Journal of Industrial Information Integration 26 (2022) 100312

Contents lists available at ScienceDirect

Journal of Industrial Information Integration

journal homepage: www.elsevier.com/locate/jii

Review article

A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues

Khizar Hameed [a,*], Mutaz Barika [b], Saurabh Garg [a], Muhammad Bilal Amin [a], Byeong Kang [a]

[a] Discipline of ICT, School of Technology, Environments, and Design, University of Tasmania, Australia
[b] University of South Australia, Adelaide, Australia

ARTICLE INFO

Keywords:
Blockchain industrial applications
Application requirements
Security requirements
Privacy-preserving
Security attacks
Countermeasures

ABSTRACT

Blockchain technology has taken on a leading position in today's industrial applications by providing salient features and showing significant performance since its beginning. Blockchain began its journey from the concept of cryptocurrency and is now part of a range of core applications to achieve resilience and automation between various tasks. However, with the integration of Blockchain technology into different industrial applications, many application designs, security, and privacy challenges present themselves, posing serious threats to users and their data. Although several approaches have been proposed to address the specific application, security and privacy challenges of targeted applications with limited security enhancement solutions, there is still a need for a comprehensive research study on the application design, security and privacy challenges, and requirements of Blockchain-based industrial applications, along with possible security threats and countermeasures. This study presents a comprehensive and state-of-the-art survey of Blockchain-based Industry 4.0 applications, focusing on potential application design, security and privacy requirements, as well as corresponding attacks on Blockchain systems with potential countermeasures. We also analyse and provide the classification of security and privacy techniques used in these applications to enhance the advancement of security features. Furthermore, we highlight some open issues of integrating Blockchain technology into industrial applications that help design secure Blockchain-based applications as future directions.

1. Introduction

The broad use of the Internet of Things (IoT) paradigm and its associated network and communication technologies is the major driving force behind the modern industrial transformation called Industry 4.0. Industry 4.0 is a compilation of cutting-edge technologies built on advanced knowledge, communication standards, and industry standards applied to manufacturing to automate processes and facilitate data exchange in real-time [1]. Furthermore, due to the rapid development of Industry 4.0, its principles and techniques are being adapted to all other industrial sectors such as energy, finance, and healthcare. With an emerging trend towards the use of disruptive technologies in Industry 4.0, academics and researchers have focused on developing Industry 4.0-based applications to benefit society. This emerging trend provides an interconnected platform to users for exchanging large amounts of data used in different processes. Considering Industry 4.0 commercial-level platforms that have gained popularity across society, many users with various requirements are realising the power of Industry 4.0 and building purpose-driven IoT platforms [2]. However, the rapid growth in the number of users and their requirements makes the interconnected networks built on the concepts of Industry 4.0 frequently encounter various design challenges such as centralisation, scalability, interoperability, and single point of failure. Additionally, due to the volume of data shared over unsecured networks, Industry 4.0-based applications are frequently subject to a variety of security and privacy concerns, including but not limited to device compromise, data modification and unavailability, and personal information theft [3]. Blockchain technology is a promising solution to address the aforementioned issues and concerns in Industry 4.0-based applications [4].

Blockchain technology promises to eliminate the need for a central third party between communication parties and to give all network nodes an equal opportunity to control and manage network operations. In general, Blockchain technology establishes a trusted

* Corresponding author.
E-mail addresses: hameed.khizar@utas.edu.au (K. Hameed), mutaz.barika@unisa.edu.au (M. Barika), saurabh.garg@utas.edu.au (S. Garg), bilal.amin@utas.edu.au (M.B. Amin), byeong.kang@utas.edu.au (B. Kang).

https://doi.org/10.1016/j.jii.2021.100312
Received 2 September 2020; Received in revised form 11 August 2021; Accepted 5 December 2021
Available online 1 January 2022

Peer-to-Peer (P2P) network with the apparent purpose of developing decentralised applications capable of executing secure computations on transactions using cryptographic algorithms. Along with secure computations, Blockchain technology also presents an exciting opportunity for storing verified transactions on a shared, immutable ledger. This immutable feature is an embellished concept of Blockchain technology that provides the irreversible guarantee of transactions stored at the distributed ledger [5]. After achieving remarkable success in the field of digital cryptocurrencies, Blockchain technology has gained considerable momentum among various business communities and even yielded the interest of various industrial application domains, including IoT [6], banking [7] and financial services [8], Smart Grid (SG) [9], transport and logistics [10] and healthcare industry [11]. Furthermore, recent years have demonstrated the adaptability of Blockchain technology in a wide range of applications to facilitate the automation of various manufacturing tasks through the use of inherent Blockchain features such as decentralisation, distributed immutable ledger, transparency, traceability, and auditability.

Considering the key features of Blockchain that make it useful for a variety of businesses and fit well into Industry 4.0, this technology was characterised by a new revolution for the aforementioned spectrum of applications. For example, in the traditional banking and financial sector, a high level of security was essential to ensure the protection of customer money, data, and information. In practice, this process required many intermediaries to move money and assets over a network infrastructure, increasing the cost of transactions and making them more prone to errors, fraud, and misinterpretations [12]. Blockchain technology has the ability to transform and innovate the way transactions and assets are securely handled without the use of a trusted third party. As a result, this entire process simplifies transactions and reduces associated expenses while maintaining complete openness and accountability. However, many application areas are still hesitant to integrate Blockchain technology due to the unique design, security and privacy requirements. This initiates a new study area that requires detailed research investigation and discussion.

1.1. Problem statement and motivation

Industry 4.0 is concerned with not only the digital transformation of manufacturing and production processes but also with providing guidelines and direction to all other industrial sectors to improve value creation processes. The character traits of Industry 4.0 (e.g., automation, virtualisation, and real-time response) can be integrated with those of other industrial sectors to create Industry 4.0-based applications through the use of new enabling technologies such as advanced network paradigms (IoT, big data, cloud, robotics, and so on) and emerging network protocols. However, the development and deployment of the Industry 4.0-based applications is not an overnight process, and several critical challenges have been are raised. These challenges are primarily concerned with the application's design and performance and the security and privacy of users and their data [13]. As previously stated, Blockchain technology is gaining popularity in a variety of Industry 4.0-based applications due to its promising features. These cutting-edge Blockchain features have the potential to address a range of issues that have increased massively in Industry 4.0-based applications.

For instance, a Blockchain-based financial application [14] is designed to address the issues associated with high transaction costs, propagation delays, and excessive latency while also providing a secure and efficient method of transforming data in a robust manner. In the healthcare industry, a Blockchain-based application [15] is proposed to address the specific needs and requirements of national health infrastructure organisations to control and manage additional health-related organisations and sectors for secure communication. In transport and logistics, a Blockchain-based secure and decentralised application called DEFEND [16] is proposed to protect the data privacy of shipping items stored in containers. Finally, in a SG environment, a private Blockchain-based decentralised application [17] is designed to provide secure end-to-end communication between the smart meter and SG without the need of any trusted third party.

From our detailed study of the use of Blockchain features in the design of Industry 4.0-based applications and our extensive analysis of existing surveys on the security and privacy challenges related to various Blockchain-based applications (a detailed discussion and comparison of these surveys is provided in Section 2), we identified several shortcomings or gaps in existing surveys, which are: (i) Survey studies (such as [18–20]) only presented a high-level overview of security and privacy issues of Blockchain-based applications without diving into the details, (ii) Most of survey studies [20–26] exclusively focused on the development of a few particular types of Blockchain-based applications, highlighted limited design requirements and lack of discussion of measuring criteria, (iii) Survey studies (such as [3, 21,26–28]) limited their discussion and analysis on a small number of security and privacy issues via the perspective of a few application scenarios, (iv) Several surveys (such as [3,18,19,26–33]) focused their discussions on limited number of attacks and solution approaches, (v) Survey studies (such as [3,18,31–33]) mainly focused on current viewpoints without highlighting unresolved issues with potential future enhancement directions.

Therefore, the aforementioned shortcomings in the existing survey studies motivate and direct us to present a comprehensive and state-of-the-art survey on this critical topic.

1.2. Our contributions

To address the shortcomings in the existing surveys, a growing trend towards the adoption of Blockchain technology across several industry sectors, and to provide the direction for both developers and research communities on how to design secure Industry 4.0-based applications that leverage Blockchain features and meet industrial design, security, and privacy requirements, we present a comprehensive and state-of-the-art research survey that focuses primarily on design, security, and privacy challenges in Blockchain-based Industry 4.0 applications, and then outline a potential attack surface along with the security techniques and solutions utilised to address them. Our concrete contributions to this paper are as follows:

- Present a detailed comparison of existing state-of-the-art surveys with the focus on design, security, and privacy issues in different Blockchain-based Industry 4.0 applications. The performed comparison provides a constructive direction, followed by the existing shortcomings, which serves as a motivation for our study in terms of research enhancement guidelines.
- Identify application and security and privacy requirements that need to be satisfied to develop secure Blockchain-based Industry 4.0 applications. We further elaborate on security and privacy requirements and classify them into different sub-requirements for secure data and information communication over industrial networks.
- Present in-depth discussion on how to design Blockchain-based Industry 4.0 applications that can meet design, security, and privacy requirements, as well as an explanation of how to accomplish these requirements through the use of security enhancement techniques.
- Provide detailed evaluation and analysis for various security and privacy attacks against Blockchain-based Industry 4.0 applications. We further classify these attacks according to various characteristics, including their layered nature, attackers' objectives, security breaches, exploited vulnerabilities, target applications, and possible countermeasures.
- Identify open issues of integrating Blockchain technology into Industry 4.0 applications on a larger scale, which provide researchers with fuel to develop potential future solutions.

1.3. Paper organisation

This paper is organised as follows. Section 2 provides a related work that includes a detailed comparison of existing published surveys on security and privacy for Blockchain-based applications and highlights their limitations. In Section 3, we provide an application-oriented classification of Blockchain technology in terms of its introduction, features, layers, types, evolution, storage structure and transaction models. Section 4 classifies the design, security and privacy requirements of Blockchain-based Industry 4.0 applications. A detailed discussion on design, security and privacy requirements for Blockchain-based Industry 4.0 applications is provided in Section 5. In Section 6, we describe and categorise the security enhancement solutions used to fulfil security and privacy requirements in Blockchain-based Industry 4.0 applications covered by our survey. Section 7 describes the different security and privacy attacks on Blockchain-based Industry 4.0 applications. Furthermore, Section 8 highlights the open issues required to address the development of secure Blockchain applications. Finally, we conclude our paper and provide some future research directions in Section 9.

2. Related work

This section compares related surveys that specifically address security and privacy issues in Blockchain-enabled applications. Based on the published year, publisher, paper title, applications covered, problems addressed, threats and vulnerabilities identified, techniques and solutions and future directions, we compare existing state-of-the-art studies related to blockchain-based Industry 4.0 security and privacy. Table 1 shows a detailed comparison of these surveys.

In a technical report, Yang et al. [18] presented the basic attacks on Blockchain applications such as DoS and 51% attacks, reviewed various solutions and recommended alternatives, such as Hawk and Enigma, to resist these attacks. However, this survey only discussed some traditional security aspects, not the most recent vulnerabilities. According to Li et al. [19], Blockchain systems are vulnerable to security and privacy risks. However, similar to earlier report [18], smart pool, Oyente, Towncrier and Hawk are discussed as basis security solutions to overcome the underlying security vulnerabilities and privacy issues in Blockchain systems. Khalilov and Levi [21] presented a survey to cover the specified concerns of anonymity and privacy in Blockchain-based digital payment systems. The authors addressed different attacks on these systems and provided a few solutions. However, this survey focused only on the security and privacy of financial applications using diverse models. Joshi et al. [24] presented a survey to highlight the security and privacy requirements required in some of the Blockchain-based applications such as finance, healthcare, mobile, defence and IoT. However, the authors only addressed two types of attacks, DoS and 51% attacks, and offered specific cryptography primitives as a solution.

