if less than $\theta(logn/logn)$ portion of the participating nodes got compromised	Real-world applications
PoS [23]	This algorithm lies on the idea of how much capital nodes hold, and, accordingly, their mining power gets decided.	By owning a certain amount of stake	Control over less than 51% of overall stake	Smart contracts, Cryptocurrency
PoB [24]	It is based on the fundamental of "destroying" and "burning" the coins and can be seen as an alternative to the PoW, as it is an energy-efficient algorithm.	Depends upon the quantity of coins	Less than 25% computing power	Cryptocurrency
PoA [92]	It comes with a hybrid approach that integrates the elements of PoW and PoS. In the mining process, it extracts template blocks (i.e., those do not consist of transaction) and then it switches to PoS.	By solving difficulty of hash	Less than 51% of online stake	Cryptocurrency
DPoS [68]	In this algorithm, stakeholders assign their work to delegates, which are responsible for accomplishing consensus during the creation and validation of recent blocks.	By owning a certain amount of stake	Number of validators is less than 51%	Cryptocurrency, Smart contracts
PoI [21]	It considers the eligibility according to the investment of nodes and selects nodes for updating the blockchain according to its proportion of contribution to the network.	Depends upon the highest priority	Less than 51% importance	IoT environments, real-world applications, cryptocurrency
PoSp [31]	It decides the legitimacy of nodes according to allocation of a certain non-trivial amount of disk space or memory for solving the challenge.	Depends upon the storage of plots	Less than 25% storage	Real-world applications, cryptocurrency, Smart Contracts

consensus algorithm rules. Some of the networks support an incentivizing mechanism to promote participation in the consensus mechanism. Depending on the blockchain developers, they can choose any distinguished consensus algorithm as its underlying mechanism [62]. These underlying mechanisms work as the governing policies, as they decide the rules and regulations for constructing ledger or validating transactions. Generally, the networks that come under this category are referred to as public blockchain networks, as they have similar fundamental functionalities, such as public participation and other governance policies.

- **Single organization** – This aspect limits blockchain governance to a single organization, and that organization is solely responsible for policy control and decisions such as participant node's role, their access control rights, and consensus mechanism management [44]. Blockchain-based in this category consumes less energy due to a higher transaction approval rate, as the organization participating nodes already have some level or complete trust among each other. Based on organization structure, and governance nature, this category can further be divided into two sub-categories: (i) private blockchain, and (ii) permissioned blockchain. In a private blockchain, nodes have to obtain appropriate permissions and authorization from a regulatory authority before their participation. Private blockchains are generally understood as partially decentralized due to their restrictive network model. However, a permissioned blockchain can be seen as a solution that approximately draws an orthogonal line between public and private blockchain by incorporating both blockchain best features into a single framework. In simpler terms, these networks are open for public participation, but participating nodes have to follow a pre-defined set of rules and regulations during their involvement.
- **Pre-selected set of nodes** – This aspect has various commonalities with previously discussed aspects, and it can be argued that this aspect can come under that categorization, where an organization may have a preselected set of nodes, or random nodes can form a preselected set of nodes. But, this aspect distinguishes itself by providing a more autonomous and less-permissive framework while maintaining agreed regulations. In this way, it fosters to development of a new blockchain governance structure, where random public nodes can become more inclusive in the underlying infrastructure network. Based on the on-chain governance or control over consensus mechanism, this aspect can also be further categorized: (i) Consortium [6], (ii) Private, (iii) Permissioned Public [96]. The idea of pre-selected nodes is to provide an alternative solution, where managing the access control operations is determined by an authorized node list, but to become part of that list is transparent and flexible. Consortium blockchain allows a group of organizations or entities to manage the consensus mechanism or other regulations. It may grant anyone read access or restricts it to a set of authorized nodes, but other governing policies should be determined through a set of authorized nodes. Although the working mechanism of public, private, and permissioned blockchain has been already discussed previously, all of them can adopt this aspect by following its distinguished features, along with their distinctive advantages.

2.3.2 Based on Chain Structure. From a database perspective, blockchain can be interpreted as a novel information management approach that provides secure distributed transaction management. In its initial design, it utilizes a single chain (preferably referred to as a mainchain) in its underlying framework. However, more recently a variety of blockchain solutions emerges, which utilizes multiple chains (preferably referred to as sidechain) on different levels to increase the performance metrics and other features. Amid the growing complexity in the interactions with blockchain and its data management, it will be significant to study and categorize these new forms of blockchain. Therefore, this category broadly covers the way of storing data in the blockchain (i.e., the level at which data blocks are being managed). A similar taxonomy is identified in Reference [18], in which authors studied different blockchain based on datalogical level. Developing sidechains concerns the infrastructure that distinguishes data based on its usage and accordingly decides the basis for the level of data structure. The flexibility of using different chains to store data depends upon the blockchain implementation. Although, different framework provides numerous ways to implement mainchain and sidechain, still they follow the fundamental properties of blockchain. The different chains and their implicit aspects are discussed below:

- **Main chain** – Sometimes, mainchain is considered as blockchain in the distributed ledger technology, as it contains valid block header of all the blocks. The process of selecting main chain in the blockchain technology can be viewed as similar to the process of electing the leader block among all the blocks [63]. In some platforms, longest chain is considered as the main chain of blockchain (e.g., longest chain rule in bitcoin). Although there are various ways of implementing main chain into DLT. However, in the current scenario, it can be categorized into two ways, including alt chain and blockchain. Here, blockchain should not be considered as the concept of blockchain technology, as it is the fundamental concept in the implementation of DLT as implemented by the Bitcoin. At the data logical level context, this blockchain term can also be understood as the distributed ledger that is used to store valid data blocks, transaction, and so on. Alt-chain is also referred as the main chain, but it presents solution to the current blockchain by implementing the alternative codebase [47]. Hence, these alt-chains can be viewed as an alternative to the fundamental bitcoin blockchain, as these chains are able to provide similar flexibility as of bitcoin blockchain. In this way, alt-chains supports various applications that are difficult to run on bitcoin blockchain. These applications are based on high speed and volume transactions, micro-payment control, auditing, privacy and resiliency against censorship, smart contracts, fast iteration, and experimentation.
- **Sidechain** – Sidechain can be better understood in context of road and transport. Hence, if the mainchain can be considered as the highway, then a sidechain can be contemplated as the road adjacent to highway that can be linked to the highway, if necessary [57]. The idea behind the sidechain comes into existence to enable scaling into the existing blockchain. Sidechain can be seen as a continuation of mainchain. Hence, it provides effortless mechanism for the exchange of assets between mainchain and sidechain to enhance the speed of transaction conformation. Despite the fact that sidechain enables bi-directional exchange of assets between sidechain and mainchain, they are isolated in nature. Sidechain provides a lot of benefits to the mainchain. For instance, sidechain has the knowledge of the history of the mainchain, but mainchain does not have any knowledge of the sidechain that enables sidechains to introduce extra layer of security (i.e., any fork in the mainchain will not directly affect sidechain) in the mainchain. It is achieved through implementing the technical changes with the help of these sidechains. Furthermore, sidechain can be categorized into two sub-categories that includes pegged sidechain and drivechain [76]. Pegged sidechain is nothing but a kind of sidechain that enables one or two-way peg mechanism for allowing interchange of data between sidechain and mainchain at a fixed deterministic rate and in a bi-directional way. In one-way pegged mechanism, for successful transfer of assets, the blockchain that is sending the asset has to destroy its asset publicly. However, receiver blockchain has to create the corresponding new asset. In two-way pegged sidechain, instead of creation and deletion of assets every time, locking mechanism is used on the sending blockchain for locking the exchanging asset, and cryptographic proof regarding the same asset is provided on the receiver blockchain. In this way, sidechains will not be able to create unauthorized assets. In fact, this two-way pegged sidechain mechanism can be achieved in two ways, including symmetric and asymmetric. The core behind the drivechain is similar to two-way pegged chain. However, it provides a control to the governing nodes in terms of when to unlock the assets and who are allowed to vote in this process. Another main feature of drivechain is that it enables interchange of data in a very low trust environment.

3 ARCHITECTURE AND TAXONOMY OF BLOCKCHAIN INTEROPERABILITY

Interoperability across a variety of application areas remains a challenge, and there lacks a well-defined approach that can be used as a cornerstone for developing domain-specific interoperable

solutions. As a result, organizations are willing to develop interoperable solutions, but they found it very ambiguous (what exactly interoperability refers to?) with respect to their application area. So, to determine an architecture for enabling interoperability among disparate blockchains and capture relationships among dependencies within architecture, we examine various working definitions of interoperability (e.g., BI definition in Section 1.1). For establishing a logical starting point, Interoperability can be defined as follows: It is the ability to establish communication among individual autonomous systems for exchanging information and services, despite having differences in various parameters (i.e., execution platform, programming language, interface, etc.). Moreover, we analyze interoperability from different perspectives, and likewise, the modular decomposition of interoperability using a layered model (determined using LISI [58] and LCIM [97] model) is discussed as follows:

- **Method 0: Isolated interoperability** – This method consists of isolated computing systems that have no way of establishing connection among them. Although, at the local level, standalone computing systems can be integrated manually for the purpose of data extraction and interaction among them.
- **Method 1: Network interoperability** – Networks provided by blockchain will continue to be distributed, heterogeneous, multi-organization, and multi-service. Different from conventional distributed systems, blockchain generally relies on various consensus algorithms and networking technologies that require more resources and availability. The method of network interoperability will provide mechanisms for enabling seamless end-to-end connectivity between systems in heterogeneous blockchain networks.
- **Method 2: Structural interoperability** – Structural interoperability can be referred as the syntactic interoperability that focuses on the data structure as an object of integration irrespective of the format. Since basic properties of the data structure (i.e., data formats and its definitions) are created by the developers of the individual systems at local level, which results in data not operationally compatible with each other. Thus, an architectural design is required for providing an interoperability among incompatible data structures [74]. Hence, this method illustrates the ability of data to be reused and accessible by involved parties by addressing the issues caused by different purposes, representations, and approaches.
- **Method 3: Semantic interoperability** – Semantic incompatibility can be understood in the way that the data model and information model may have different understanding and operational procedures. Moreover, in some cases, the semantic differences develop when an old procedure is used for new purpose and as a result, incorrect information may be arbitrated among systems. Hence, semantic interoperable model provides a mechanism for developers that is able to interconnect among these semantically different models [75, 102]. This mechanism ensures that the meaning of the exchanged information between the provider and the requester have a common meaning.
- **Method 4: Specification interoperability** – Semantic level interoperability models will not be able to enumerate the differences in the properties (i.e., such as array accessing mechanism or float-point precisions) of the object. Hence, the purpose of the specification interoperability model is to extend the semantic interoperability model by offering several advantages in terms of higher-level of integration. It assists in the process of information hiding, and hence it can successfully decrease the dependency on low-level interoperability [67, 78]. Moreover, it also broadens the range of participating programming languages.
- **Method 5: Platform interoperability** – Due to the flexibility in selecting blockchain framework and consensus mechanisms, blockchain faces various issues in terms of platform interoperability. There are various different platforms developed for specific blockchain

networks, such as Ethereum, Hyperledger initiative, and so on, each having several versions or platforms to provide services to the users. This inconsistency may cause an impediment for application developers in the process of developing cross-platform blockchain applications. The platform interoperability model enables cross-platform communication without gaining the extensive knowledge of any particular blockchain platform. Hence, heterogeneous platforms are federated to develop innovative blockchain applications, which can be used among all domains.