Conti et al. [22] analysed the Bitcoin significant vulnerabilities and categorised each of them with their proposed solutions and approaches. Although the study analysed Bitcoin's significant vulnerabilities in the literature, it only addressed the financial system's security requirements and challenges. Feng et al. [20] presented a survey study underlining the relevance of anonymity and transactional privacy in financial applications. However, this study focused on DoS and Sybil attacks on financial applications. Concerning IoT, healthcare, and some cloud computing applications, Salman et al. [29] summarised the importance of several security services. This study's main shortcoming is that it only discusses security services and challenges for a few blockchain applications. Dasgupta et al. [30] outlined the various security services offered in Blockchain-based applications such as big data, medical, and social networks. According to Hassan et al. [25], integrating IoT and Blockchain technology for public service provisioning raises privacy concerns. However, this survey is a preliminary study for privacy preservation techniques of IoT-based applications with a limited target scope.

Zhang et al. [23] studied the security and privacy requirements for Bitcoin-like cryptocurrency systems. In this study, Various security attacks on Blockchain systems, such as DoS and mining attacks, are discussed. Because this study focused on distinct financial transaction models, it was limited in scope. Casino et al. [27] emphasised the relevance of Blockchain technology and its underlying properties in many real-time applications, ranging from industrial to corporate sectors. However, this study did not address security or privacy vulnerabilities in these Blockchain applications. Mohanta et al. [31] emphasised the importance of Blockchain in many Blockchain applications, including healthcare, banking, IoT, cloud computing, power grids, smart transportation, and so on. This survey study's flaw is that it only discussed security and privacy issues, not solutions. Wang et al. [34] explored user identity and transactional privacy in Blockchain systems. This research study explored zero-knowledge proof and ring signatures, channel protocol, encryption, and coin mixing mechanisms (Mix, Blind, Coin join, etc.) to ensure privacy using Blockchain technology. However, this study only investigated limited privacy protection solutions based on Blockchain.

Akram et al. [26] evaluated existing security solutions for Industry 4.0 applications. However, this study only examined a few Blockchain-based security options, evaluated their advantages and disadvantages, and highlighted interoperability and governance issues. In another study, Maesa and Mori [32] explored the usage of Blockchain in Industry 3.0, linking its underlying applications and discussing the problems and solutions. Only the importance of Blockchain technology in Industry 3.0 is discussed in this study, leaving out security and privacy concerns. According to Perera et al. [33], the construction industry might benefit greatly from implementing Blockchain technology by demonstrating its relevance with different use-case perspectives. However, this study did not detail the security risks and issues associated with these applications or possible countermeasures. Fernandez-Carames and Fraga-Lamas [28] presented a survey to analyse the advantages and disadvantages of using Blockchain and smart contracts in Industry 4.0 applications. However, this study only described a basic roadmap for Industry 4.0 researchers to adopt Blockchain for more cybersecurity industries. Bodkhe et al. [3] performed a survey to assess the potential of Blockchain-based solutions for various smart applications, particularly in Industry 4.0. This study focused on the pros and cons of available solutions with a few countermeasures, but not on the security and privacy problems in Blockchain-based applications.

The revolutions in Industry 4.0 have brought new paradigms to the manufacturing industry, for example, Cyber–Physical Production Systems (CPPSs), which can provide many advantages and future opportunities, such as self-awareness, self-prediction and self-reconfiguration. While CPPSs try to link virtual and physical manufacturing, a unified computing platform is required to implement them in the real world. Therefore, Lee et al. [2] studied the implications of using Blockchain in real-world cyber–physical systems from both a creation and implementation standpoint. Further, to achieve the security and privacy of the devices and networks in industrial manufacturing processes under a smart factory setup, Lin et al. [35] presented a Blockchain-based secure mutual authentication system to enforce fine-grained access policies. Other examples include digitalisation and automation of business process management (BPM) and open inter-operations of service providers to achieve asset trustworthiness using Industry 4.0 and Blockchain technology features such as decentralisation, immutability and accountability. Using automated process management solutions, Viriyasitavat et al. [36] examined a business process management method in composition services where Blockchain technology is used to identify the best possible combinations and assess partner firms' trustworthiness. There is also a way for leveraging Blockchain technologies and capabilities to construct more robust and transparent autonomous smart manufacturing applications, allowing multiple stakeholders to trust the production process [4].

Table 1
Existing surveys on security and privacy of Blockchain-based Industry 4.0 applications.

Ref	Year published/ Publisher	Paper title	Applications covered	Problems addressed	Threats/ Vulnerabilities discussed	Attacks highlighted	Techniques/ Solutions discussed	Future directions
[18]	2016 R3-Zcash	Survey of confidentiality and privacy preserving technologies for Blockchain	Not defined	Confidentiality and privacy in Blockchain	Not defined	Denial of service (DoS) attack, 51% attack	Zero-knowledge proofs, Ring signatures, Mixing Pedersen commitments with range proofs, Hawk, Enigma	Not applicable
[19]	2017 Elsevier	A survey on the security of Blockchain systems	Not defined	Security threats to Blockchain	51% vulnerability, Privacy key security, Criminal activities, Double spending issues, Transaction privacy leakage	Selfish mining attack, Decentralised autonomous organisations (DAO) attack, Border gateway protocol (BGP) hijacking attack, Eclipse attack, Liveness attack, Balance attack	Smartpool, Quantitative framework, OYENTE, Hawk, Town Crier	Develop efficient and less time-consuming consensus algorithms, Design scalable and efficient privacy preserving schemes for decentralised applications, Improve the data cleanup and detections method in smart contracts
[21]	2018 IEEE Communications Surveys & Tutorials	A survey on anonymity and privacy in Bitcoin-like digital cash systems	Bitcoin-like digital cash systems	Anonymity and privacy	Discovering Bitcoin addresses and identities, Mapping bitcoins addresses to IP addresses, Linking bitcoins addresses and their mapping to geo-locations	DoS attack, Majority attack, Re-identification attack, Fingerprinting attack, Man-in-the-middle (MITM) attack,	Mixing, Blind signatures, Ring signatures, Homomorphic encryption, Zero-knowledge proof	Investigate more effective methods to improve anonymity and privacy in Bitcoin, Design more secure cryptography protocols, Improve scalability in the existing Bitcoin-related cash systems, Balance the trusted and integrity relationship with anonymity and privacy of users
[24]	2018 Mathematical Foundations of Computing	A survey on security and privacy issues of Blockchain technology	Finance, Healthcare, Mobile, Defence, Automobile, IoT	Security and privacy in Blockchain	Privacy leakage, Selfish mining, Personally identifiable information security	DoS attack, 51% attack	Traceability, cryptography techniques	Design secure Blockchain-based applications in the areas of security and privacy

(*continued on next page*)

3. Application-oriented classification of Blockchain technology

Blockchain is a decentralised and Distributed Ledger Technology (DLT) that follows the P2P network fashion in which participating nodes can interact and communicate with others without having trusted third parties. The distributed ledger is a shared, timestamped, immutable and append-only database that records transactions in a block structure. Each block is connected to its predecessor block by a cryptography hash stored in the block header to form a complete chain structure called a Blockchain. Each block structure contains multiple

Table 1 (*continued*).

Ref	Year published/ Publisher	Paper title	Applications covered	Problems addressed	Threats/ Vulnerabilities discussed	Attacks highlighted	Techniques/ Solutions discussed	Future directions
[22]	2018 IEEE Communications Surveys & Tutorials	A survey on security and privacy Issues of Bitcoin	Bitcoin	Security and Privacy in Bitcoin	51% vulnerability, Sybil and double-spending, Mining pool, Client-side Security	Bitcoin system attacks, Bitcoin network and entities attacks	CoinJoin, CoinShuffle Xim, CoinShuffle++, DiceMix, ValueShuffle, Dandelion, SecureCoin, CoinParty, MixCoin, BlindCoin, TumbleBit	Propose game theory and stability, Design of cryptography and keying protocols, Improve Blockchain consensus algorithms, Design of incentive mechanisms for miners, Generation of privacy preserving smart contracts
[20]	2019 Elsevier	A survey on privacy protection in Blockchain system	Finance	Privacy (Identity and transaction)	De-anonymisation, Transaction pattern	DoS attack, Sybil attack	Centralised and decentralised mixing schemes, Ring signatures, CryptoNote, Non-interactive zero-knowledge (NIZK)	Design of scalable system, Design of a robust privacy scheme, Compatibility of transaction structure with different privacy requirements, Traceability and account-ability of transactions
[29]	2019 IEEE Communications Surveys & Tutorials	Security services using Blockchain: A state of the art survey	IoT, Healthcare, Cloud computing	Explore security challenges, problems, and services, (Authentication, privacy, integrity, confidentiality, non-repudiation, data provenance) in existing security architectures	Vulnerabilities in traditional centralised architectures	MITM attack, Data theft attack	Presented the multiple Blockchain-based architectures to enhance and support security services	Design the different solutions covering the large scale applications and real-time environments
[30]	2019 Springer	A survey of Blockchain from security perspective	Big data, Medical, Social networks, Sports, Shopping, Education, Entertainment, Finance	Security and privacy in Blockchain	Keys, Quantum, Identity, Reputation, Application, Manipulation, Service, Malware	Replay attack, Impersonation attack, Sybil attack, Eclipse attack, Time jacking attack, Race attack, DDoS attack, Double spending attack, Finney attack, Vector76 attack, Collusion attack	Cryptography operations	Design resilient security solutions to overcome the cyberattacks, Propose energy-efficient mining algorithms, Design query architecture for Blockchain

(*continued on next page*)

Table 1 (*continued*).

Ref	Year published/ Publisher	Paper title	Applications covered	Problems addressed	Threats/ Vulnerabilities discussed	Attacks highlighted	Techniques/ Solutions discussed	Future directions
[25]	2019 Elsevier	Privacy preservation in Blockchain-based IoT systems: Integration issues, Prospects, challenges, and future research directions	IoT (Healthcare, Energy, Intelligent transporta-tion, Finance)	Privacy in IoT	Identity privacy, Transaction privacy	Address reuse attack, De-anonymisation analysis using graphs attack, Wallet privacy leakage attack, Sybil attack, Message spoofing attack, Linking attack	Anonymisation, Encryption, Private contract, Mixing, Differential privacy	Explore and design the further Blockchain-based IoT areas such as Industrial IoT, Internet of farming, cities, Mobile things, Smart cities, Mobile crowdsensing
[23]	2019 ACM	Security and Privacy on Blockchain	Financial transaction	Security and privacy issues in Blockchain	Inconsistencies between ledgers, Falsifying or forging the certificates, Data unavailability, Double spending problem, Disclosure of information,	DoS attack, DDoS attack, Double spending attack, 51% consensus attack, de-anonymisation attack,	Mixing, Anonymous signatures, Homomorphic encryption, Attribute-Based Encryption (ABE), Secure multi-party computation, Non-interactive zero-knowledge (NIZK) proof, The trusted execution environment (TEE)-based smart contracts, Game-based smart contracts	Design efficient consensus algorithms, Develop lightweight cryptography algorithms, User identity problem, Linkability of transactions
[27]	2019 Elsevier	A systematic literature review of Blockchain-based applications: current status classification and open issues	Financial applications, Governance public sector, Voting, IoT, Healthcare, Business Applications, Education, Data management, Construction and real state, Banking and Insurance, Waste management	Impact of Blockchain on different applications	Not applicable	Not applicable	Not applicable	Suitability of Blockchain for specific applications, Explore the latency and scalability issues, Explore sustainability of mining protocols
[31]	2019 Elsevier	Blockchain technology: a survey on applications and security privacy challenges	Healthcare, Financial, IoT, Legal perspective, Power grid, Transport, Commercial clouds, Data reputation systems, Education	Use of Blockchain in various applications and their linked challenges	Not applicable	Double spending attack, Privacy leakage attack, Private key attack, Mining attack, Balanced attack,	Not applicable	Not applicable

(*continued on next page*)

information, such as timestamp, nonce and transaction-related, to a specific event. A timestamp indicates the time of creating each block, whereas nonce is a unique random number generated to each block and used in different cryptography operations. In a Blockchain, each block can contain multiple verified transactions stored as hash values that cannot be changed or modified regardless of the need for a lot of computing power [5,37].

Blockchain allows the network's participating nodes to interact and communicate with others without a significant third party to manage and provide verification services. Communication between network nodes is first validated and then stored as a transaction in a Blockchain database. Different cryptography primitives, such as digital signatures, are used in Blockchain to determine the level of trust for broadcasting transactions between nodes. Usually, there are two types of nodes

Table 1 (*continued*).

Ref	Year published/ Publisher	Paper title	Applications covered	Problems addressed	Threats/ Vulnerabilities discussed	Attacks highlighted	Techniques/ Solutions discussed	Future directions
[28]	2019 IEEE Access	A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories	Industrial Internet of Things, Vertical and horizontal integration systems, Cyber–Physical Production System (CPPS), Industry augmented and virtual reality, Big data and data analytics, Autonomous robots and vehicles, Cloud and edge computing, Additive manufacturing, Cyber security, simulation software	Analysing benefits and challenges of Blockchain in Industry 4.0 applications	Not applicable	Not applicable	Not applicable	Scalability, Consensus mechanism, privacy and security, Energy efficiency, Management of multiple chains
[26]	2020 Wiley	Adoption of Blockchain technology in various realms: Opportunities and challenges	Energy, Health, Supply chain, IoT, Resource monitoring	Blockchain-based security solutions for Industry 4.0 applications	Not applicable	Not applicable	Not applicable	Interoperability, Rules and regulation for governance
[32]	2020 Elsevier	Blockchain 3.0 applications survey	E-voting, Health care, Record and identity management, Decentralised notary, Intellectual property, Supply chain management	Use of Blockchain in various industrial applications	Not applicable	Not applicable	Not applicable	Not applicable
[33]	2020 Elsevier	Blockchain technology: Is it hype or real in construction industry	Finance, Identity protection, Foreign-aid, Voting, Transportation, Food and agriculture, Healthcare Logistics management, Multiple data applications for construction businesses	Applicability of Blockchain in various construction applications and their feasibility	50% vulnerability, code vulnerability, private key security criminal activity exposing identities	Not applicable	Not applicable	Not applicable

(*continued on next page*)

involved in the Blockchain network which are responsible for creating and validating blocks. One is a simple node that can create the account wallets and transactions in the network. Simultaneously, the others are full nodes (also called miner nodes) responsible for verifying or validating transactions before grouping and adding them to the Blockchain. Although both types of nodes can access all the blocks in the distributed ledger, no one has full control of the blocks and cannot modify them [38].

To ensure the reliability of data and transactions and to maintain trust between decentralised nodes, Blockchain systems follow the consensus concept, in which nodes do not accept any trusted third party's services to manage their behaviour and interactions. Each interaction

Table 1 (*continued*).

Ref	Year published/ Publisher	Paper title	Applications covered	Problems addressed	Threats/ Vulnerabilities discussed	Attacks highlighted	Techniques/ Solutions discussed	Future directions
[3]	2020 IEEE Access	Blockchain for Industry 4.0 A Comprehensive Review	Supply chain and logistics, Energy domain, Digital content distribution, Tourism and hospitality industry, Smart healthcare, Smart city, Businesses, IoT, Manufacturing, Agriculture,	Blockchain-based solutions in various Industry 4.0 applications	Not applicable	Not applicable	Not applicable	Not applicable

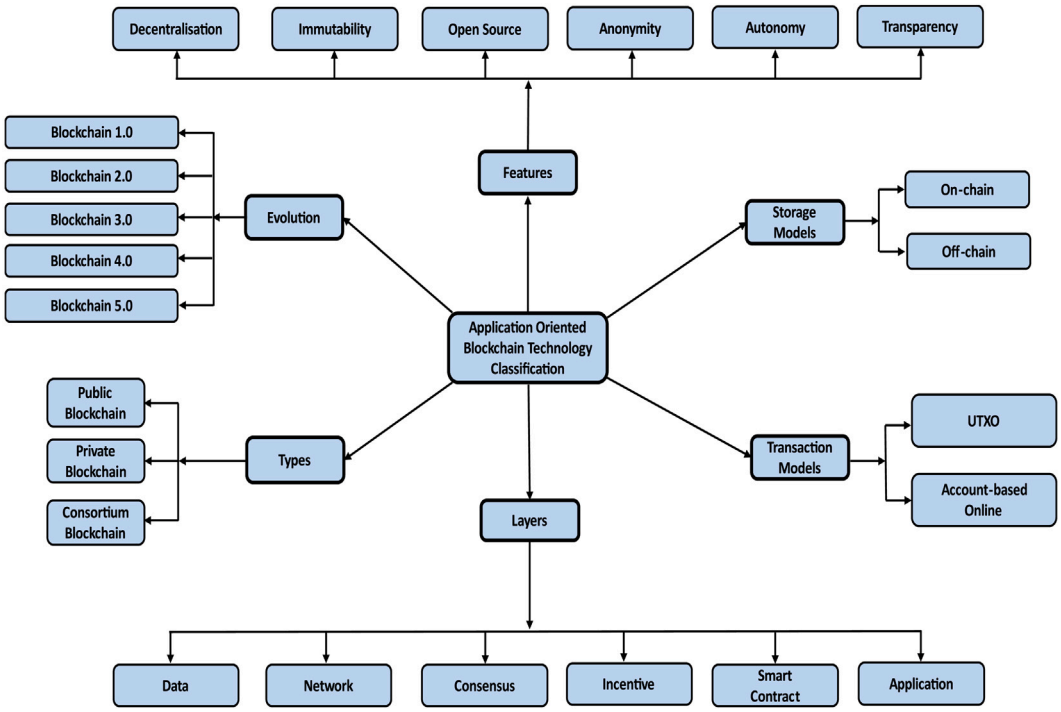


Fig. 1. Application-oriented classification of Blockchain technology.

between the communicating nodes is cryptographically secured and recorded in the distributed ledger. By receiving broadcast transactions, full nodes or miner nodes on the Blockchain network can verify transactions using computational procedures. After verification, the miner nodes build a new block of validated transactions and add them to the Blockchain. To conclude, the complete process of validating and adding transactions to the Blockchain is called mining, followed by some decision-making or consensus mechanism. Each consensus mechanism is associated with miners' rewards for their effort and computation [39].

Depending on the Blockchain systems and their types, several consensus mechanisms have been proposed. Nevertheless, the commonly used consensus mechanisms in most Blockchain systems are PoW (Proof of Work) [40], PoS (Proof of Stake) [41], PBFT (Practical Byzantine Fault Tolerance) [42] and DPoS (Delegated Proof of Stake) [43]. The Bitcoin cryptocurrency generally uses the PoW consensus mechanism, while the Ethereum Blockchain systems use the PoS. Apart from these consensus mechanisms, several other consensus mechanisms have also been developed, such as PoA (Proof of Authentication) [44], PoET (Proof of Elapsed Time) [45], PoSpace (Proof of Space) [46] and PoI (Proof of Importance) [47].

Blockchain technology can be classified into the following set of properties that may vary depending on the design perspectives of each application, ranging from single-user level to business level. These properties include evolution, layered architecture, Blockchain types, storage structure and transaction models. A generalised overview of Blockchain, which illustrates its features, evolution, layers, types, storage structure and transaction models, is shown in Fig. 1.

3.1. Features

Blockchain technology can be summarised with the following features: decentralisation, immutability, open source, anonymity, autonomy and transparency, which are used to achieve a set of security goals for different applications.

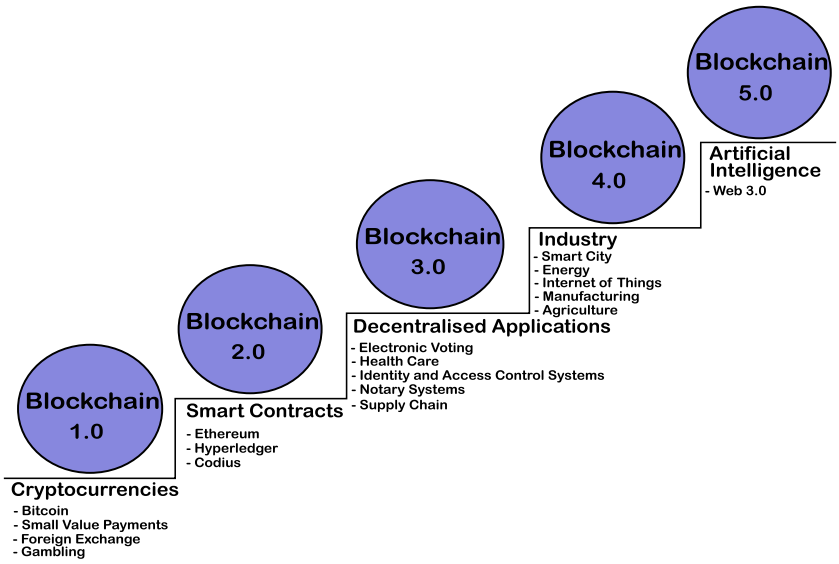


Fig. 2. Blockchain evolution.

3.1.1. Decentralisation

The decentralisation feature allows a group of nodes to be organised in a P2P manner and is responsible for maintaining the network's overall structure, rather than relying on a single governing authority to control and manage network-wide operations [48].

3.1.2. Immutability

Immutability is a key feature of Blockchain technology related to the distributed ledger structure and refers to the permanent state of Blockchain, and its data after the majority of miner nodes validated it. Thus, an immutability feature ensures the integrity and traceability of Blockchain data in a verifiable manner [49].

3.1.3. Open source

An open-source feature of Blockchain technology allows developers to build trust between network nodes and their data, using some of the available code features constructed. Additionally, this feature enables the creation of new decentralised applications to govern the code and adopt a flexible approach [50].

3.1.4. Anonymity

Anonymity applies to an entity's status as being secret and unrevealed means that no one can access the users' true identity from their behaviour or their transactions in the system [51].

3.1.5. Autonomy

An autonomy feature of Blockchain technology is defined as a protocol that is self-governing in nature and capable of completing certain activities autonomously in order to accomplish particular goals without the intervention of a centralised third party [52].

3.1.6. Transparency

Transparency is a key feature of Blockchain technology since it enables users to join the network and verify transactions before they are added to the distributed ledger. For example, transparency in the Bitcoin application enables users to track the history of all transactions, including who initiated and verified them [53].

3.2. Evolution

Blockchain technology continues to evolve its underlying architecture through a sequence of phases or evolution for developing a variety of applications, as illustrated in Fig. 2. To date, the Blockchain evolution phases (1.0 to 4.0) have been presented to provide a number of perspectives, including functionality, application range, features, strengths, challenges, and security issues. The latest version, Blockchain 5.0, is actively being developed to expand its functionality for various business models. Table 2 summarises the different Blockchain evolution phases (from 1.0 to 5.0) with respect to their applications, consensus mechanisms and features for each evolution.

3.2.1. Blockchain 1.0

Satoshi Nakamoto proposed a popular cryptocurrency named Bitcoin in 2009 during the first evolution phase called Blockchain 1.0 [54]. As a result, the words "Cryptocurrency" [66], "Cash for the internet" [67] and "Internet of money" [68] are frequently used on the internet to describe the Bitcoin concept. Blockchain 1.0 has been a popular version for fast-developing digital payment systems embraced by financial companies worldwide [69]. However, interoperability and adaptability issues in Blockchain 1.0 have been identified as significant barriers to its wider adoption.