- **Method 6: Organizational Interoperability** – Nowadays, there are various organizations that support blockchain as their primary technology. However, they are utilizing different blockchain networks according to their needs. Despite having variety in their technical architecture, sometimes they have the need for establishing effective communication to exchange specific information. Organizational interoperability focuses on developing methods that can be achieved through the cooperation among different organizations having common goals. Although the method of organizational interoperability cannot be individually achieved without developing the specification, structural, and semantical interoperability methods.

In accordance with the scope of interoperability, the above discussion of the methods or models of interoperability can also be seen from granularity perspective. For instance, structure interoperability, semantic interoperability, and specification interoperability come under first level of granularity. The second granularity level focuses on network interoperability and platform interoperability. Organizational interoperability can be considered as the higher granularity level of interoperability. Along with these different methods of achieving interoperability, Joint Vision 2010 and Joint Vision 2020 [78] present three general perspectives of designing interoperability architecture, as shown in Figure 5.

For providing the correct set of standards, protocols, and decision rules while designing architecture, it is necessary to have a better understanding of these three perspectives that are discussed as follows:

- **Operational architecture** – It defines the description of the information flows, assigned responsibility, operational elements, and frequency of the exchanged information. Thus, it can be considered as the representation of the roles, nodes, processes, data exchange, and interrelationships.
- **System architecture** – It defines the location, physical connection, identity of the nodes, and networks that are associated with the exchanged information. Moreover, it specifies the parameters of system performance and design for specifying the operational requirements as per the definition of the technical architecture standards.
- **Technical architecture** – This architecture is used to define the interfaces, system services, and their relationships. It also provides the framework, which is used for deriving specifications and managing the system implementation.

3.1 Layered Reference Meta-architecture for Blockchain Interoperability

By taking the aforementioned three perspectives into consideration, we propose a generic high-level reference model for interoperable blockchains from the technical architecture point-of-view, as shown in Figure 6. For providing interoperability across chains, a framework somewhat similar to our proposed architecture has been presented in Reference [39]. However, their framework lacks in providing the layers technical perspective and addresses only the aforementioned challenges mentioned in their paper. Moreover, our proposed reference architecture is designed for

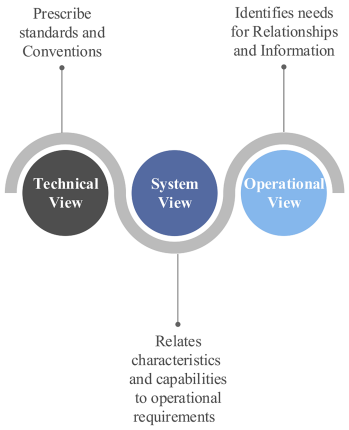

Fig. 5. Distinct perspectives to design an architecture.

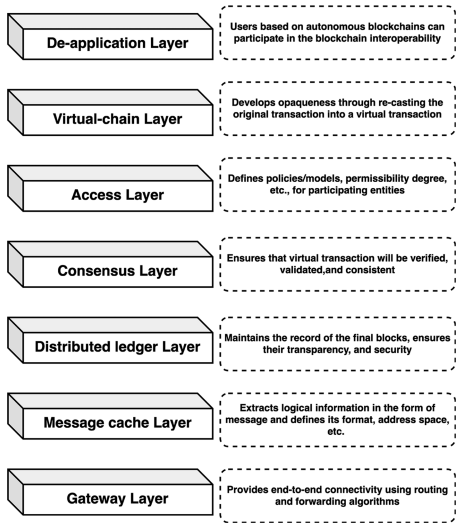

Fig. 6. Layered reference blockchain interoperability meta-architecture from technical perspective.

achieving interoperability under the proposed definition (Section 1.1) among heterogeneous blockchain-based systems, irrespective of their different implementation strategies and functionalities. It can be seen as a logical point to provide a clear understanding of identifying the specifications, protocols, structures, and standards that are required to implement BI and, most importantly, this architecture is not limited to specific platforms, vendors, services, or products. It is achieved on the assumption of separating the functionalities of cross-chain connecting protocols into seven distinguished layers. It means that this is a multi-layered cross-chain software reference architecture that separates the asset value from its underlying implementation (e.g., governance model) regardless of its source/destination ledger by describing the function and structure of interoperability protocols and standards. In this way, each blockchain involved in the interoperability can choose its own set of protocols, and it should not be concerned about other layers in the architecture. It will serve the purpose of the model, which is not that every blockchain network will have to strictly implement the same set of protocols, but to provide a standard model for troubleshooting the interoperability problems among blockchains. The motivation behind proposing a software reference architecture is adopted from the OSI model and Reference [38] to some extent, and this architecture is somewhat different from most of the state-of-the-art approaches [54, 61, 64, 66, 83, 94, 103]. Since their methods of implementing interoperability are limited to either a set of blockchains or just two blockchains. Moreover, they mandate the adoption of their protocols/operating systems to implement interoperability. Some of them achieve interoperability by separating business logic and implementing it through the logical and virtual layer [54, 66], and others achieve interoperability at the transaction level [61, 64, 83, 94, 103]. A detailed discussion of these projects is given in Section 4, and after analyzing them, this article reinterprets some layers/methods (besides their limitations) based on the scope of the proposed architecture. The comprehensive discussion for the layers in the proposed architecture and how they address the challenges are entailed below.

- **Gateway layer** – There are broadly two-fold arguments behind the inclusion of this layer in the architecture stack: One is motivated by the DARPA project [11, 14] in which the notion

of gateways is defined for connecting distinguishable networks, and the other is to provide end-to-end communication between disparate blockchains. Hence, the protocols designed under this layer should define the configuration that supports cross-blockchain routing for transferring messages. In Reference [38], the authors also described blockchain gateways as the key to support blockchain interoperability, although they did not mention any specific layer for accommodating these nodes. However, they presented significant reasoning and discussion regarding how gateway nodes (referred as interdomain gateways) can assist in achieving interoperability/interconnectivity. Similarly, this article believes that gateway nodes can play a significant role in interoperability; however, there are challenges ahead in their implementation, such as in selecting gateway nodes, as currently there exists no such mechanism, and how decentralization can be ensured. To address the challenge of transaction security highlighted in Reference [38], this layer will transfer the message, which does not represent the original transaction, and also the message is in encrypted form. In Reference [66], instead of using blockchain gateways, they relied upon the transport layer of the TCP/IP model, which is also a substantial argument; however, as already mentioned, their architecture imposes some restrictions. In Reference [39], somewhat similar to the functionalities supported by the proposed gateway layer, they designed the network layer for supporting the cross-chain communication; however, they also listed challenges in implementing this layer. In general, most of the layered schemes focus on developing a separate layer for handling the cross-blockchain transaction. Hence, this article emphasizes designing gateway-layer protocols for enabling end-to-end connectivity to transfer messages between disparate blockchains. While designing such protocols, this article suggests that using SDN gateways [93] can significantly increase the overall performance and provides an ease to deal with the interoperability regarding complex issues (e.g., without a centralized server, how to lookup for the trusted IP addresses). Other common suggestions include mutual attestation of message delivery, session key establishment, authentication, and so on, that should be adopted in the protocols.

- **Message cache layer** – This layer protocol should aim to define the message that consists of logical information (e.g., it should assist in routing, identification, authentication, non-repudiation), and also defined format should be supported by gateway-layer protocols. Notably, the notion of "message" proposes to cover blockchains implementing either token-based ledgers or any other system-based ledgers. Similar to this layer, in Reference [66], the authors proposed a message layer; however, that layer has different functionality, as it is primarily used for storing logical information about the transaction and message digests. Despite several dissimilarities, the proposed layer adopts several functionalities supported by the message layer implemented in Reference [66], and besides, this layer suggests several other features that it must provide. For instance, first, it argues that while defining the scope of the address space of the proposed message, it should not limit itself to a specific blockchain, and along with it, the value field in the message should be able to represent both fungible and non-fungible assets. Second, this message should have a standard syntax (e.g., "v.l.vtindex.bindex.mindex" should refer to message at index "mindex" in the block at index "bindex" of the distributed ledger layer in the virtual transaction at "vtindex," with the level specified in the "l" parameter on value "v"), so this message will be referable by different blockchains. A similar proposal for compound syntax is supported in Reference [66], where they want to provide opportunities for developing standard libraries. This message should also consist of metadata (e.g., OP_VALID), which have the potential to prove its validity among participating blockchains. Moreover, similar to the transaction format of any autonomous blockchain, this message format will also consist of a unique field that should

be able to identify the sender and receiver of the asset. For enhancing privacy, potential protocols can provide anonymous messages (e.g., using cryptographic primitives), since on distributed ledger layer, transparency-like features are ensured. However, on this layer, there are no such restrictions. For instance, it will utilize cryptographic primitives before sending them to the gateway layer; however, when this layer receives the encrypted message from the gateway layer, it will again utilize cryptographic primitives to decrypt the information. Hence, in this way, the encrypted message can securely travel among gateway nodes in the presence of malicious entities. This layer is seen to be similar to the off-chain layer or information out of the chain [66], due to its other suggested functionalities, such as until the information will be successfully exchanged among gateway layers, there will be no change in the state of the distributed ledger layer. In this way, there is no need to store temporary information on the distributed ledger layer and, also, interoperability can be achieved without any relay/side chains or trusted brokers.