3.2.2. Blockchain 2.0

Blockchain 2.0 introduces the notion of smart contracts, which are small executable user programmes that operate in the Ethereum Blockchain environment to perform various automated functions and make legitimate choices [70]. These programmes run automatically, based on defined logic and criteria, such as time, performance, decision and verification policies. It is also worth noting that these programmes (or contracts) run with user identities to secure personal data in the Blockchain network [71]. To summarise, Ethereum is the most widely used Blockchain 2.0-based application that allows users to securely design and execute smart contracts [60].

3.2.3. Blockchain 3.0

Some of the primary drawbacks of Blockchain technology (1.0 and 2.0) include reliance on public networks and the inability to store large amounts of data. Examples of public platforms include Bitcoin and Ethereum, where data is generated and stored on the Blockchain at regular intervals; thus, enormous amounts of data must be stored in multiple locations, such as data servers and clouds [72]. Blockchain

Table 2
Different Blockchain generations: An overview of their applications, Consensus mechanisms, and unique features.

Generations	Applications	Consensus mechanism used	Unique features
Blockchain 1.0	• Digital currencies – Bitcoin [54], Bitcoin Cash [55], Litecoin [56], Ripple [57], etc. • Small value payments [58] • Foreign exchange • Gambling • Money laundering	• PoW [40] • PoS • Proof of Elapsed Time (PoET) • Proof of Space • Federated Byzantine Agreement (Federated BA) • Proof of memory	• Mostly designed for cryptocurrencies • Simple ledgers • Public Blockchain
Blockchain 2.0	• Ethereum [60] • Hyperledger [61] • Codius [62]	• PoS [41] • Practical Byzantine Fault Tolerance (PBFT) [42] • Byzantine Fault Tolerance (BFT) - BFT-SMaRt	• Use of smart contracts • Micro-transactions • Digital assets [59] • Privacy • Decentralised Autonomous Organisations (DAOs) • Decentralised Autonomous Corporations (DACs) [63] • Has own contact-oriented language (Solidity) • Public Blockchain
Blockchain 3.0	Enterprise Blockchain applications [32] • Electronic Voting (E-voting) • E-Healthcare (E-health) • Identity and access control systems • Notary systems • Supply chain	Only a few of them are listed here but not limited to [64] • Tendermint • DPoS • Raft • Casper • Staller	• Instantaneous transaction • High scalability • Interoperability • Sustainability • Governance • Cloud servicing • Multi layer middle-ware
Blockchain 4.0	Industrial perspectives [65] • Cyber Physical Systems (CPS) • Smart manufacturing • Industrial Internet of Things (IIoT) • Agriculture • Energy trading • Smart product • Smart city	Only a few of them are listed here but not limited to [64] • Hash DAG • Proof of Importance (PoI) • Proof of Burn (PoB) • Proof of Value (PoV) • Proof of Majority (PoM) • Proof of History (PoH)	• Industry consortium • Consensus mechanism efficiency • Transparency • Improve scalability • Energy efficiency
Blockchain 5.0	Web 3.0 Applications	Not available	Combination of artificial intelligence and DLT • Data privacy • Security • Interoperability

3.0 is introduced to store massive volumes of data and legally support multiple communication channels to overcome this issue. Furthermore, blockchain 3.0 allows developers to build application code in any language because it uses system calls to interface with the decentralised system. However, apart from the benefits, these decentralised networks face numerous security issues, including authentication, authorisation, and access control of users and their data [17]. To demonstrate Blockchain 3.0, smart contract developers introduced Genaro [73], a first Turing machine-based public Blockchain that allows users to build and deploy native smart contracts in decentralised storage systems with many network modules.

3.2.4. Blockchain 4.0

Blockchain 4.0 is presented as the next step in the successful journey of leading Blockchain versions (1.0 to 3.0) to solve the industrial constraints and limitations of real-world applications. Blockchain 4.0 intends to make it practicable for designing and running real-life applications in a safe and decentralised fashion in the industrial environment [74]. Moreover, Blockchain 4.0 enables industries and businesses to migrate their whole structure and operations transparently to self-recording applications built on a decentralised, distributed, and immutable ledger. Industry 4.0, a new technological wave for interconnection between people and machines, enables significant industry growth and productivity transformation, favourably impacting people and the environmental quality of life [64].

Integration of Industry 4.0 with Blockchain 4.0 establishes a new paradigm based on trusted networks that eliminate the requirement for a third party and further transforms individual manual processes into linked systems via automated and autonomous systems. This convergence is primarily centred on the use of Blockchain features such as public ledgers and distributed databases, as well as the implementation of smart contracts in industry processes to remove the need for paper-based contracts and to control the network through consensus [28].

There are several examples of Industry 4.0 with Blockchain 4.0 integration that have recently implemented this new version into their business processes, including financial services [7], IoT [75], Transport and Logistics [76], SG [77,78] and E-Health [79].

3.2.5. Blockchain 5.0

Blockchain 5.0 is designed to address the demands of the future generation of business people by standardising and simplifying the digital age. In this revolutionary environment, it is vital to have Blockchain 5.0, which combines Artificial Intelligence (AI) with DLT, to create the next generation of decentralised Web 3.0 applications, ensuring data privacy, security, and interoperability. By choosing this direction, a startup named “Relictum Pro” is well on its way to make a success in the new Blockchain 5.0 era [80].

3.3. Layers

The layered architecture of Blockchain can be divided into the following categories from top to bottom: application layer, smart contract layer, incentive layer, consensus layer, network layer and data layer [81,82]. Fig. 3 illustrates the layered architecture of Blockchain.

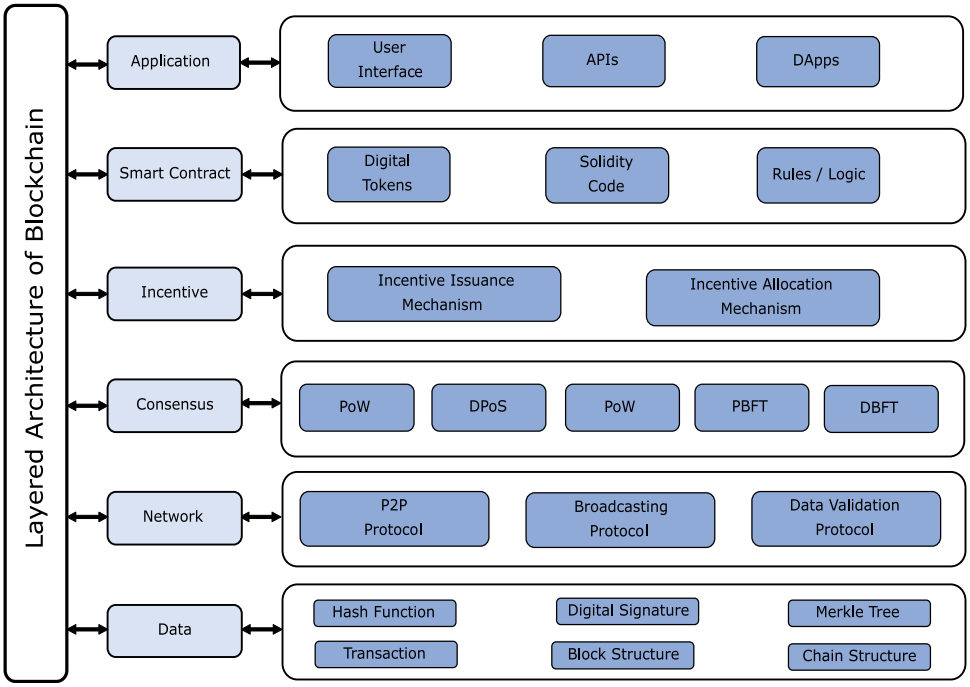


Fig. 3. Layered architecture of Blockchain.

3.3.1. Application layer

The application layer is a critical component in any architectural layout because it allows humans to interact with the existing system and promotes communication between individuals or systems through a network. In Blockchain, the application layer comprises smart contracts, chain code, scripts, application programme interfaces (APIs), user interfaces and frameworks responsible for delivering specific user interface components and encompasses everything that makes an application work, including protocols and code.

3.3.2. Smart contract layer

The smart contract layer contains a smart contract script and algorithmic logic for specific functions within the Blockchain application. A smart contract script is a piece of code recorded on the distributed ledger, whereas algorithmic logic defines a set of rules and circumstances that govern how parties interact and communicate.

3.3.3. Incentive layer

The incentive layer is the third layer in the Blockchain layered architecture and is responsible for rewarding contributors. The incentive method has two main components: issuing and allocating rewards. Besides that, this layer encourages nodes to engage in Blockchain verification. For example, in Bitcoin, miners receive bitcoins, while in Ethereum, ethers are used as mining incentives.

3.3.4. Consensus layer

This layer enforces network rules that govern how nodes should behave to reach consensus on broadcasted transactions and guarantees the integrity of Blockchain records. To accomplish this goal, the consensus layer incorporates several consensus protocols that enable Blockchain nodes to agree on the authenticity and legitimacy of newly created data blocks. Various consensus mechanisms, such as PoW, PoS, DPoS, PBFT, DBFT, etc., have been proposed and used by various Blockchain-based applications.

3.3.5. Network layer

The network layer is the fifth layer in the Blockchain layer architecture, and it facilitates communication between Blockchain nodes. Although numerous components make up the network layer and enable nodes to communicate on a Blockchain network, three basic components are essential: the P2P network, the broadcasting protocol, and the validation mechanism. Because the P2P network is decentralised, every node has an equal chance to generate a new block in the Blockchain network. Each node generates a block to establish a chain and broadcasts it to the P2P network for validation. The validation method obtains a new block containing information from other peer nodes and verifies it before adding it to the Blockchain.

3.3.6. Data layer

The data layer maintains the data structure and physical storage space based on secure distributed ledger technology. The ledger is built from asymmetrically encrypted Merkle trees, which are connected lists of blocks. The data layer includes hash functions, asymmetric cryptography, Merkle trees, transactions, block structures, and chain structures. Because transactions are saved in the block as hashes, a hash function is employed to convert transactions. Asymmetric encryption, such as public/private key pairings, is frequently used to secure network transactions. The Merkle tree is used to store and arrange transactions on the Blockchain. On the other hand, blocks are utilised as data structures that combine all transactions and distribute them to all nodes in the P2P network for verification. The user-specified transactions are linked in the chain structure by storing the root hash of the previous block.

3.4. Types

There are three types of Blockchain: public, private and consortium. These types are divided according to their assessment criteria and permission rules, all of which require access to the Blockchain network.

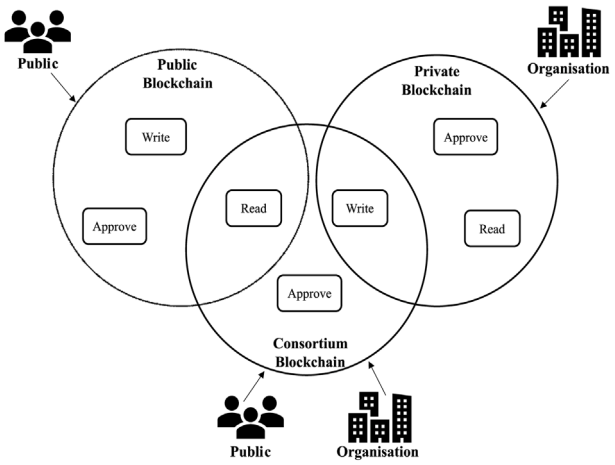


Fig. 4. Consortium Blockchain with different access policies.