- **Distributed ledger layer** – Security, transparency, immutability are a few of the utmost priority goals of any autonomous blockchain ecosystem. Hence, these kinds of features should be ensured in the interoperability scenario for building a level of trust and assurance among the participating blockchains. State-of-the-art projects also emphasized on developing separate security mechanisms in an interoperability scenario, although their approach to implement/enable is different from one another. For example, in References [8, 94], security concerns raised in sidechains due to their immature design, or any threats discovered by any malicious entity, will not affect the mainchain, as these kinds of challenges are confined to sidechains. In Reference [83], although they have adopted better security features, there exists a challenge within their network topology that can exploit their topology, since if there arises a problem with the security issue in the zone, there is no stated mechanism that validates the proposed transactions within the zones [66]. Now, considering the major goal (i.e., security), this layer aims to enable similar features in the interoperable blockchain scenario as provided by an individual blockchain. This layer's protocols will define the way to record the virtual block (i.e., created by virtual-chain layer and validated by consensus layer). In simple words, this layer will serve as a storage layer for the cross-blockchain transactions (e.g., virtual transactions) and hence, accountable for features such as traceability, tamper-resistance, transparency, and so on. On the contrary to a single blockchain, in this layer, the scope of the recorded transactions should not be limited to a single blockchain, which means that the transactions would be validated (i.e., referenced and reachable) in any participating blockchain. The potential protocols should also include all the operations (e.g., the global identifier for valid ledger entry) needed for implementing functionalities like distinguishability (as mentioned in the virtual-chain layer). For example, for the time, ignore the dichotomy of other layers. Let User A (on Blockchain A) transfer the ownership of a particular asset "X" to a User B (on Blockchain B). Now, after successfully recording the ownership of asset "X" on Blockchain B, the global transaction identifier will assist User B,= to sell that asset locally (on Blockchain B), or globally (other than Blockchain A). This layer is of significant importance; however, it is driven by other layer's functionalities as well. For example, the access layer determines governing model that decides the visibility of the ledger.
- **Consensus layer** – This layer specifies the protocols that will be accountable for verifying, validating, and ensuring the transaction's consistency, and it can be referred to as the consensus engine of the interoperable blockchain architecture. In Reference [39], the authors gave reasoning regarding cross-chain consensus protocols and, particularly, they reinterpreted the consensus protocols as verification protocols. In Reference [38], the authors suggested that the autonomous blockchains can interconnect using gateways

irrespective of their different underlying consensus protocols. For both cross-ledger transactions and normal transactions, in Reference [103], they have used relay chains as their primary mechanism to implement consensus among parachains. For providing security-related parameters in the hub and specifically during inter-zone transactions, the Cosmos project [83] implemented the Tendermint protocol as its consensus mechanism. In Reference [66], they did not specify any specific consensus protocol and instead of that, their proposed mechanism can deal with different consensus protocols, which can be considered one of the advantages. After analyzing these projects, it is noticed that although they deal with the challenge of consensus differently, directly or indirectly they recommend developing a mechanism/approach that can be implemented for an interoperable scenario. Based on this and also from empirical analysis, this article believes that in the case of trustless interoperability, implementing a consensus mechanism becomes a complex matter. However, this article wants to suggest that implementing a decentralized consensus might be a better way and for more reliable performance, nodes can be selected from the pool of already authorized nodes in the participating blockchains. The reasoning for this is that it will not interfere with the participating blockchain's internal consensus mechanism and still, it will be able to implement a decentralized governance model for consensus during interoperability. Currently, the existing consensus protocols do not support the suggested functionality; hence, there is a need to develop a similar/or better protocol by following this direction. In addition to the suggested functionality, the potential protocols should be able to work in a coordinated way with distributed ledger layer, access layer, and message cache layer. In the reference architecture stack, this layer might have two operational perspectives: (i) if the end-user is a sender; (ii) if the end-user is a receiver. From the sender's perspective, the implementation of consensus protocol can ensure that the virtual blocks (i.e., created by virtual chain layer) get validated and only after validation, this layer will be able to send the validated blocks to the distributed ledger layer. While from the receiver's perspective, it takes transactions directly from the message cache layer and after applying the consensus protocol, this layer sends the validated transactions to the distributed ledger layer.

- **Access layer** – This layer's protocols will ensure that there should be well-defined access control policies/models for participating entities (e.g., it assists in determining whether the same nodes can participate in two or more blockchains or not [38]). Moreover, it is necessary to determine the degree of permissibility for participating blockchains so data committed on one blockchain can be verified on another blockchain (as pointed out in the recommended definition). Along with deciding the level of permissibility, this layer can provide several other features that broadly include the degree of anonymity and security of the participating nodes and end-users. In Reference [66], the authors argued that business logic and control logic has to be separated from the transaction level. In Reference [38], the authors have also argued that these mentioned features are responsible to some extent for differentiating blockchains, although they did not suggest which logic needs to get separated to avoid this differentiation. Concerning both arguments, this layer can be seen as a way to distinguish between business logic and control logic and hence, this layer can also address the security challenges such as deciding that the same public key pair can be used in two or more distinct blockchains or not. For addressing the challenge of trustless interoperability, this layer's protocols should define the governing model, similar to the Bitcoin blockchain permission model (e.g., blockchains that want to support interoperability are allowed to participate openly, and also no central blockchain platform/service is needed for asset swapping/transferring). One can argue that what is the need for a separate access control layer, as individual blockchains have their governing models and security policies.

However, this article believes that these have a local scope, and also these are the primary roadblock in the way of interoperability. Hence, it is better to design new policies/models for BI. Based on this, requirements can be set up on a potential interface that connects the virtual-chain layer and consensus layer. And therefore, this interface can also be referred to as the Secure Interface Point.

- **Virtual-chain layer** – In this layer, an opaqueness is developed between the De-application layer and other layers through recasting the actual transaction into a virtual transaction (e.g., similar to the application-level transaction [38]). This virtual transaction is particularly built from extracting and then, logically separating the transaction information (e.g., business logic, asset value, metadata). Thus, it is an independent transaction that can accommodate multiple ledger-level transactions (i.e., where transactions can belong to different blockchains). This layer will ensure that newly created virtual transactions will be ordered in a defined sequence (e.g., based on the protocol), and the order of transactions will be independent of the order in their respective ledgers. Although the filtering and ordering layer [66] has a few similar functionalities to this layer, it also has several limitations (e.g., for ordering, only those transactions that have a compliant hash to the BPI accommodated in the virtual block, which serves as a limitation, because they are indirectly imposing participating blockchains to implement their infrastructure). On the contrary, this layer proposes to accommodate different protocols, with the suggestion that they can validate the ownership of the asset, and also they can distinguish between the participating blockchains (e.g., from naming, routing, and addressing perspective [38]). For example, protocols of this layer can develop mechanisms to create a block that contains virtual transactions or their hash; however, these protocols should not enforce any restrictions similar to the ones mentioned in Reference [66]. Moreover, a block can consist of any number of transactions and for ensuring distinguishability, the blocks can be placed at different levels (e.g., by using more than one chain) in distributed ledger layer, but only after a valid consensus. This layer will also support other functionalities (i.e., it all depends upon the type of service required), such as confirming that the intended data is received/transferred, probably by exchanging acknowledging messages similar to the TCP/IP model transport layer. To support these functionalities, what kind of protocols/services should be defined is discussed in the De-application layer. This layer should also define the format for the virtual transaction, which should be valid globally. It is critical, because most of the blockchains have different transaction formats, and this diversity can impede the information exchange among blockchains. For instance, Ethereum and Hyperledger sawtooth have different transaction formats, resulting in no direct communication among these blockchains. The same concern is also highlighted in Reference [39], where the authors suggested implementing a module, namely, data generator, that can play the role of middleware to enable direct interactions among different blockchains. From the reference architecture point of view, this layer supports protocols that act as a wrapper for the rest of the layers. In Reference [39], the authors propose a smart contract layer below the application layer, which extensively limits the purpose of their reference architecture. Moreover, they did not even clearly mention the purpose of this layer.
- **De-application layer** – This layer will be responsible for managing applications, regardless of their different underlying distributed ledger technologies, and will allow them to participate in the interoperability. Although the basic argument behind this layer is influenced by the application layer in the TCP/IP model. However, based on our scope, its principles are re-interpreted to support blockchain interoperability. This layer will define multiple services and protocols, which can be used by any application and will allow them to communicate with each other by working with the virtual chain layer to send and receive transactions. For

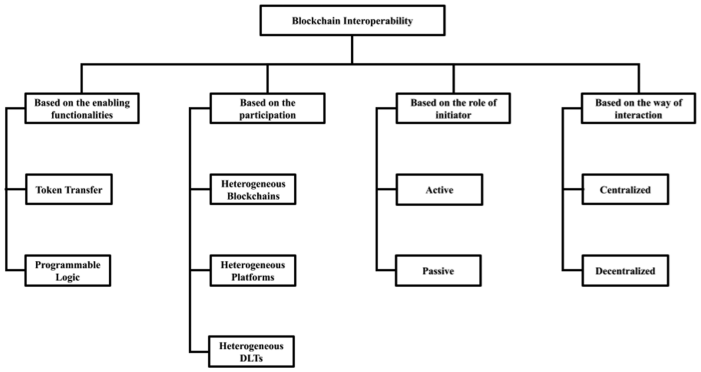

Fig. 7. Typical research taxonomy of blockchain interoperability according to empirical approach.

instance, a variety of services are described for addressing the challenges, such as different underlying block confirmation finality mechanisms (e.g., fast finality, probabilistic finality, deterministic finality) raised by the heterogeneous requirements of blockchain platforms and state-of-the-art blockchain interoperability projects (as they also support different finality, as depicted in Table 5). The notion of multiple protocols is described by considering several potential forms of blockchain interoperability (e.g., asset swapping protocols generally differ from asset transferring protocols). In terms of reliability and survivability, it should support methods that will ensure that the initiated transaction got confirmed and immutably recorded by the ledger. Similar to the TCP/IP model-based applications, this layer should define the awareness degree that an application must be aware of while communicating. This layer can be interpreted as a simplistic roadmap for developing technology-independent higher abstraction methods/services, as compared to the application layer defined in Reference [66]. Since, in Reference [66], they followed the approach of using a BPI, which primarily defines the rules that an application must follow before adding the messages in the Overledger. It indirectly limits the purpose of this layer, as compared to our purposed layer. There exists other similar literature that focus on developing an application layer. In Reference [38], they comprehensively illustrate the purpose of this layer by following the application layer of TCP/IP model, and in Reference [39], the authors provided an abstract description of this layer without depicting functioning and detailed purpose of this layer.

3.2 Taxonomy of Blockchain Interoperability

The diversity in the ongoing research and development of BI provides various ways of categorizing in this field. In this article, we present the research taxonomy for BI that gives intended classification based on the various factors that includes enabling functionalities, participation, role of initiator, and way of interaction, as shown in Figure 7, and are discussed as follows:

3.2.1 Based on Enabling Functionalities. To provide the means of connecting incompatible blockchains, developers have to substantially satisfy the functional requirements. During the creation of an entirely new blockchain, developers prefer to alter its functionalities to fulfill the specific requirements. This leads to potentially different functionalities that blockchain can utilize according to the use case scenario. Therefore, according to the functionalities that can be carried out during BI, there are two major categories in which BI can be achieved that are discussed as follows:

- **Token transfer** – This is one of the promising functions that is required in the process of establishing connection among heterogeneous blockchains. For a successful token transfer, it is necessary that tokens are destroyed on the source blockchain and successfully created on the destination blockchain [27, 28, 35, 60]. Moreover, the important point here to understand is that exchange of tokens is totally different from the process of transferring the tokens among heterogeneous blockchains. Since in the process of exchanging the tokens among heterogeneous blockchains, it is not necessary to destroy the token on the source chain, while in the token transfer, it is necessary. Moreover, in a typical scenario, this token transfer can be further categorized as direct token transfer and indirect token transfer. In indirect token transfer, interaction among different blockchains can be established through an intermediate platform. This platform is used for collecting the necessary prior knowledge, which is necessary for token transfer. In the indirect way of token transfer, efficiency of interaction is degraded. In the process of direct token transfer, tokens are transferred during the flow of communication without maintaining any prior knowledge. This category of BI is surely handled with the research directions that are trying to swap tokens between different blockchains.
- **Programmable logic** (according to cross-programmable logic interaction) – Nowadays, programmable logic is considered as an important aspect to identify the true potential of blockchain networks. This opens various possibilities in the application areas of the blockchain and is more popularly known as smart contract. Hence, this category deals with the realization of the possibilities of application-level BI. This application-level interoperability can sometimes be considered as the generic interoperability that is concerned more about passing the arbitrary information in a trustless way among heterogeneous blockchains. Smart contract interoperability not only describes the way of how smart contract interacts with each other; it also describes the way in which smart contracts can run on heterogeneous blockchains [101, 106]. Although, the most primary prerequisite for establishing cross-blockchain programmable logic interaction is to develop a cross-blockchain communication protocol for exchanging arbitrary information in a trustless way.