3.4.1. Public Blockchain

The most fundamental type of Blockchain network is the public Blockchain, which allows any user to participate, send, receive, and validate transactions on the network [83]. The validation procedure is carried out by specially selected nodes known as miners, who execute the consensus algorithm in order to verify the transactions and add validated blocks to the current Blockchain [84]. Indeed, consensus algorithms like PoW [40] and PoS [41] are typically used in public Blockchains, in which miners are rewarded for their services (hashing or calculations), and the reward is proportional to the effort performed by each miner [85]. Furthermore, several cryptography techniques are used in the public Blockchain to identify and secure user transactions, yet each participant's identity remains anonymous [86]. The most common and well-known public Blockchain networks are Bitcoin [54], Ethereum [60], Litecoin [56] and Monero [87].

3.4.2. Private Blockchain

Unlike a public Blockchain, a private Blockchain is a permission-based network that allows an organisation or group of people to read or write blocks. For instance, a single authority defines the rules and procedures for the entire private Blockchain configuration. A private Blockchain is meant for organisations that want to keep their data safe within certain boundaries, such as finance and audit firms [19,88].

3.4.3. Consortium Blockchain

The hybrid Blockchain network is referred to as a consortium Blockchain because it incorporates the properties and characteristics of both public and private Blockchain networks. For instance, a read request to access a particular block may originate from a public Blockchain, whereas a write request is restricted to private Blockchain nodes [89].

Fig. 4 illustrates a variety of access permissions (read, write, and approve) on a consortium Blockchain that is executed by public and private Blockchains. The consensus process used in consortium Blockchains is controlled and maintained by the initial group of nodes designated to control and maintain the Blockchain configuration [90].

3.5. Storage structure

Blockchain technology leverages various cryptographic properties to enable the development of real-time and networked applications based on decentralised and distributed databases. Due to the high volume of data generated by real-time applications, it is critical to manage and secure the storage locations used internally (a local hard drive) or externally (a server or cloud). In general, there are two types of storage models utilised by Blockchain applications to store real-time data, such as on-chain storage and off-chain storage. The following sections describe the storage structures in depth.

3.5.1. On-chain storage

Due to the fact that blockchain-based applications make use of the distributed ledger concept to manage data across a network, the primary storage used by Blockchain is referred to as on-chain storage. The data is recorded on the Blockchain in the form of transactions, and each block is linked to the preceding block to form a complete chain. The miner nodes are responsible for validating the blocks in order to add them to the Blockchain [91].

This entire process adds significant storage overhead to the system for operations like transaction execution and verification, reward distribution, and decentralisation. However, there are several benefits to storing data on an on-chain Blockchain; for example, users are not required to maintain two storage locations, which reduces the compute and storage costs associated with off-chain storage [92].

3.5.2. Off-chain storage

Off-chain storage is used in Blockchain-based applications when user transactions are stored on a system (or storage) different than the actual storage, limiting user access. Unlike traditional databases, blockchain transactions are recorded in a hash comprising the actual transaction data. Using off-chain storage in Blockchain has various benefits, including enhanced user privacy when access is restricted and governed by access control policies. However, adopting the Blockchain off-chain method has several drawbacks, such as lack of user confidence and the requirement to disperse data across different storage places via hash references. In addition, the cost of storing data off-chain is also high since users must manage the record with extra computation power [93].

3.6. Transaction models

The transactions in the Blockchain and their related applications are designed and maintained in a specific way. The basic idea behind the design of different transaction models is that they can resist various attacks on Blockchain applications. The two most commonly used transaction models in Blockchain applications are the Unspent Transaction Outputs (UTXO) and Account-based Transaction.

3.6.1. UTXO model

The UTXO is the primary transaction model used in Bitcoin and related cryptocurrency applications. The bitcoins, a Bitcoin currency, are recorded as a transaction on the Blockchain and are represented in the wallet of the users. To represent bitcoins in the wallet, the user maintains a list of unspent transactions that include all transaction parameters such as amount, owner and time [94]. Due to the anonymity and scalability of transactions, the UTXO paradigm has proven quite popular in cryptocurrencies, particularly Bitcoin [95].

3.6.2. Account-based online transaction model

Unlike the UTXO model, this model uses an address of a sender to represent the transactions in Blockchain [96]. The Ethereum-based applications use the account-based model to generate and deploy smart contracts on the Blockchain. The account-based architecture seeks to improve the efficiency and reliability of consensus methods by reducing block verification time [97]. In this model, ethers (or gas) are stored as transactions on the Ethereum Blockchain, with acceptable properties, such as signature, approval, and balance. Unlike the UTXO model, this approach provides unlimited space to store users information because ethers do not keep unnecessary details like bitcoins.

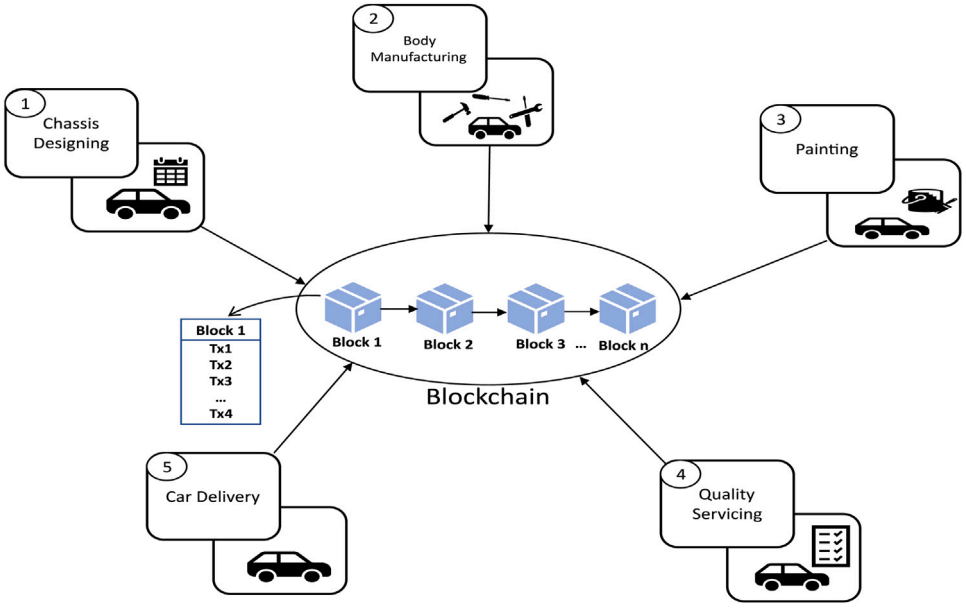


Fig. 5. Car manufacturing process in smart factory under Industry 4.0.

4. Requirements for Blockchain-based Industry 4.0 applications

This section provides an in-depth introduction to Industry 4.0, with a particular emphasis on design, performance, and security and privacy challenges and how the integration of Blockchain Technology with Industry 4.0 can address these challenges through the use of several popular blockchain architectures (or applications). As a result, we define a set of requirements for developing Blockchain-based Industry 4.0 applications, where these requirements are further categorising into application design requirements and security and privacy requirements.

4.1. Industry 4.0 and Blockchain technology

The fourth industrial revolution (also referred to as Industry 4.0) is changing the way we live, work, and communicate. Industry 4.0 is a new stage in the coordination and planning of industrial manufacturing processes. The manufacturing process of Industry 4.0 has now transformed fully, through a succession of digital transformations, to achieve productivity and automation of the entire process. This shift in industrial processes allows traditional businesses and factories to evolve into smart factories, or Industry 4.0. Smart factories can be established by integrating objects, operators, and background information into an industry framework over the internet [98].

Similar to most other technological drivers, the internet is the most significant technology in Industry 4.0. Based on the internet, IoT and other related technologies such as distributed networks, completely automated protocols, and competitive production networks are driving Industry 4.0. The integration of leading technology players such as IoT, Blockchain, big data, edge and cloud computing, robotics, artificial intelligence, and open-source software has extended the scope of Industry 4.0, benefiting both industry and partners [99]. Incorporating these players into Industry 4.0 creates an integrated and automated system (a cyber–physical system, or CPS), turning the industrial infrastructure into an autonomous and dynamic system. Components in these fully integrated CPSs must interact and operate intelligently to collaborate autonomously and achieve a common goal [100]. In Industry 4.0, data computing infrastructure enables warehouse-scale networks to connect in real-time, increasing efficiency and collaboration [101].

Ultimately, Industry 4.0 aims to improve manufacturing processes, operational efficiency, and customer service while enabling new business models and opportunities beyond automation and real-time discovery. Industry 4.0 integrates different components such as smart devices, sensors, robots, and humans into the manufacturing process to collect data to improve quality and sustainability. In the manufacturing process, the modules or working processes collect data from the sensors embedded in the machine equipment, perform some computations and send them to the next module as an output transaction. In addition, each module in the manufacturing application communicates with others. In most industrial setups, many processes at diverse locations contribute to overall system functionality [102].

Industry 4.0 is concerned with the digital transformation of various industrial sectors and value-generating processes. With the advent of new technologies like mobile data networking and network protocols and IoT stack components and security features, it is now possible to exploit Industry 4.0 features, which may then be integrated with other industrial sectors to develop Industry 4.0-based applications. This shift in Industry 4.0 has prompted business and research communities to explore beyond manufacturing processes to other industrial applications such as healthcare, energy, financing, logistics, and supply chain [103].

With the various new and developing breakthroughs, numerous new and forthcoming challenges arise in the industry sectors. These challenges involve the design and performance (e.g., scalability and interoperability), as well as the security and privacy, trust, and transparency of a large number of Industry 4.0 applications [13]. For example, centralised architecture can become a bottleneck in large industrial systems, causing scalability and single point of failure issues. Moreover, because industrial applications handle and store large amounts of data, storage challenges such as data heterogeneity and redundancy and data privacy and security must be addressed. The use of Industry 4.0 capabilities by many industries makes them attractive targets for attackers. Therefore, security is a critical issue in the effective implementation of Industry 4.0-based applications [4,28].

Blockchain technology, as a leading player, has the ability to address the issues raised above in relation to Industry 4.0-based applications. For instance, Blockchain technology can establish a trustworthy platform for data exchange and transaction processing, and self-executing smart contracts can drastically shorten processing time and eliminate the need for intermediaries. In addition, the immutability feature of distributed ledgers prevents attacks and establishes trust since transactions are linked together using cryptographic hashes to create blocks, making it difficult for attackers to change or remove information. Furthermore, the consensus mechanism of Blockchain enables the verification of transaction authenticity and the modification of information during

the process. The traceability and auditability features help clients and suppliers track the product's origins and transit. For instance, in agriculture, traceability enables the tracking of records, with a particular emphasis on the origin and quality of foods. In particular, these features can benefit Industry 4.0 applications by increasing scalability, transparency, efficiency, effectiveness, and resilience.

Due to many promising features such as decentralisation, distributed immutable ledger, transparency, anonymity, autonomy, open source, verifiability and security, Blockchain technology is now gaining popularity in numerous Industrial 4.0 applications worldwide. Numerous Blockchain architectures have been proposed and became famous for usage in several Industry 4.0-based applications to facilitate integrating these features. Following is a summary of Blockchain architectures utilised in various industries; however, these are not limited to:

- **Codefi** [104] is a blockchain-based financial architecture launched in September 2019. It is made up of modules that enable the next generation of commerce and finance. Codefi's blockchain suite provides decentralised networks, scalability, and greater access to web-based technology.
- **MedRec** [105] is a well-known blockchain implementation for health care applications that provides secure and efficient data storage. The patient, doctor, and the insurance company can all update the patient health record in this design. **Medicalchain** [106] is another decentralised health care architecture based on blockchain technology that is used in the UK for patient data management. User demands are prioritised while keeping a single reliable version of data on a distributed ledger.
- **PowerLedger** [107] architecture is built on Blockchain technology to allow buying and selling of energy resources based on an allocation market. **Bankymoon** [108] is another blockchain-based energy architecture that provides blockchain-enabled smart prepaid energy metres to schools and communities globally.
- **Electronic Product Code Information Services (EPCIS)** [109] is a blockchain-based food traceability architecture that employs EPCIS services and shows its benefits. Because less data is saved on-chain and more is stored off-chain using EPCIS, this architecture provides a higher level of security. **OriginTrail** [110] blockchain-based architecture designed to offer transparency to global supply chains. This platform is commonly used in the food business to locate food products.
- **IBM Watson IoT Platform** [111] enables isolated Blockchains for IoT data sharing, giving an additional degree of security and integrity. Another Blockchain architecture, **ADEPT (Autonomous Decentralised P2P Telemetry)** [112], uses Blockchain technology in IoT network and employs Ethereum, Telehash's functions and BitTorrent.