3.2.2 Based on Participation. In the current landscape, the proliferation of various DLTs, including blockchain, provides alternatives to the developers to choose an appropriate DLT platform according to their requirements. Accordingly, it can be depicted that there can be numerous ways for participation in BI. For instance, both source and destination belong to the different DLTs (i.e., one entity is working on blockchain and the other is working on the Tangle). Hence, to examine all the possible aspects of participation, they are discussed as follows:

- **Heterogeneous platforms** – State-of-the-art blockchain platform sophisticated features can be seen as a starting point for creating fragmentation in the current blockchain landscape. As a result, some of these platforms belong to the same underlying blockchain working principles (e.g., governance model for consensus). However, still these remain disparate from each other in terms of establishing a decentralized connection. For instance, both ethereum and bitcoin are based on a similar blockchain governance structure (e.g., in terms of incentivized public participation in the consensus process). However, despite their homogeneous underlying working principles, currently, there is no mechanism to establish decentralized communication (i.e., in a trustless environment) that is internally supported by these platforms. Although influenced by other dimensions of blockchain interoperability, there exists a few platforms and protocols that establish connectivity (with some dependencies) using trusted brokers, hash-locking, and atomic exchanges (detailed discussion is given in Section 4). One example of such protocols (sometimes these protocols are referred to as

cross-chain protocols) is provided by Zendoo [73], which allows communication among heterogeneous platforms having a homogeneous (i.e., in this case, platforms similar to bitcoin) working mechanism.

- **Heterogeneous blockchains** – Contrary to the previous categorization, this points out the notion of BI, which deals with blockchain platforms that have heterogeneous working principles. This means that among them, there exist no or very few similar underlying working mechanisms. For example, an application "A" implemented on platform "X" (e.g., based on public blockchains) and other application "B" implemented on platform "Y" (e.g., based on private blockchains) want to establish communication between them for exchanging assets. The interoperability required in these kinds of scenarios comes under this category, along with potential approaches (e.g., Quant Overledger [66]) commonly referred to as cross-blockchain protocols/platforms, as in this categorization communication needs to be established among two different blockchains, as compared to the previous category where communication needs to be established between two chains belonging to the same blockchain (e.g., sidechains and mainchain) or platforms having similar working principles.
- **Heterogeneous DLTs** – Blockchain and DLTs are often used interchangeably among academia and organizations. However, these concepts are distinctive (as discussed in Section 1). Hence, this article believes that blockchain is just one way to implement DLT, and also several technologies claim that their implementation criterion is somewhat or completely different from the blockchain. For example, some of them do not create batches of transactions into a block for validation purposes, such as every transaction is confirmed in real-time by the Corda platform [29]. Hence, considering the broader domain of DLTs, interoperability should not limit itself to the blockchain, and there should be mechanisms that can enable interoperability across the range of DLTs. However, currently, there is such interoperability solution, but based on the empirical analysis, this article suggests this categorization, and accordingly, it covers potential mechanisms for bridging the communication gap between these two technically different technologies. Its significance even gets increased due to unprecedented growth in the utilization of various DLTs across applications (e.g., use of DLTs to the IoT [108]).

3.2.3 Based on the Role of Initiator. This category is based on the flow of information between sender and receiver chain. In BI scenario, generally sender chain and receiver chain refer to different blockchains. Therefore, during the interaction, the flow of information will be considered from one blockchain to another blockchain. For ease of expression, this flow can be illustrated between the sender and receiver chain. The nodes that are of particular interest to the sending chain are referred as source nodes and based on the correlation of these nodes, the nodes selected on the receiving chain are referred as the destination nodes. Now, based on the role of the initiator in the process of establishing connection between different blockchains, interoperability can be classified into two modes—active and passive. A similar classification is done by Jin et al. [39], which classifies BI based on the mode of operation. This classification is discussed as follows:

- **Active Mode** – In active mode of interoperability, the initiator is in the role of the sender chain. In other words, in this mode of interoperability, source nodes are responsible to initiate the process of interaction between heterogeneous blockchains. In this mode, the transaction is issued by the source nodes, and after issuing the transaction successfully, they wait for the destination node's response. Although this mode of interoperability is difficult to implement, as it needs functional support of different blockchains, it can be considered better in terms of cost, as it can operate without the need of polling-based read method.

- **Passive Mode** – To achieve the goal of BI in the passive mode, receiver chain performs the role of the initiator. In this mode, the responsibility of the destination node is to continuously monitor the activities that are performed by the source nodes. In simple terms, it means that whenever a transaction will be issued by the source node, the destination node will have to take a correlated action. As a consequence, passive mode will certainly consume more resources, and hence, it is not considered as a cost-effective method of interoperability. However, it is a more convenient way of achieving BI as compared to active mode, especially in the situation where it is very difficult to make changes to the underlying system architecture of the sender chain. This is because of the fact that during the entire process of BI, sender blockchain has no need to perceive the existence of receiver blockchain. Hence, in this case where sender chain is not aware of the existence of the receiver chain, the flow of information will come out by polling-based read method.

3.2.4 Based on the way of Interaction. This category of BI primarily determines two ways of establishing communication among heterogeneous blockchains/platforms/DLTs. Since it is crucial to understand the connection method to figure out the dependencies in BI-based ecosystem. Put simply, the way of interaction categorization also helps in determining the security assumptions and other crucial features in BI. Furthermore, it is required to understand the characteristics of the methods of interaction. These methods are discussed as follows:

- **Centralized** – Under this BI categorization, it requires a central trusted entity (e.g., trusted broker or escrows), and this entity is responsible for establishing the connection among heterogeneous blockchains. The intention is to process the cross-blockchain/chain information through the functionalities backed by a single or set of centralized entities. In this method, first, the source chain sends the information to the centralized entity, then this intermediate entity processes the information and sends it to the destination chain/and vice versa. Concerning the centralized way of interaction, there are various challenges in terms of security and efficiency. Tampering of data is also easily feasible in this method, as an illegitimate entity has to only compromise the centralized system's security. This method is also highly inefficient in terms of scalability and can face a single-point-of-failure (e.g., some centralized platforms only support communication between two blockchains at a point in time). However, apart from several disadvantages, this method of interoperability is currently seen as a best-supported method, as there are various challenges ahead in the pathway of trustless interoperability.
- **Decentralized** – This article points out in various sections that the development of mechanisms/methods under this category should be prioritized rather than developing sidechains, escrows, or any other centralized way to enable BI as these direct/indirect centralized approaches may be an alternative solution. However, these do not align with one of the principal concepts of the blockchain (i.e., decentralization). Notably, these category methods ensure independent interoperability and hence, vision of a direct paradigm of interaction among heterogeneous blockchains. Atomic exchanges and Hash locking are two mechanisms using which several protocols achieve partial decentralization. However, still these approaches have a limited scope of interoperability. Hence, these can be seen as hybrid approaches. But in this article, we assume them under this categorization. This article found that, currently, there is no such approach/mechanism/architecture that supports truly decentralized interoperability. However, for covering potential approaches, this article proposed this categorization. The goals along with decentralization that can be satisfied by this category include no forking is required in existing blockchains, and also scalability, security, and performance will depend on the existing platforms rather than a centralized platform.

4 STATE-OF-THE-ART FOR BLOCKCHAIN INTEROPERABILITY

There is a prominent research question in the field of interoperable blockchains: "How can we achieve interoperability without modifying the fundamental mechanisms of blockchain?" At the time of writing this article, there exist a significant state-of-the-art contributions having different ways and goals for enabling interoperability among blockchains. Therefore, this section contributes to outlining these works, described as follows:

- **COSMOS** – It is a blockchain network architecture that connects various independent blockchains, called zones, which are powered by Tendermint consensus algorithm. The first zone in the architecture is referred as Cosmos Hub. An IBC protocol is used for establishing communication and transferring tokens between zones and hub. Coin packet is special kind of IBC packet that is used for transferring the token from one zone to another. Although there are various transaction types that are accepted by the cosmos hub, there are two primary kinds of transactions that are defined by IBC protocol: An IBCBlockCommitTx is a transaction used for proving that it is current block-hash, and another transaction IBCPacketTx is used to prove the publisher of the given packet. ABCI is an interface that connects Tendermint to the blockchain application written in any programming language. Tendermint supports both non-negative and positive amount of voting powers and possesses positive voting powers called validators. A locking mechanism and voting ($> 2/3$) decide security in Tendermint protocol. There are various advantages of the Cosmos ecosystems, such as validators can accept any kind of individual token or combination of different kinds of tokens as their fees for processing the transaction. Another advantage is that by allowing separate IBC transactions, receiving chain has the freedom to determine which packets get acknowledged, and simultaneously sending chain has also the freedom to choose the allowed number of outbound packets. Along with various advantages, Cosmos has various disadvantages, such as Hub blockchain in the Cosmos performs the role of the central ledger. Hence, if the security of the Hub compromises, then the whole ecosystem is under threat. Another disadvantage is that users have to take the responsibility of the sent tokens, as Hub does not have the ability to execute or verify transactions that are committed on various other zones, which clearly means that hub is not held accountable for the zone failure. For more in-depth study of the Cosmos, readers are suggested to refer to the Cosmos whitepaper [83].
- **POLKADOT** – Polkadot takes much of its architecture from Chain fibers, which was designed for executing interchain communication in the year 2014. Polkadot provides the underlying "parachains" that are used for executing validated data structure to provide trust-less interchain transactability and pooled security. It scales down its development risks by addressing much of its complexity at the middleware level and hence, it will be able to develop needed software application within an abridged time span. Polkadot network comprises of four roles: validator (i.e., basic and availability validator), collator, nominator, and fisherman. Consensus over the relay chain is achieved by the asynchronous BFT consensus algorithm that is motivated by Honey Badger Byzantine fault-tolerant algorithm and Tendermint algorithm. Along with this consensus algorithm, for incentivizing honest validators, PoS consensus algorithm is used. One of the main advantages of the polkadot architecture is that it uses Substrate as its underlying technology. It means that it provides a set of tools that assists in developing one's own blockchain. Another advantage of using Substrate is that it can support any language that has the ability to be compiled in web assembly, which provides flexibility to developers. Along with various advantages, Polkadot architecture has various disadvantages, such as relay chain validators are considered as the final authority over any upgrades in the parachain. Hence, if a situation occurs where validators continuously deny accepting the blocks in specific parachains, then the progress of parachains will

Table 4. Comparison among State-of-the-Art Projects for Providing Interoperability among Blockchains