Developing secure Blockchain-based applications using Industry 4.0 guidelines is a critical challenge that usually requires an appropriate relationship between the architectural components of the underlying domain and the Blockchain features in order to achieve optimal usability at various levels [113]. Moreover, developers and researchers must comply with security and privacy regulations to ensure adequate user and industry partner compliance [114]. For example, a Blockchain-based IoT application must meet domain, security, and privacy requirements to build trust between nodes [75].

Fig. 5 illustrates a car manufacturing process in a smart factory that utilises Blockchain-based services to support Industry 4.0 and complies with the Blockchain-based application's requirements. A decentralised network enables everyone to complete tasks independently of the central party. Each transaction from a module participating in the manufacturing process is maintained on an immutable distributed ledger using distributed ledger technology. The distributed ledger data maintains a complete record of chassis design, body manufacture, painting, quality servicing, and successful unit delivery. Using this Industry 4.0 example, we can derive two perspectives of requirements for designing secure Blockchain-based Industry 4.0 applications. For decentralised and distributed Industry 4.0-based applications, we cover design requirements for architecture, functional, non-functional and performance, and security and privacy for users and processes in Blockchain. The industrial application design requirements are detailed in Section 4.2.

In security and privacy requirements, we include users and their transactions, storage structures, control and management, and different privacy perspectives. Security and privacy are significant challenges for Industry 4.0 applications since unauthorised data breaches, or information leaking might result in critical data loss. Malicious attacks on sensing devices and supply chain processes can interrupt overall production processes and reveal personal information related to identity and transactions. Thus, in the realm of Industry 4.0 application development, the security of integrated modules and their generated data is critical. Section 4.3 elaborates on the security and privacy requirements.

4.2. Application design requirements

This section goes into depth about the requirements and sub-requirements for designing Blockchain-based Industry 4.0 applications. We break down each design requirement into sub-requirements and describe them from an industry perspective. These requirements are decentralisation, scalability, correctness, efficiency, interoperability, consistency, usability, flexibility, protection, modularity, fairness, completeness and transparency. Fig. 6 illustrates a high-level taxonomy of requirements and their sub-requirements.

Along with determining the requirements and sub-requirements, we examined the numerous measuring criteria that explain how to achieve these requirements rationally, as given in Table 3.

4.2.1. Decentralisation

Decentralisation is an important requirement for Blockchain-based industry applications to share the loads among the manufacturing entities. Decentralised architecture removes a centralised entity's requirement from the overall process to eliminate intermediaries costs and provide access control to all network users. There are three types of Blockchain networks following the decentralisation requirement concept such as: public, private, and consortium [115].

Apart from that, distributed storage is a fundamental requirement for any decentralised design that values equality in a P2P network. Each node has equal rights to validate and verify database transactions. Owing to the unavailability of a central authority in the Blockchain network, each node is responsible for both computing data and sending updated copies of data to all other nodes to ensure network consistency. In this regard, each node handles its storage, rather than relying on centralised storage systems [17].

The decentralised requirement can be further broken into sub-requirements, including the following:

- **Fully Decentralised:** Fully decentralised networks allow anyone to join as a node and send transactions to other nodes without a trusted third party. A public Blockchain is an example of a fully decentralised network.
- **Partially Decentralised:** In a partially decentralised network, some nodes are allocated to monitor and administer network operations, while others may participate like in a completely decentralised network. An example of a partially decentralised network is a consortium Blockchain.
- **Distributed Storage:** Distributed storage is a requirement for any decentralised architecture that emphasises equality between P2P nodes in order to validate and verify transactions stored in the database.

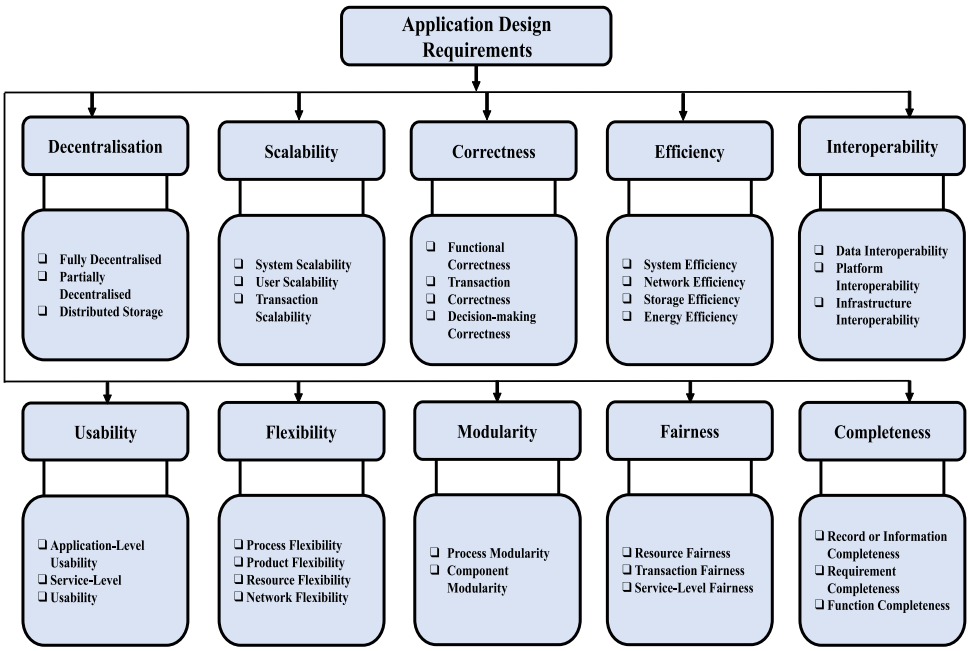


Fig. 6. A taxonomy of design requirements for Blockchain-based Industry 4.0 applications.

4.2.2. Scalability

With the rapid development of Blockchain applications and their growing popularity in Industry 4.0, scalability has become a critical requirement [15,116]. However, when real-time applications generate data or transactions, the network may be constrained in certain conditions, such as traffic bottlenecks and storage overflows. Financial applications require hundreds or thousands of transactions per second, as Bitcoin handles five on average per second [117]. Thus, scalability is required for Blockchain-based applications to accommodate maximum user and transaction numbers possible. So, for example, scalability requires:

- **System Scalability:** System scalability covers the need for scalable server capabilities to satisfy future interaction volume and response time per user request.
- **User Scalability:** The maximum number of concurrent users the system can support without compromising performance.
- **Transaction Scalability:** Transaction scalability is defined as the ability to respond to an increasing number of user queries within a given time frame, compared to the increasing database output, employing multi-processing systems.

4.2.3. Correctness

Correctness is a requirement for analysing computing results and measuring real-time system behaviour and can be determined by tests, simulations, mathematical analysis, logical proof, and formal modelling [118,119]. The number of transactions, block creation time, consensus time, transparency level, and system integrity can all be used to measure correctness in Blockchain applications. Similar to performance parameters, the correctness of security and privacy-preserving schemes for Blockchain-based applications is achieved by detailed security analysis and robustness against various privacy attacks [35].

The correctness requirement has several sub-requirements, such as:

- **Functional Correctness:** The relationship between inputs and outputs from industrial processes is determined by functional correctness rather than other system efficiency settings like computation time, communication, and memory overhead.
- **Transaction Correctness:** A transaction's correctness concerns the correct execution of its activities in terms of its abstract meanings and data structures.
- **Decision-Making Correctness:** A rational decision-making correctness ensures that decisions are made based on facts, systematic data collecting, and analysis. The user is also notified of the reasonable input data values.

4.2.4. Efficiency

In summary, efficiency is the system's ability to perform more with less effort. Computational power, communication bandwidth, and storage capacity are key system efficiency parameters [8]. The miner's ability to solve challenges in a given time is the most widely used metric for Blockchain applications efficiency [120]. For example, Bitcoin takes roughly ten minutes to solve a block and add it to the Blockchain. Further, each consensus method requires a specific amount of energy (or power) from adherent hardware resources in order to solve a computational problem such as a puzzle [121].

The efficiency requirement has several sub-requirements, such as:

- **System Efficiency:** When a computation system performs optimally with minimal inputs, it is said to be an efficient.
- **Network Efficiency:** To maintain adequate bandwidth, network efficiency is efficiently exchanging or transmitting information to local and worldwide networks.
- **Storage Efficiency:** Data must be stored and processed efficiently in order to save space and have little impact on output.
- **Energy Efficiency:** The degree of energy efficiency evaluates how much less energy is required to achieve a goal.

4.2.5. Interoperability

Interoperability design requirement enforces process integration across decentralised application components to improve interaction and communication [122]. Moreover, interoperability allows decentralised applications to securely exchange information over the network via a Blockchain. Thus, the Blockchain platform must allow for seamless data exchange between multiple Blockchains, and the interoperability feature must not allow Blockchain applications to exceed the boundaries specified for system interoperability using fair access procedures [123].

Sub-requirements of interoperability include:

- **Data Interoperability:** Data interoperability allows multiple common frameworks to build, trade, and handle data to share definitions, understand context, and share responsibility.

- **Platform Interoperability:** Platform interoperability allows users and applications to discover, access, integrate, and analyse data on a common platform. It also enhances system flexibility by standardising software bundles, metadata, and identifiers.
- **Infrastructure Interoperability:** It involves updating and expanding IT infrastructure to include newer technologies such as clouds so that all applications and related technologies function seamlessly. Furthermore, infrastructure interoperability ensures data integrity and security by securely connecting new and existing systems.

4.2.6. Usability

Because Blockchain technology is decentralised, it can overcome scalability and efficiency difficulties in traditional IoT systems. However, most Blockchain solutions provide the basic functionality required to process and confirm network transactions without considering usability issues that may deter consumers from utilising such systems [10]. Accordingly, usability is a key requirement that must be met in order for people to feel comfortable communicating with various Blockchain systems. As a result, an easy-to-use interface is required to improve customer satisfaction [124].

The usability requirement includes sub-requirements such as:

- **Application-Level Usability:** Application-level usability examines how users interact with an application. The resulting data is utilised to improve the system's capabilities and suggest improvements to the interface.
- **Service-Level Usability:** Unlike application-level usability, service-level usability refers to a system's capacity to respond to user requests and assess their expectations. At this level, each user request is assessed against the system's services.

4.2.7. Flexibility

The efficiency of secure and reliable transactions without a central entity has proven to be a possible answer for different business and Industry 4.0 needs. Furthermore, a flexible Blockchain system can let other technologies integrate, deploy modules, and provide solutions [118]. Additionally, optimising performance for integrated Blockchain systems requires addressing the flexibility of diverse applications focused on the system should have built-in Blockchain functions [125]. Flexibility has the following sub-requirements:

- **Process Flexibility:** In the industrial context, process flexibility is required to efficiently respond to external influences such as changes in supply or demand. Process flexibility can boost system outputs while decreasing external costs like time.
- **Product Flexibility:** The requirement for product flexibility can be quantified in terms of adaptability to any future changes to the product, including new designs and variations. Flexible product design reduces redesign costs and increases customer response time.
- **Resource Flexibility:** The ability of resources to efficiently perform a wide range of manufacturing operations is typically evidence of resource flexibility.
- **Network Flexibility:** Flexible networks can handle procedures that must be executed and transferred between modules, which is called industrial network flexibility.