Parameters→ Projects↓	Interoperability protocol	Security	Governance mechanism	Native token	Approach	Scalability
Cosmos [83]	IBC	Hubs and zones are responsible for their own security	Every zone has its own governance, and Hub has a different human readable constitution.	COIN	Relay	Use hubs to enable horizontal scaling
Polkadot [103]	ICMP	Shared Security Model	On-chain and approval voting mechanism where DOTs plays an important role; passive stakeholders consist of 24-member council.	DOT	Relay	Use sharding
Chainlink [34]	Off-chain Aggregation	Intel SGX and four security services are responsible for ensuring security	Smart contracts	LINK	Relay	Use attested off-chain computation
Wanchain [100]	Cross-chain communication	Hypothesis of Rational Participants	Distributed super financial market	Wancoin	Relay	Use Plasma/ Raiden
Interledger [64]	Interledger	Conditional transfer using SHA-256	BFT agreement	Not Defined	Hashed time-lock contract	Can achieve by making connector stateless
Virtualchain [54]	Human-in-the-protocol	Blockstack Auth	Stacks blockchain	Stacks	Relay	Using metadata
Quant Overledger [66]	Vendor-Independent Protocol	Protocol level	Filtering and Ordering layer contains a set of rules	Quant	Relay	Restricted by underlying ledgers
AION-1 [61]	Bridge and Connecting Network Protocol	Aion Virtual Machine	Self-governance	Token	Relay	Use multi-tier system
Blockchain Router [7]	Blockchain Router	BFT	Not defined	ZAC	Relay	Not clearly determined
Metronome [88]	Proof-of-exit	BFT	Self-governed through smart contracts	MET	Relay	Not clearly determined
Tast Project [27][25] [26]	Deterministic Witness	Not defined	Not defined	PAN	Relay	Not clearly determined
Sidechains [8, 94]	Authority Round and Tendermint	Not defined	Not defined	ERC20	Atomic swap / SPV proof	Using two-way peg
ION Interoperable Framework [40][2]	ION	Not defined	Any ledger governed by any consensus mechanism	ERC223	Relay	Not clearly determined

get stopped. For more in-depth study of the Polkadot, readers are suggested to refer to the Polkadot whitepaper [103].

- **ChainLink** – Chainlink is a decentralized oracle network that provides a bridge between off-chain and on-chain circumstances. In both the environments, its core design objective is to enable modular functionality to provide upgradation in different components [34]. Three steps responsible for on-chain workflow are: oracle selection, data reporting, and result aggregation. Current schema system that operates ChainLink is the JSON schema. There are three decentralized approaches that provide insurance against faulty nodes: distribution of data sources and oracles, and utilization of trusted hardware. For ensuring security in ChainLink, it employs four main security services: Contract-upgrade service, Certification service, Reputation system, and Validation system. In this way, ChainLink achieves secure decentralized interaction of smart contracts with resources that are external to the blockchain.

Table 5. Comparison among State-of-the-Art Projects for Providing Interoperability among Blockchains (Cont'd from Table 4)

Parameters→ Projects↓	Consensus algorithm	TPS	Bridging environment	Finality	Block time	Level of interoperability
Cosmos [83]	Any algorithm that compiles with ABCI specification; currently Tendermint is the only one that adheres the ABCI specification	Approx. up to 1,000	Hubs and zones	Fast finality	Approx. 6–7 sec	Any number of heterogeneous blockchains at a time can communicate with each other with the help of connector
Polkadot [103]	GRANDPA, Aurand, and Rhododendron	Approx. up to 1,500	Parachain and Relay chain	Provable finality	Approx. 6 sec	
Chainlink [34]	Based on threshold signature	Approx. up to 160,000	On-chain and off-chain	Near-fast finality	Approx. 5 min	
Wanchain [100]	Galaxy based on PoS	Approx. up to 3,000	Wanchain and supported blo ckchain	Probabilistic finality	Approx. 5–10 sec	Only two heterogeneous blockchains at a time can communicate with each other with the help of connector
Interledger [64]	Ripple Consensus Ledger	Approx. up to 3,000	Connector and blockchain	Absolute finality	Not tested	
Virtualchain [54]	Combination of PoW and PoB	Approx. up to 10/chain	Virtualchain and blockchain	Probabilistic finality	Not tested	
Quant Overledger [66]	Relay-chain consensus	Approx. up to 100,000	Virtualchain and blockchain	Probabilistic finality	Not tested	Any number of heterogeneous blockchains at a time can communicate with each other without connector
AION-1 [61]	Proof-of-intelligence	Approx. up to 100,000	Bridge between participating and connecting network	Probabilistic finality	Approx. 10 sec	Any number of heterogeneous blockchains at a time can communicate with each other using connector
Blockchain Router [7]	PoS	Not tested	Blockchain and subchains	Probabilistic finality	Not tested	Blockchain router enables communication among different blockchains by establishing connection via Crosschains
Metronome [88]	Combination of PoS and PoW	Not tested	Chainhop across blockchain	Probabilistic finality	NA	It uses the mechanism of cross-chain token, and interoperability can be achieved through import redemption and export receipt
Tast Project [27][25] [26]	Proof-of-intent	Not tested	Simple payment verification-based cross-chain	Probabilistic finality	Not tested	By transferring tokens with deterministic witnesses among blockchains in the decentralized way
Sidechains [8, 94]	Combination of self-defined consensus	Not tested	Private sidechain and blockchain	Probabilistic finality	Approx. 15 sec	Any number of blockchains can operate in parallel, by allowing execution of function calls that are able to manage the state of other sidechain
ION Interoperable Framework [40][2]	Clique Proof-of-authority	Not tested	Cross-chain smart contract	Immediate finality	Approx. 2 min	It can continuously execute atomic cross chain swaps with the help of decentralized exchanges

In the current version of ChainLink, there is a limitation that it is only built on ethereum blockchain.

- **Wanchain** – Wanchain addresses two main problems of BI. First is to ensure that the transferred value is no longer accessible in the sender blockchain, and second is the trust-less verification of the transaction on the sender blockchain itself. Hence, to solve these two problems, Wanchain uses storeman nodes for verifying transactions and successfully transferring the original values [100]. Wanchain supports solidity programming language-based smart contracts and private transactions that are based on the ring signatures. Wanchain is implemented in the GO programming language, called as Gwan. Gwan is also considered as the command line interface for the Wanchain. There is another interface to the Wanchain, known as iWan, that provides access to the wanchain test and main network. Wanchain

implemented Galaxy consensus mechanism based on the PoS protocol to provide efficient and secure development and governance of the network.

- **Quant overledger** – Overledger is an operating system that not only assists in the process of building multi-scale application on top of the existing applications, but also provides a platform for interconnecting existing blockchain networks [66]. By re-distributing tasks among different layers, it provides a specific platform that can accommodate different blockchain architectures regardless of their consensus mechanisms, addresses, and ledger implementation. It consists of four layers that include transaction layer, filtering and ordering layer, messaging layer, and application layer. Transaction layer consists of operations that are needed for providing consensus mechanism in heterogeneous platforms. Although, it is not possible to make transactions valid outside the scope of their ledger. Hence, transaction layer in the overledger architecture is described by distinctive isolated ledgers. Messaging layer can be considered as a logical layer, as it is used to collect all the pertinent information (i.e., metadata, transaction data, and smart contracts) from different ledgers. After successfully collecting the information, this layer is also responsible for storing all message digests and transaction information. Filtering and ordering layer is used for creating messages that are extracted from the transaction information stored in the messaging layer. Only the information that is referenced through the hash is filtered and ordered. This layer is also useful in developing the connections between messages of the messaging layer. Application layer interacts with the messages that are valid and has the requested message and signature.
- **Interledger** – It is a network of nodes that is able to route values across different autonomous networks. These nodes can have various roles that include sender, router, and receiver. Interledger Protocol suite (ILPv4 or ILPv6) plays an imperative role in the interledger network, as it defines a set of rules regarding ILPv4 packets. It is a request/response protocol suite, which is able to split payment information into multiple ILPv4 packets (i.e., Prepare, Reject, and Fulfil). This ILPv4 suite consists of four layers of protocols: Link, Transport, Application, and Interledger protocols. By utilizing hashed timelock agreements, interledger secures the payments, as participants use these hashlocks for carrying out the procedure of accounting with their peer nodes [64].
- **Virtualchain** – It is a kind of layer that can be installed on top of the existing blockchain networks for introducing new operations and functionality. Although the logic or operations for processing the transactions are stored in virtualchain layer, they are encoded in the metadata of valid transactions. Hence, it is not even necessary that the underlying blockchain is familiar with presence of virtual blockchain layer. Virtualchain library is used for defining the rules for the blockchain operations, and the accepted operations that are handled by the virtualchain layer are used for building the database [54]. This database is used to store the information related to global state of the blockchain system and state changes of the block.
- **AION-1** – The fundamental goal of the Aion project is to provide BI by reducing the dependency of central entity in the interoperable infrastructure. Aion-1 can be referred to as the public version of the blockchain [61]. In the bridging protocol, Byzantine Fault Tolerant algorithm is used, and initially the Zcash Equihash scheme is adapted as the mining algorithm. In the Aion ecosystem, bounties and grants are used to incentivize third parties for implementing specific tasks. Aion and Wanchain have collaboratively decided to form an interoperability alliance to expedite the process of introducing interoperability standards. Moreover, for creating decentralized applications, there are a number of tools that are provided by the Aion platform.
- **Blockchain router** – In Reference [7], the authors proposed a cross-chain communication mechanism, namely, Blockchain Router, in which communication is handled by blockchain

router, and it can also communicate to another blockchain router or a sub-chain. In this mechanism, there are four participants, each having a particular role. Validators are used to forward, verify, and concatenate blocks towards the right destination. It has to execute the full client and authorize the collected blocks from the sub-chains. Although nominators have no specific function in the blockchain router, they get rewarded for their contribution of their own rights to the validators. Surveillants have the role of monitoring the behavior of the blockchain router to reduce the occurrences of unauthorized behavior. Finally, connectors are responsible for transmitting the information from blockchain router to the sub-chains and vice versa.

- **Metronome** – Bloq developed a cryptocurrency that is not limited to one blockchain platform, although currently it is running on Ethereum platform [88]. It has a token "MET" that can operate on different chains. This token can be initiated by committing it on the target blockchain, and afterwards, it obtains the proof-of-exit as the receipt for source chain token removal. Subsequently, the receipt is presented by the receiving blockchain to the target blockchain for claiming their tokens. There are three key components in the Metronome that include import, export, and validation. The role of the import function is to process the receipt and then issue the tokens to the received blockchain. The export function enables sending blockchain for deleting its relevant tokens and then issuing an evidence in terms of receipt. Validation has several responsibilities and it handles the same in three phases: phase 1 validates and investigates the export receipts, phase 2 constructs and validates the Merkle tree of the receipt hashes, and finally, phase 3 handles hash validation of every chain containing tokens.
- **TAST Project** – Towards conducting the research in the field of interoperable blockchain, there are three similar works that focus on TAST. In Reference [27], the authors reviewed various blockchain projects that are relevant to their project. In addition, they introduced a cross-chain token "PAN" that plays crucial role in their project. In Reference [25], the authors proposed a protocol that is used for exchanging the assets between different chains with the help of claim-first transaction. In Reference [26], the authors carried forward their previous work and demonstrated a use case for their claim-first transactions.
- **Sidechains** – Several projects focus to develop sidechains for enabling communication among blockchains. Among them, we analyzed two projects, namely, Ethereum private sidechains [94] and Sidechains by Blockstream [8]. Both of them focus on building ad hoc chains that are able to interact with the main chain based on their developed approach. In Reference [94], this technology has implemented permissioning for restricting the number of sidechains, and also, it assists in limiting the access control among sidechains. They aim to provide a private environment for enterprises to carry their business process effectively without interfering with the main chain. Moreover, their approach of value transfer and posting the transaction proofs (i.e., it has been successfully included in the block) is very similar to the definition in Reference [8]. Some of their intersecting features are highlighted in Tables 4, 5, and it is depicted that both the projects are determined to support complex applications. In both, the security is consolidated at a lower level, resulting in enabling security for sidechains and mainchain separately (i.e., security risks for one chain do not bother any other chain).
- **Ion interoperable framework** – This project mainly targets interoperability between permissioned and private blockchains. In its earliest phase, it develops a mechanism for swapping ERC-223 token between different ethereum chains [40]. A library of tools was developed, which provides the ability to smart contracts to work in an interoperable scenario. Although the framework will only allow those smart contracts to execute that are

verified. In this way, it gives an interface to the developers for constructing proofs-of-state to verify and validate state transition [2]. This framework presented various examples of smart contracts that are used for interoperability.