4.2.8. Modularity

Modularity allows diverse associated organisations to join and use network resources to create comprehensive services with the power of reusability [126]. Moreover, developers can design decentralised applications using diverse languages that run on heterogeneous platforms. Examples include Komodo [127], an open source Blockchain modular architecture meant to help users integrate alternative end-to-end communication modules to handle challenges of scalability, security, and interoperability.

The modular requirement is further broken into two sub-requirements:

- **Process Modularity:** Process modularity is a requirement that breaks down a single big process into many sub-processes that can run on multiple machines.
- **Component Modularity:** A modular design is frequently regarded as splitting functions into discrete, compact, and scalable modules, requiring substantial usage of well-defined standardised interfaces.

4.2.9. Fairness

Blockchain applications need to be fair to build confidence between industries and the proposed security models. In other words, fairness is addressed by offering middleman agreements, or smart contracts, that conform with the rules and requirements [86,169]. Furthermore, fairness defines the logic and criteria for the parties to engage without trusted third parties. As a result, it is vital to building security mechanisms for Blockchain applications that are fair to all users and keep them engaged.

The fairness requirement can be further subdivided into many sub-requirements, including the following:

- **Resource Fairness:** Resource fairness is a need in an industrial setup because it allows a system to allocate resources fairly among its processes. A single user's transactions can overwhelm the system, causing poor performance for other users.
- **Transaction Fairness:** Fair transactions are required to promote fair remuneration to individuals who engage in and join the network for mining.
- **Service-level Fairness:** Service-level fairness promotes equal access to system resources and software for all network users.

4.2.10. Completeness

Completeness, as a design requirement, aims to ensure users' specific needs and requirements to complete any application. For example, in Blockchain-based applications, the security and privacy models are deemed complete if they prove the satisfactory computational requirement and comprehensive security analysis, using multiple proofs and logic [86].

The completeness requirement has various sub-requirements, including:

- **Record or Information Completeness:** Data completeness is expressed as an expected degree of data completion, with optional data frequently eliminated. So as long as the data meets the standard and criteria, it is complete.
- **Requirement Completeness:** To ensure proper implementation and verification, an individual requirement is considered complete if it contains all necessary information meets the customer demands.
- **Function Completeness:** A function completeness ensures that the system behaves correctly and provides the functionality required to fulfil tasks.

4.3. Security and privacy requirements

This subsection outlines the security and privacy requirements for Blockchain-based Industry 4.0 applications in detail. Fig. 7 illustrates a taxonomy of security and privacy requirements.

Table 3
Designing Blockchain-based industry 4.0 Applications: Requirements, Sub-Requirements and Measuring criteria.

Requirements	Sub-Requirements	Measuring criteria
Decentralisation		
	• Fully decentralised	• **Network:** Fully decentralised or partially decentralised.
	• Partially decentralised	• **Storage:** Distributed ledger technology (DLT) [128].
	• Distributed storage	• **Control:** Fully centralised (public Blockchain), centralised (private Blockchain), partially centralised (consortium Blockchain) [129].
		• **Communication Topology:** P2P [130].
Scalability		
	• System scalability	• **Transaction Per Second (TPS):** Used to compute the number of transactions processed and recorded on the Blockchain per second.
	• User scalability	• **Block Creation Time:** The amount of time taken to build a new block [64].
	• Transaction scalability	• Block Size: Block size (in bytes) for storing several transactions.
		• **Throughput:** The transaction throughput is characterised as the rate at which valid transactions are accepted and stored by the Blockchain within a given time frame.
		• **Response Time Per User Request:** The system's initial response to user requests submitted to the system.
		• **No. of Open Connections:** Determine the number of connections per system needed to accommodate a large number of users.
Correctness		
	• Functional correctness	• **Model Driven Engineering (MDE):** A technique for addressing software development complexity by using models at different levels of abstraction [131–133].
	• Transaction correctness	• **Experiments and Simulations:** A collection of performance parameters used to determine the system's performance [134–136].
	• Decision-making correctness	• **Formal Verification:** A formal specification language used to construct complex software systems by applying mathematical methods or techniques [137].
		• **Mathematical Modelling:** The use of mathematics to predict and make decisions in the real world [138].
		• **Logical Evidences:** The logical proof is used to validate or invalidate an idea using certain logic, in which deductive reasoning can be used to conclude to provide logical evidence [139].
Efficiency		
	• System efficiency	• **Throughput:** The amount of time it takes to append correct records to blocks. It is generally measured as the total number of committed and saved records (after being validated) divided by the total time to validate and save records.
	• Network efficiency	• **Latency:** The time interval between when a transaction is submitted and when it has been written to the ledger [140].
	• Storage efficiency	• **Bootstrap Time:** The time it takes to load all of the information and data needed to create a block [141].
	• Energy efficiency	• **Bandwidth Overhead:** The propagation of all information associated with each block in the Blockchain network [142].
		• **Transaction Size:** The size of a single transaction (in bytes) stored in each block, which results in the development of the Blockchain [143].
		• **Block Size:** The total number of transactions saved on each block [144].
		• **Data Provision:** Ensure that the data is open to all users with sufficient permissions and in a protected manner [145].
		• **Computational Complexity:** Current hash rate of a consensus mechanism, such as PoW, in a public Blockchain [146].
Interoperability		
	• Data interoperability	• **The usage of APIs:** The interaction of two Blockchain networks through a specially built application programming interface such as smart contracts [147].
	• Platform interoperability	• **Multi-Chain:** Using crypto-dependent tools such as side chains to insure interoperability [148].
	• Infrastructure interoperability	• **Separate Blockchain:** An intermediary Blockchain sitting between the two existing Blockchains [149].
		• **Off-chain:** Using middleware such as state channels, or atomically swap boxes [150].
Usability		
	• Application-level usability	• **Usability Test Approaches:** [151,152].
	• Service-level usability	• **Combination of Different Metrics:** (Effectiveness, Efficiency, Fault tolerance, etc.) [153].
Flexibility		
	• Process flexibility	• **Asynchronous Operations:** Asynchronous operations are used to determine the flexibility of system modules [154].
	• Product flexibility	• **Decision-Modelling Approach:** Define the hypothesis and then evaluate it using qualitative methods [155].
	• Resource flexibility	• **Other Proposed Frameworks:** [156–158].
	• Network flexibility	
Modularity		
	• Process modularity	• **Business Process and Modelling approaches:** [4]
	• Component modularity	• **Quantitative Modelling Approaches:** Using quantitative modelling methods to assess modularity [159].
Fairness		
	• Resource fairness	• **Incentive Mechanism:** Provide equal incentives to users who participated in the creation of the block [160,161].
	• Transaction fairness	• **Time Commitment:** Before the timer runs out, the committer party must reveal a secret [162].
	• Service-level fairness	• **Price Calculation:** Maintain the rates paid for services [163].
		• **Usage Intention:** Ensure that the specifics of the usage intention are accurate [164].
Completeness		
	• Record or information completeness	• **Information Centred Approach:** The relevant information is available to the relevant authorities at the right moment [165,166].
	• Requirements completeness	• **Software Validation Strategies:** Software validation techniques can be used to ensure that functional and non-functional requirements are met [167,168].
	• Functions completeness	

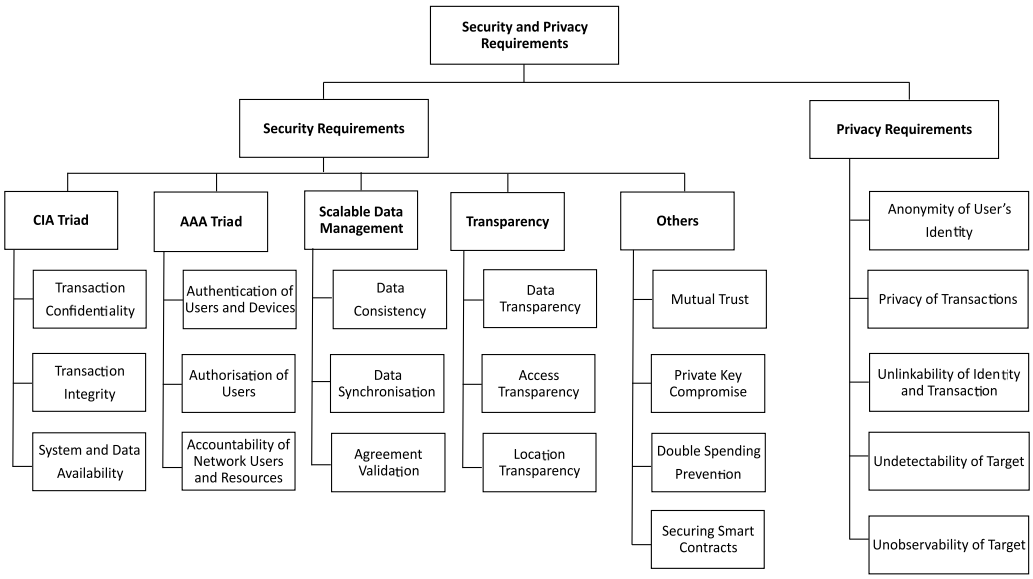


Fig. 7. A taxonomy of security and privacy requirements for Blockchain-based Industry 4.0 applications.

4.3.1. Security requirements

We categorise the security requirements of Blockchain-based Industry 4.0 applications into the following different types.

- **Confidentiality, Integrity, Availability (CIA) Triad:** Confidentiality, integrity, and availability, sometimes referred to as the CIA triad, is a security requirement model used to define application-specific information security policy. Our CIA triad security requirements include the confidentiality of transactions, the integrity of transactions, and the availability of systems and data.
  - **Transaction Confidentiality:** As the name implies, confidentiality is the key security requirement of any application or system designed to protect transactions from unauthorised access. In a wide variety of applications, such as financial, IoT, and healthcare, users desire to restrict their transactions, including personal data, secret information, and trade values. Since the Blockchain network is open to everyone, which enables users to send transactions publicly to other users, keeping transactions, secure is a major concern [170].
  - **Transaction Integrity:** The integrity of transactions is a critical requirement when implementing Blockchain-based systems to support several services, such as big data marketplace services [171] and product delivery in transportation and logistics systems [172]. This security feature ensures the authenticity and dependability of transactions throughout their life cycle. Furthermore, this feature also prevents adversaries from changing or modifying data stored in databases or communicating over network channels. However, besides increasing transaction costs in above said Blockchain-based applications, introducing falsification or forgery into the transactions chain raises the danger of falsely signing or forging a transaction. Therefore, the system must guarantee the integrity of transactions and keep fraudulent transactions from being created [173].
  - **System and Data Availability:** Any application or system built for a particular purpose should make it possible for the users to view the transaction data, regardless of the device's location. It is possible to accomplish these tasks at systems and transaction levels. For example, while the system continues to run even in the event of a network attack, the entire system should maintain an operation at the system level, and while data access at the transaction level can be made available to authorised users without being failing, incorrect, or distorted [174,175].
    The availability of Blockchain-based applications can also be defined as the interaction of validated Blockchain transactions, primarily dependent on the availability of two Blockchain functions, namely reading and writing. The Blockchain system's read-availability response is always higher than the written-availability response; hence variations in measured time can cause availability failure [176].
- **Authentication, Authorisation and Accounting (AAA) Triad:** Similarly to the CIA triad, authentication, authorisation, and accounting (AAA) refer to a fundamental security mechanism for ensuring proper network resource utilisation and user access for various applications. AAA triad aims to operate intelligently in Blockchain-based systems and gives users access to computer resources by implementing stringent access and auditing regulations.
  - **Authentication of Users and Devices:** Over the next decade, the number of IoT devices is expected to grow to 25 billion [177]. With the growth of IoT devices, security risks can have severe consequences for human life. For example, the Mirai botnet was used to target the network infrastructure corporation, causing several of the Internet's most popular sites to go offline in 2016. Authentication protects IoT devices and network users' identification and is the first line of network security defence. As a result, an appropriate authentication system is a critical requirement that can protect the identity of IoT devices and network users, acting as the first line of defence for network security. Unfortunately, current authentication systems, such as Public Key Infrastructure (PKI), are centralised and incapable of fulfilling the growing authentication demands of users and IoT devices [178].
  - **Authorisation of Users:** Preventing unauthorised access to critical resources has always been a powerful tool for improving computer security. To achieve this, authorisation or access control restricts a user's actions on a computer system while also preventing adversaries from accessing critical resources without authorisation. Nevertheless, similar to authentication procedures, standard authorisation methods

in the IoT rely on existing approaches, which incur overhead and centralisation. However, proposing decentralised, dynamic, and adaptable access control mechanisms is a critical requirement for resolving conventional authorisation or access control systems issues [179,180].