We compare the above-discussed projects based on a set of substantial parameters. For better readability, we have captured some of them in Table 4 and rest in Table 5. Apart from these projects, there are several other applications that give their contribution in the area of interoperable blockchain. For example, Luo et al. [42] developed a multi-chain network for management of routing in the heterogeneous blockchain environment. The authors proposed hierarchical architecture that is able to solve the issue of interoperability by encapsulating the services into four different layers. Hardjono et al. [38] also discussed the issue of BI by considering Internet architecture as the underlying design philosophy. All these ongoing research projects are aiming to solve the problem of interoperability in various contexts that gives specific directions in the field of interoperable blockchains.

5 OPEN ISSUES AND FUTURE RESEARCH DIRECTIONS

BI is a significant notion; however, currently, it is in the early stages of its development. Hence, it will confront different challenges/issues in its realization and development. This section presents specific challenges that can be derived during the adoption of the BI paradigm. Moreover, based on the in-depth analysis of BI in this article, it enlists various future research directions that can foster efforts in this area.

5.1 Possible Challenges in Achieving Blockchain Interoperability

To accomplish the goal of interoperability, there is a need to disentangle the challenges that are diverged across many dimensions. Before discussing these challenges, it is necessary to understand the key points that differentiate among independent blockchains. These key points are discussed as follows:

- **Policies and operations** – Basic structure of blockchain has different policies and operations that are used to govern the network. The applications interacting with a particular blockchain work according to these rules.
- **Transaction confirmation** – Every blockchain platform has its own way of confirming the transactions. Accordingly, there is change in the speed of transaction throughput. Other factors, such as the size of the blockchain and consensus mechanism, also vary the speed of transaction.
- **Permissionability** – This is one of the main bottlenecks in the realization of BI. The foundation of the blockchain technology leads towards its public architecture. However, other kinds of blockchain architecture include private blockchain networks and consortium blockchain networks. Hence, there is a need to develop an interoperable solution for all these blockchain networks.
- **Cryptographic mechanisms** – Cryptography is the key aspect that enables blockchain as a trustless distributed ledger technology. However, in terms of interoperability, cryptography creates a lot of complexities. For instance, one blockchain network is working on "X" cryptographic hashing mechanism and another blockchain network is working on "Y" cryptographic hashing mechanism. Then, exchanging transactions between these two cryptographically different networks is a challenging task.
- **Anonymization** – The concept of anonymity in blockchain networks pertains to the anonymity of the participating nodes and end-user. In some cases, one or both can be used in

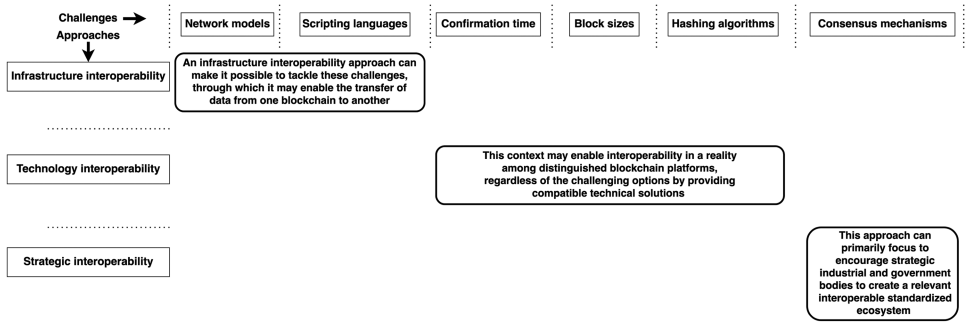

Fig. 8. Contextual approaches to tackle challenges associated with the development of BI solutions.

blockchain networks for providing stronger anonymization in the network. This anonymization property can create more complexity during establishment of communication between two semantically different blockchain networks.

These points solely turn blockchain platforms to become incompatible with each other and are also responsible for thoroughly introducing multi-dimensional challenges in the adoption of BI. In addition, for a better understanding of these challenges within the interoperability context, we split these challenges into a two-dimensional view based on three approaches, as shown in Figure 8. These challenges are enlisted below.

- **Network models** – In the current situation, majority of blockchain projects have been developed on heterogeneous network models, with almost no common standard in their functional and operational mechanisms. Now, the challenge of BI is to establish connection in a trusted way between different network models. This requires that the nodes from different models connected via BI are indistinguishable from each other. Although this concept cannot be fully expressed when the individual network nodes have specific requirements with respect to computing power, storage, and bandwidth. Hence, for different network models, it can be considered as a substantial challenge.
- **Confirmation time** – Confirmation time generally represents the total time taken by a specific action for triggering and confirmation, which totally depends upon how much time it will take to get validated by other blocks in the blockchain and how much time it will take to get successfully appended in the blockchain. Depending upon the blockchain's underlying network model, this time varies. In fact, in some cases, it can also vary in the same network model. Some of the early-stage blockchain models have very low confirmation time. However, nowadays, there are various blockchain models that have much higher confirmation speed. Various approaches also effectuate the confirmation time, such as deterministic way of adding new block takes different confirmation time from the stochastic adding of new block. Currently, there is no standard confirmation time in the blockchain, and hence, there is the challenge during the interoperability among blockchains of how different blockchains will coordinate for interchanging their data.
- **Scripting languages** – Typically, general-purpose programming languages are Turing-complete, which formally refers to the fact that for simulating any Turing machine, it is possible to execute an algorithm on these languages. In other words, these languages can perform arbitrary computations. However, there are various other languages that are different from this category, due to their specific design reasons. Blockchain-based systems support the modification of conditions that are specified in a particular algorithmic manner,

generally referred as smart contracts. Scripting languages are used to draw these algorithms, and hence, this is a more flexible way because the scope of the algorithm is decided by the user. It is worth noticing that developers have to choose the scope of the scripting language before implementing it into the blockchain. In this way, developers choose different scopes during the implementation of blockchain, and resulting blockchains have different scope for scripting language. For instance, EVM can perform arbitrary computations and hence, it is based on the algorithms that are Turing-complete in nature. However, bitcoin scripting language has a limited scope and hence, it is implemented on a non-Turing complete language. And because of these different scopes of scripting languages in blockchains, it is very difficult to establish connection among heterogeneous blockchains. In this way, BI faces challenges in terms of scripting languages.

- **Block sizes** – Block size determines the number of transactions that are processed by the blockchain network, and various blockchains restrict the size of the block to prevent clogging and spamming in the blockchain network. However, over the years, various proposals and implementations on blockchain have come into the picture to compete with other mainstream technologies. This technique of increasing block size addresses the scalability challenge in the blockchain network. However, it causes an increase in the overall cost of running the blockchain. As a result, various nodes are not able to participate in the network leading to partial centralization of the network. Limited block size introduces the challenge of different block sizes in blockchains that leads to difference in their overall throughput. These blockchains also face difficulty during communication among them. Therefore, different block sizes can be seen as a challenge in the concept of BI.
- **Hashing algorithms** – For maintaining security and privacy, blockchain implements various cryptographic primitives, both at operational and technical level. Digital signature, hashing algorithms, and private/public key infrastructures are used for ensuring integrity, authenticity, and confidentiality. Most of the blockchains use ECDSA as their digital signature scheme and versions of SHA (i.e., SHA-256, SHA512) as their hashing algorithm. However, they are not universally accepted cryptographic techniques in the blockchain. For generating fingerprints of blocks, different blockchains use a variety of hashing techniques. There are several other solutions (such as keccak 256) that are utilized as an alternative to the conventional techniques, so the computation will become efficient and scalability would increase. Hence, while establishing connection among different blockchains, there is a difficulty to validate the data block in foreign blockchain. This multiple hashing algorithm scenario will definitely create bottleneck in BI.
- **Consensus mechanisms** – Based on the required features, different blockchains choose different consensus algorithms. Moreover, blockchain-based systems can also choose their layout for establishing consensus based on CNT. This CNT describes the kind of information flow between the nodes and kind of interconnection among them. Therefore, while selecting efficient consensus mechanisms for blockchain, one blockchain may differ from other blockchain due to the underlying consensus mechanism. Hence, the more differences there are in the consensus mechanism, the more challenges will be faced by the blockchain during the process of interoperability.

5.2 Future Research Directions

In the light of analyzing the different perspectives of the state-of-the-art BI solutions, this article suggests that flexibility, integration, standardization, and so on, are some of the research goals that are yet to be achieved in the path of blockchain interoperability. This will provide enormous benefits in the wide-scale adoption and further development of blockchain technology. This article

believes that due to the need for BI and its immature solutions to date, there is immense research potential in the domain, which consequently leads towards possible future research directions that are discussed as follows:

- **Trustless interoperability** – The realization of blockchain interoperability primarily relies on the method of achieving it. As the current research scope focuses on developing solutions relying on trusted brokers, hash-locking, and relays. As a result, purpose of developing blockchain will get diluted. Put simply, state-of-the-art blockchain interoperability platforms, instead of addressing the core of the problem, will develop an obfuscation ecosystem where these platforms will not be able to communicate with each other. Although, based on the organization's needs, an appropriate approach to achieve blockchain interoperability can be chosen. However, there is a critical need for developing platforms under the umbrella of trustless interoperability approach to avoid any further complexities. The notion of "trustless interoperability" intends to establish foundational pillars for platform-independent interoperability and recommends implementing a holistic approach that can accelerate the trustless interoperable solutions to bridge disparate blockchain platforms.
- **Software reference architectures** – To make collaborative efforts in the direction of developing standards (i.e., next discussed research direction), first, there is a need to propose and implement software reference architecture similar to recommended layered architecture in this article and in References [38, 39, 66]. On the contrary to this pathway, existing platforms/protocols consolidate the implementation of BI within their scope (as discussed in Section 4), which significantly limits its potential and may lead to other uncertainties and challenges. Choosing the reference architecture is also another level of challenge, as the presence of more than one architecture will make them difficult to be interpreted that which is correct or more suitable. To address this challenge, formalization and open-source are two of the future directions that may lead to the adoption of a particular reference architecture, among others. Moreover, the reference architecture should not promote a particular platform, application, or technology, since it should be able to provide guidance to address the broader and concrete challenges. Currently, there is no well-established reference architecture that is acceptable for developing applications, approaches, and so on. Hence, there is a significant research potential in this direction.
- **Standardization through collaborative initiatives** – Currently, for staying competitive, a variety of BI research initiatives are in progress or already developed; however, their agility and efficiency to meet the demands of different blockchains are too fragmented (e.g., some of them connect only two blockchains). One of the primary reasons behind this is the lack of standardization and due to this, there is no common understanding of blockchain or blockchain interoperability among stakeholders. Hence, research should not be prioritized for gaining short-term benefits, but it should be focused on achieving long-term benefits that can pave the demand for a common foundation for blockchain interoperability. To fill this research gap, the organization should focus on developing standards that can be understood and implemented by any stakeholders. Standardization efforts can be made at multiple levels. For example, through data standardization, it can be ensured that while data validation, participants (e.g., validators or miners) will be able to understand the form of the exchanged data among heterogeneous blockchains to verify the trustworthiness.
- **Resilience to heterogeneity** – This direction suggests that the approaches should synchronize their functionalities based on the vast requirements of existing and even in potentially developed blockchain-based applications/platforms. Since organizations will continue to use blockchains based on their requirements, resulting in different ways of implement-

ing them. Hence, there should be efforts on both sides, which means that the developed solutions should be able to provide interoperability among newly developed blockchain-based platforms, and potential platforms should also consider the requirements for interoperability during their design and development. To sum up, this research points out the need for solutions that are adaptive towards absolute heterogeneity, as the development of these customizable solutions will enhance overall sustainability and hence, can contribute in the long-run by reducing the effort and cost.

- **Interoperability bridges** – The efforts made in this research pathway can also significantly provide flexible connectivity among disparate blockchain platforms through the development of bidirectional bridges [55], which can assist as independent and transparent interoperable connectors. Notably, these potential bridges should be open source and worked as a decentralized middleware infrastructure that need not to be a separate blockchain, but should be able to blur the boundaries between disparate blockchains. In terms of security, these bridges should not exterminate the scope of security of autonomous blockchains. Indeed, it should have the ability to provide multiple-layer security to guarantee undisrupted interconnectivity. For example, three basic security requirements need to be as a part of underlying bridge design: (a) the information that needs to be exchanged should be securely validated and verified on participating blockchains; (b) during the transmission of information from source chain to destination chain, it should be secure and reliable; (c) the security protocols should not conflict with the existing security protocols of participating blockchains. Implementation of these requirements will enhance trust in the participating entities and increase collaborations among organizations. This article believes that this research direction will unlock pathways to foster solutions for overcoming challenges without replacing or forking the existing blockchains.
- **User-friendly** – The vision for the blockchain interoperability realm is an attempt to create more opportunities in the blockchain ecosystem through the fusion of its scattered platforms/applications. For encouraging participation in this realm, the operational procedures of the underlying approaches should be user-friendly. This article believes that the above-mentioned research directions should be prioritized as compared to this, but simultaneously, it can also be considered as a long-term initiative towards blockchain interoperability if potential approaches developed under this direction will not conflict with other direction's goals; for example, a feasible user-friendly approach to enable BI is API or a set of APIs. However, functional or other requirements of cross-blockchain APIs should not limit the scope of collaborative efforts made by other research directions. Apart from this, developing APIs for enabling connections among disparate blockchains is itself a challenge, as it may require less information (e.g., source and destination blockchain address) for transferring assets from one blockchain to another. However, the result to be returned containing that transaction is recorded successfully in the foreign blockchain depends upon various external factors.

6 CONCLUSION

This article argued that the development of siloed blockchain platforms causes fragmentation across its applications, leading to the limits in the acceptance of blockchain. Considering this, it described the BI domain's holistic perspectives by presenting a comprehensive and systematic review of the BI landscape, along with by providing insights into BI and blockchain taxonomy and its other principles. We began the investigation by analyzing and comparing literature work that studied blockchain technology and its different application areas. Subsequently, we delved into the general underlying principles of blockchain technology and its various platforms. Thenceforth,

we proposed the blockchain taxonomy from the perspective of the governing model and chain structure. We highlighted consensus mechanisms by providing insight on features of different existing consensus algorithms. Subsequently, we considered BI opportunities and determined broader applications that may be feasible because of its accomplishment. Afterwards, we proposed a layered architecture for providing a road map for solutions/approaches to establish the connection at different levels among disparate blockchains. We also proposed a research taxonomy for covering the practical multitude of aspects, which can be imposed for developing BI solutions/approaches. Moreover, we examined and compared state-of-the-art BI projects by focusing on their research initiatives and adopted methodology during design and development. Finally, we highlighted various open research issues and perspective research directions within the scope of BI.

To conclude, there is broad research potential for BI, and more practical approaches are needed for achieving trustless or equivalent BI. This article is aimed to provide considerable knowledge and fosters the need for BI among early-stage researchers, academia, and other stakeholders who want to work in this domain. This article believes that there are enormous challenges that will act as a bump in the road of BI development; however, this article will serve as a cornerstone for the research community to confront these challenges for better outcomes in the prolonged run. We expect that this article's arguments may start new avenues for the implementation and development of BI.

REFERENCES

[1] Stephen O'Neal. 2019. Blockchain Interoperability, Explained. Retrieved from https://cointelegraph.com/explained/blockchain-interoperability-explained.

[2] Clearmatics. 2018. Ion Interoperability Framework. Retrieved from https://github.com/clearmatics/ion.

[3] ISO. 2020. Blockchain and distributed ledger technologies — Vocabulary. Retrieved from https://www.iso.org/standard/73771.html.

[4] Gartner. 2020. Reviews for Blockchain Platforms Market. Retrieved on 4 April, 2020 from https://www.gartner.com/reviews/market/blockchain-platforms.

[5] O. ITU. 2019. Technical Specification FG DLT D1.1 Distributed ledger technology Terms and definitions. Retrieved on 10 February, 2020 from https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf.

[6] Deborah Dobson. 2018. The 4 Types of Blockchain Networks Explained. Retrieved on 10 February, 2020 from https://iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained?ssopc=1.

[7] H. Wang et al. 2017. Blockchain router: A cross-chain communication protocol. In *6th International Conference on Informatics, Environment, Energy and Applications*. 94–97.

[8] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. 2014. Enabling blockchain innovations with pegged sidechains. Retrieved from http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains. 72 (2014).

[9] Christian Cachin. 2016. Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, Vol. 310. 4.

[10] Christian Cachin and Marko Vukolić. 2017. Blockchain consensus protocols in the wild. *arXiv preprint arXiv:1707.01873* (2017).

[11] Vinton Cerf and Robert Kahn. 1974. A protocol for packet network intercommunication. *IEEE Trans. Commun.* 22, 5 (1974), 637–648.

[12] Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. 2020. A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Comput. Surv.* 53, 3 (2020), 1–43.

[13] Usman W. Chohan. 2018. The narcotized blockchain: A potcoin case study. Retrieved from *SSRN 3119917* (2018).

[14] David Clark. 1988. The design philosophy of the DARPA Internet protocols. In *Symposium Proceedings on Communications Architectures and Protocols*. 106–114.

[15] Amie Corso. 2019. Performance analysis of proof-of-elapsed-time (PoET) consensus in the sawtooth blockchain framework. University of Oregon.

[16] Chris Dannen. 2017. *Introducing Ethereum and Solidity*. Vol. 1. Springer.

[17] Erikson Júlio De Aguiar, Bruno S. Faiçal, Bhaskar Krishnamachari, and Jó Ueyama. 2020. A survey of blockchain-based strategies for healthcare. *ACM Comput. Surv.* 53, 2 (2020), 1–27.

[18] Joost De Kruijff and Hans Weigand. 2017. Towards a blockchain ontology. Retrieved from semanticscholar.org/0782/c5badb4f407ee0964d07eda9f74a92de3298. pdf (2017).
[19] Evan Duffield and Daniel Diaz. 2018. Dash: A payments-focused cryptocurrency. *Whitepaper*. Retrieved from https://github.com/dashpay/dash/wiki/Whitepaper. (2018).
[20] Ali et al. 2017. IoT data privacy via blockchains and IPFS. In *7th International Conference on the Internet of Things*. 1–7.
[21] Andrey et al. 2019. Review of existing consensus algorithms blockchain. In *International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS'19)*. IEEE, 124–127.
[22] Ali et al. 2018. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* 21, 2 (2018), 1676–1717.
[23] Bach et al. 2018. Comparative analysis of blockchain consensus algorithms. In *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO'18)*. IEEE, 1545–1550.
[24] Barhanpure et al. 2018. Proof of stack consensus for blockchain networks. In *International Symposium on Security in Computing and Communication*. Springer, 104–116.
[25] Borkowski et al. 2018. Caught in chains: Claim-first transactions for cross-blockchain asset transfers. *Technische Universität Wien, Whitepaper* (2018). [Accessed on 04/01/2020].
[26] Borkowski et al. 2018. Deterministic witnesses for claim-first transactions. *TU Wien: Technische Universit at Wien, Report* (2018). [Accessed on 04/03/2020].
[27] Borkowski et al. 2018. Towards atomic cross-chain token transfers: State of the art and open questions within TAST. *Distributed Systems Group TU Wien (Technische Universit at Wien), Report* (2018). [Accessed on 04/07/2020].
[28] Borkowski et al. 2019. DeXTT: Deterministic cross-blockchain token transfers. *IEEE Access*7 (2019), 111030–111042.
[29] Benji et al. 2019. *A Study on the Corda and Ripple Blockchain Platforms*. Springer, 179–187.
[30] Chang et al. 2016. Data analysis of digital currency networks: Namecoin case study. In *21st International Conference on Engineering of Complex Computer Systems (ICECCS'16)*. IEEE, 122–125.
[31] Chalaemwongwan et al. 2018. State of the art and challenges facing consensus protocols on blockchain. In *International Conference on Information Networking (ICOIN'18)*. IEEE, 957–962.
[32] Dinh et al. 2018. Untangling blockchain: A data processing view of blockchain systems. *IEEE Trans. Knowl. Data Eng.* 30, 7 (2018), 1366–1385.
[33] Dwivedi et al. 2019. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* 19, 2 (2019), 326.
[34] Ellis et al. 2017. ChainLink: A decentralized oracle network. *White paper*. [Accessed on 02/23/2020].
[35] Frauenthaler et al. [n.d.]. Towards efficient cross-blockchain token transfers. [Accessed on 04/05/2020].
[36] Gao et al. 2019. Quorum chain-based malware detection in Android smart devices. In *International Conference on Future Network Systems and Security*. Springer, 212–224.
[37] Hsieh et al. 2018. Bitcoin and the rise of decentralized autonomous organizations. *J. Organiz. Des.* 7, 1 (2018), 14.
[38] Hardjono et al. 2019. Toward an interoperability architecture for blockchain autonomous systems. *IEEE Trans. Eng. Manag.* 67, 4 (2019).
[39] Jin et al. 2018. Towards a novel architecture for enabling interoperability amongst multiple blockchains. IEEE, 1203–1211.
[40] Johnson et al. 2019. Sidechains and interoperability. *arXiv preprint arXiv:1903.04077* (2019).
[41] Kim et al. 2019. Is Stellar as secure as you think? In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'19)*. IEEE, 377–385.
[42] Kan et al. 2018. A multiple blockchains architecture on inter-blockchain communication. In *IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C'18)*. IEEE, 139–145.
[43] Kumar et al. 2017. A traceability analysis of monero's blockchain. In *European Symposium on Research in Computer Security*. Springer, 153–173.
[44] Lo et al. 2017. Evaluating suitability of applying blockchain. In *22nd International Conference on Engineering of Complex Computer Systems (ICECCS'17)*. IEEE, 158–161.
[45] Losa et al. 2019. Stellar consensus by instantiation. In *33rd International Symposium on Distributed Computing (DISC'19)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
[46] Li et al. 2017. A survey on the security of blockchain systems. *Fut. Gen. Comput. Syst.* 107 (2017).
[47] Lizcano et al. 2019. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. *J. Comput. High. Educ.* 32, 1 (2019), 1–26.
[48] Luo et al. 2019. Blockchain enabled trust-based location privacy protection scheme in VANET. *IEEE Trans. Vehic. Technol.* 69, 2 (2019).
[49] Müller et al. 2019. HIDALS: A hybrid IoT-based decentralized application for logistics and supply chain management. In *IEEE 10th Information Technology, Electronics and Mobile Communication Conference (IEMCON'19)*. IEEE, 0802–0808.

[50] Milutinovic et al. 2016. Proof of luck: An efficient blockchain consensus protocol. In *1st Workshop on System Software for Trusted Execution*. 1–6.
[51] Mingxiao et al. 2017. A review on consensus algorithm of blockchain. In *IEEE International Conference on Systems, Man, and Cybernetics (SMC'17)*. IEEE, 2567–2572.
[52] Maull et al. 2017. Distributed ledger technology: Applications and implications. *Strateg. Change* 26, 5 (2017), 481–489.
[53] Muratov et al. 2018. YAC: BFT consensus algorithm for blockchain. *arXiv preprint arXiv:1809.00554* (2018).
[54] Nelson et al. 2016. Extending existing blockchains with virtualchain. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*.
[55] Nazarov et al. 2020. Bridging the Governance Gap: Interoperability for blockchain and legacy systems. *WEF, White Paper* (2020). [Accessed on 01/27/2021].
[56] Nadia et al. 2020. Inclusive deployment of blockchain for supply chains: Part 6 – A framework for blockchain interoperability. *WEF, White Paper* (2020). [Accessed on 09/16/2020].
[57] Parizi et al. 2019. Integrating privacy enhancing techniques into blockchains using sidechains. In *IEEE Canadian Conference of Electrical and Computer Engineering (CCECE'19)*. IEEE, 1–4.
[58] Rezaei et al. 2014. Interoperability evaluation models: A systematic review. *Comput. Indust.* 65, 1 (2014), 1–23.
[59] Salviotti et al. 2018. A structured framework to assess the business application landscape of blockchain technologies. In *51st Hawaii International Conference on System Sciences*.
[60] Sigwart et al. 2019. Towards cross-blockchain transaction verifications. ([n. d.]).
[61] Spoke et al. 2017. Aion: Enabling the decentralized internet. *AION, White Paper, Jul* (2017). [Accessed on 03/11/2020].
[62] Sun et al. 2019. Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment. *IEEE Internet Things J.* 6, 3 (2019), 5791–5802.
[63] Singh et al. 2019. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *J. Netw. Comput. Applic.* 149 (2019), 102471.
[64] Thomas et al. 2015. A protocol for interledger payments. Retrieved from https://interledger.org/interledger.pdf.
[65] Treleaven et al. 2017. Blockchain technology in finance. *Computer* 50, 9 (2017), 14–17.
[66] Verdian et al. 2018. Quant Overledger®. [Accessed on 03/17/2020].
[67] Wileden et al. 1991. Specification-level interoperability. *Commun. ACM* 34, 5 (1991), 72–87.
[68] Xu et al. 2019. Improvement of the DPoS consensus mechanism in blockchain based on vague sets. *IEEE Trans. Industr. Inform.* 16, 6 (2019).
[69] Yaga et al. 2019. Blockchain technology overview. *arXiv preprint arXiv:1906.11078* (2019).
[70] Zhang et al. 2017. *Network-assisted Raft Consensus Algorithm*. 94–96.
[71] Zhang et al. 2020. A refined analysis of Zcash anonymity. *IEEE Access*8 (2020), 31845–31853.
[72] Kurt Fanning and David P. Centers. 2016. Blockchain and its coming impact on financial services. *J. Corpor. Account. Finan.* 27, 5 (2016), 53–57.
[73] Alberto Garoffolo, Dmytro Kaidalov, and Roman Oliynykov. 2020. Zendoo: A zk-SNARK verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains. *arXiv preprint arXiv:2002.01847* (2020).
[74] Bernhard Haslhofer and Wolfgang Klas. 2010. A survey of techniques for achieving metadata interoperability. *ACM Comput. Surv.* 42, 2 (2010), 1–37.
[75] Sandra Heiler. 1995. Semantic interoperability. *ACM Comput. Surv.* 27, 2 (1995), 271–273.
[76] Md Nazmul Islam and Sandip Kundu. 2019. Enabling IC traceability via blockchain pegged to embedded PUF. *ACM Trans. Des. Autom. Electron. Syst.* 24, 3 (2019), 1–23.
[77] Dmitry Ivanov. 2017. Simulation-based ripple effect modelling in the supply chain. *Int. J. Product. Res.* 55, 7 (2017), 2083–2101.
[78] Mark Kasunic. 2001. *Measuring Systems Interoperability: Challenges and Opportunities*. Report. Carnegie-Mellon University, Pittsburgh PA Software Engineering Institute.
[79] Thomas P. Keenan. 2017. Alice in blockchains: Surprising security pitfalls in PoW and PoS blockchain systems. In *15th Conference on Privacy, Security and Trust (PST'17)*. IEEE, 400–4002.
[80] Merve Can Kus Khalilov and Albert Levi. 2018. A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Commun. Surv. Tutor.* 20, 3 (2018), 2543–2585.
[81] Song-Kyoo Kim. 2019. Blockchain governance game. *Comput. Industr. Eng.* 136 (2019), 373–380.
[82] John Kolb et al. 2020. Core concepts, challenges, and future directions in blockchain: A centralized tutorial. *ACM Comput. Surv.* 53, 1 (2020), 1–39.
[83] Jae Kwon and Ethan Buchman. 2016. Cosmos: A network of distributed ledgers. Retrieved from https://cosmos.network/whitepaper.
[84] Weiyi Liu. 2019. Portfolio diversification across cryptocurrencies. *Finan. Res. Lett.* 29 (2019), 200–205.
[85] Ankur Lohachab, Saurabh Garg, Byeong Ho Kang, and Muhammad Bilal Amin. 2021. Performance evaluation of Hyperledger Fabric-enabled framework for pervasive peer-to-peer energy trading in smart cyber-physical systems. *Fut. Gen. Comput. Syst.* 118 (2021).

[86] Ankur Lohachab, Anu Lohachab, and Ajay Jangra. 2020. A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. *Internet Things*9 (2020), 100174.
[87] Damiano Di Francesco Maesa and Paolo Mori. 2020. Blockchain 3.0 applications survey. *J. Parallel Distrib. Comput.* 138 (2020).
[88] Metronome. 2018. Metronome owner's manual. Retrieved from https://www.metronome.io/download/owners_manual.pdf.
[89] Preston Miller. 2016. *The Cryptocurrency Enigma*. Elsevier, 1–25.
[90] Satoshi Nakamoto. 2019. *Bitcoin: A Peer-to-peer Electronic Cash System*. Report. Manubot.
[91] Till Neudecker and Hannes Hartenstein. 2018. Network layer aspects of permissionless blockchains. *IEEE Commun. Surv. Tutor.* 21, 1 (2018), 838–857.
[92] Giang-Truong Nguyen and Kyungbaek Kim. 2018. A survey about consensus algorithms used in blockchain. *J. Inf. Proc. Syst.* 14, 1 (2018).
[93] Benjamin J. Parker. 2017. Software-defined Networking Gateway. US Patent 9,680,870.
[94] Peter Robinson, David Hyland-Wood, Roberto Saltini, Sandra Johnson, and John Brainard. 2019. Atomic crosschain transactions for ethereum private sidechains. *arXiv preprint arXiv:1904.12079* (2019).
[95] Pratima Sharma, Rajni Jindal, and Malaya Dutta Borah. 2020. Blockchain technology for cloud storage: A systematic literature review. *ACM Comput. Surv.* 53, 4 (2020), 1–32.
[96] Paolo Tasca and Claudio J. Tessone. 2017. Taxonomy of blockchain technologies. Principles of identification and classification. *arXiv preprint arXiv:1708.04872* (2017).
[97] Andreas Tolk and James A. Muguira. 2003. The levels of conceptual interoperability model. In *Fall Simulation Interoperability Workshop*, Vol. 7. Citeseer, 1–11.
[98] Zhiyong Tu and Changyong Xue. 2019. Effect of bifurcation on the interaction between Bitcoin and Litecoin. *Fin. Res. Lett.* 31 (2019).
[99] Moshe Y. Vardi. 2019. The long game of research.
[100] Wanchain. 2017. *Building Super Financial Markets for the New Digital Economy*. Whitepaper.
[101] Ke Wang et al. 2018. ReviewChain: Smart contract based review system with multi-blockchain gateway. In *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 1521–1526.
[102] Peter Wegner. 1996. Interoperability. *ACM Comput. Surv.* 28, 1 (1996), 285–287.
[103] Gavin Wood. 2016. Polkadot: Vision for a heterogeneous multi-chain framework. *White Paper* (2016).
[104] Min Xu, Xingtong Chen, and Gang Kou. 2019. A systematic review of blockchain. *Finan. Innov.* 5, 1 (2019), 1–14.
[105] Y. Wenli et al. 2019. A survey on blockchain-based internet service architecture: Requirements, challenges, trends, and future. *IEEE Access*7 (2019), 75845–75872.
[106] Z. Wenbin et al. 2018. Blockchain-based distributed compliance in multinational corporations' cross-border intercompany transactions. In *Future of Information and Communication Conference*. Springer, 304–320.
[107] Rui Zhang et al. 2019. Security and privacy on blockchain. *ACM Comput. Surv.* 52, 3 (2019), 1–34.
[108] Qingyi Zhu, Seng W. Loke, Rolando Trujillo-Rasua, Frank Jiang, and Yong Xiang. 2019. Applications of distributed ledger technologies to the internet of things: A survey. *ACM Comput. Surv.* 52, 6 (2019), 1–34.
[109] S. Zoican et al. 2018. Blockchain and consensus algorithms in internet of things. In *International Symposium on Electronics and Telecommunications (ISETC'19)*. IEEE, 1–4.

Received October 2020; revised February 2021; accepted April 2021