  - **Accountability of Network Users and Resources:** After successfully authenticating and authorising users, an accountability process monitors resources consumed by network or application users. A method of accountability can be through session statistics, such as the duration of a session, and user information, including the amount of data, transmitted and received [181]. Accountability has been adopted as a critical requirement for most blockchain-based systems because internal users can act as adversaries in the network and engage in fraudulent activities such as data modification and unauthorised access to critical resources. Moreover, accountability enables the administrator to monitor internal or external users who exceed the resource limits set to them [182].

- **Scalable Data Management:** Management of distributed databases, such as blockchain technology, is one of the most essential security requirements in many Blockchain-based applications, namely the maintenance and control of an interconnected network of records with wide-scale data expansion [23]. A requirement for scalable data management can be further subdivided into the following sub-requirements.

  - **Data Consistency:** It is another essential requirement with the massive increase in the scale of Blockchain, which includes a wide variety of diverse devices that generated different types of data. Lack of data consistency could lead to serious security issues in this modern world, such as using insecure security software that has not been carefully tailored to the individual device.
  - **Data Synchronisation:** It is another critical requirement for Blockchain-based applications. However, it is sometimes a time-consuming task to achieve as it is difficult to detect, maintain, and evaluate the header-to-header information for massive blockchain network datasets.
  - **Agreement Validation:** It requires a reasonable demand for data synchronisation in Blockchain network in order to achieve anonymity with a rapidly increasing number of users. Agreement validation in Blockchain-based applications can be accomplished through the use of Ethererum's smart contract functionalities.

- **Transparency:** It is one of the most important requirements for public Blockchain users. Many people are confused about the principles of privacy and transparency, even though the implementation is fundamentally different. For example, in Blockchain-based systems, cryptographic primitives are regarded as the most powerful means of achieving user-transparent transactions. Regardless of the openness of the Blockchain, users' transactions must be transparent and invisible to other users [117]. The requirement for transparency includes several sub-requirements, such as:

  - **Data Transparency:** Many industries today require data transparency to allow open communication and ensure that everyone has access to the same information.
  - **Access Transparency:** In order to achieve access transparency, all objects, static or mobile, must share the same access functionalities. Also, the interface required to access an object should match its system position.
  - **Location Transparency:** Location transparency is the ability to access entities and system resources without knowing their exact location.

- **Mutual Trust:** A decentralised network such as the Blockchain is maintained via consensus protocols that all nodes on the network must adopt. One such protocol is PoW, which has a 51% attack vulnerability that attackers can exploit to take control over the entire network. To explain it another way, in the case of the event above, a single mining pool may wield an excessive amount of mining power, potentially resulting in mistrust among network nodes. One such use is the deployment of Blockchain in IoT-based smart home networks, where an attacker can compromise the majority of devices that connect and share data with one another [183]. As a result, establishing mutual trust among network nodes through a secure and efficient consensus protocol is a critical requirement for the majority of Blockchain-based applications [184,185].
- **Private Key Compromise:** Private key protection is a critical requirement for practically all applications that rely on cryptography operations to secure their communication. Since users generate and manage their private keys in Blockchain-based applications rather than relying on third-party agencies, it is the user's responsibility to protect the secret key, as recovering a private key after it has been lost can be rather difficult in some situations. For instance, if an attacker obtains control of the private key of users, then the user's blockchain account becomes vulnerable to security credential manipulation [30].
  To generate the private keys, a few Blockchain-based implementations such as Bitcoin and Ethereum use a particular elliptic curve called secp256k1, which provides quick and easy computations due to its unpredictable and non-deterministic design. However, as explained by Bernstein and Lange [186], there are numerous weaknesses in the secp256k1 scheme that could cause problems for user's private keys. Further, the random number generator is fundamental to several cryptographic algorithms, like ECDSA and other algorithms that rely on secure random numbers. Thus, in the event that a private key can be recovered given a public key generated with a bad random number generator, it may be possible to derive the private key.
- **Double Spending Prevention:** Trading digital currency in decentralised financial systems presents a significant challenge due to the threat of double-spending that means spending currency more than once. Centralised systems employ a central trusted third party to ensure that digital currency has not been double-spent. Conducting transactions in a decentralised network environment, on the other hand, is a key challenge that requires the design of robust security measures capable of preventing double-spending in such networks [187].
- **Securing Smart Contracts:** The importance of smart contracts is apparent, especially in various electronic services and information applications, which can include a diverse array of business, financial, IoT, E-health, medicine, etc. In essence, smart contracts are computer programmes that regulate legislation and agreements and are autonomously enforced by consensus mechanisms among contractual parties on the Blockchain when predetermined criteria are met. As with the majority of software, smart contracts are insecure, and their security is technically equivalent to that of any other software [188]. Smart contracts written to integrate with blockchain systems are open to exploitation. Further, as being immutable, smart contracts can also create huge issues when integrated into unsecured blockchain applications. At the same time, their security depends entirely on the programmer's most up-to-date knowledge. However, due to poorly designed programming approaches, several smart contracts are prone to exploits [189]. For example, such an attack called decentralised autonomous organisation (DAO), resulted in the loss of USD 60 million worth of cryptocurrencies [190].
  Therefore, the security issue surrounding smart contracts has emerged as a fundamental requirement for increasing their adoption and effectiveness in a broad range of Industry 4.0 applications.

4.3.2. Privacy requirements

We classify privacy requirements for Blockchain-based industry 4.0 applications into the following five significant categories:

- **Anonymity of User's Identity:** Network objects, such as users or devices, are identified by their unique identities. However, a significant challenge of transmitting user data securely over integrated networks requires repeating user authentication to identify, resulting in high costs in system overhead uniquely. In addition, in some cases, some intermediaries parties may also inadvertently reveal the identities and data of the user to others. There are many instances in which one or both participants in the transaction are unwilling to disclose their actual identity. As a result, anonymisation of user identities within the network is an essential aspect of achieving privacy [23]. To ensure the anonymity of the user's identity, pseudonymisation techniques have been widely implemented in Blockchain-based systems; however, pseudonymisation is not a mechanism of anonymisation but a technique that helps to reduce the association between a data set and the actual identity to which it relates [191].
- **Privacy of Transactions:** Most financial internet transactions are completed to expect users to keep their transactions and account information private to achieve transactional privacy. The transactional privacy requirement in financial or non-financial applications requires the user to accomplish the following objectives: unauthorised users cannot access users' transaction data, entities (e.g., users, administrator) are prohibited from disclosing personal information to others, and transaction data should be stored in a secure place [34].
  In a Blockchain, the distributed immutable ledger consists of several verified transactions updated and maintained by the network users. Each user is responsible for sending the updated transaction to all other network users and updating the distributed ledger. However, during the transmission or interchange of transactions among Blockchain users, the transaction's information can easily be obtained by an adversary in the network [192]. The adversary follows different approaches to steal personal information from a transaction related to a specific user. The transaction graph pattern method is one of the standard methods that link and retrieve users' personal information from a transaction [193].
- **Unlinkability of Identity and Transaction:** Unlinkability (also called untraceability) is a critical privacy requirement that states that multiple interactions with a system by the same user should not be linked [194]. Unlike anonymity, which prevents people from disclosing their real identities, users always want their transactions protected from the linked scenario. Unlinkability must be accomplished for both identification and transactions of the users on the Blockchain. For instance, it should be difficult for the adversary to link many addresses (or identities) and transactions associated with the same user interaction with Blockchain-based systems such as Bitcoin. Once all transactions involving a particular user can be linked, the other adversary can easily extract information about the user, such as personal information and balance. Anonymous use of a system requires both pseudonymity and unlinkability. Though the Blockchain in Bitcoin provides pseudonymous identification, unlinkability does not extend to user transactions, as a pseudo-identity only supports anonymity [23,195].
- **Undetectability of Target:** Undetectability, another privacy requirement, specifies that an attacker is not unable to determine whether a target exists or not. A target can be any system or network element, including a device, a user, a service, or a specific resource or piece of data. In Blockchain-based systems, particularly financial applications, the requirement for undetectability prevents an attacker from analysing the identity-related data kept in the user's wallet, resulting in illegal access to system resources or services. Undetectability is maximised when it is entirely indistinguishable whether a target exists or not; this is referred to as perfect undetectability [194].
- **Unobservability of Target:** Unobservability is also an important privacy requirement, as it prevents users from being observed or monitored while accessing an underlying system's resources or services [194]. In other words, the unobservability assures that a user may access the resources or services of the systems without others, particularly third parties, to observe his/her activity. For instance, in Blockchain-based systems, an attacker act as a miner to access the system's resources for mining purposes and protect their identity even from other miners interested in the same system resources [196]. Unobservability can also be related to unlinkability in the sense that an attacker attempts to disclose individually identifiable information of the users by only monitoring and analysing the data rather than linking it.

5. Discussion on security and privacy requirements for Blockchain-based Industry 4.0 applications

The interest in Blockchain technology and its implementation in Industry 4.0 has evolved to capture new opportunities. Many Blockchain-based applications have been developed and deployed across industries such as energy, finance and banking, healthcare and supply chain and logistics. Also, the adaptation of Blockchain technology in IoT, big data and cloud, crowdsensing and E-Commerce technologies has been explored. With the use of Blockchain technology across industries, considerations about security and privacy requirements are crucial.

This section provides a detailed discussion on the security and privacy requirements of various Blockchain-based Industry 4.0 applications. For each application, we provide an overview, present integration challenges with Blockchain technology and discuss additional security and privacy requirements to meet the needs of a secure environment. We also discuss how these requirements could be met effectively using security enhancement techniques.

5.1. Financial industry

The industrial age has influenced financial services such as internet payments, digital loans, and currency trading. A wide range of financial institutions benefits from the broad constructive expansion of digital innovation in the Industry 4.0 financial sector [197]. Therefore, Industry 4.0 has impacted the financial services sector in numerous ways. For example, it reduces human work and expenses while providing worldwide banking services [198]. The rise of Blockchain-based financial services also has a significant impact on financial institutions. For instance, intermediaries, centralised administration, fraud and burglary can be reduced using Blockchain technology and smart contracts, making it easier for the transparency mechanism to minimise financial services liability [199].

One of the key principles of Blockchain technology is to build a trustworthy and transparent relationship across multiple platforms from which users can obtain and share their data anonymously, storing transactions on a tamper-proof distributed ledger. The distributed ledger also plays a vital role in many cross-organisational situations where people may trust one other and help streamline the financing process. Banking institutions are increasingly adopting Blockchain to transfer digital assets to other banks locally or globally. In the financial industry, decentralised Blockchain networks eliminate financial intermediaries by allowing each financial partner to contribute to the network via a P2P network, so that direct money transfers can be made. In addition, each financial organisation maintains a distributed ledger with a finite volume of financial transactions per block. Fig. 8 presents an example to compare the traditional centralised financial system with the current Blockchain-based financial system. In conventional banking

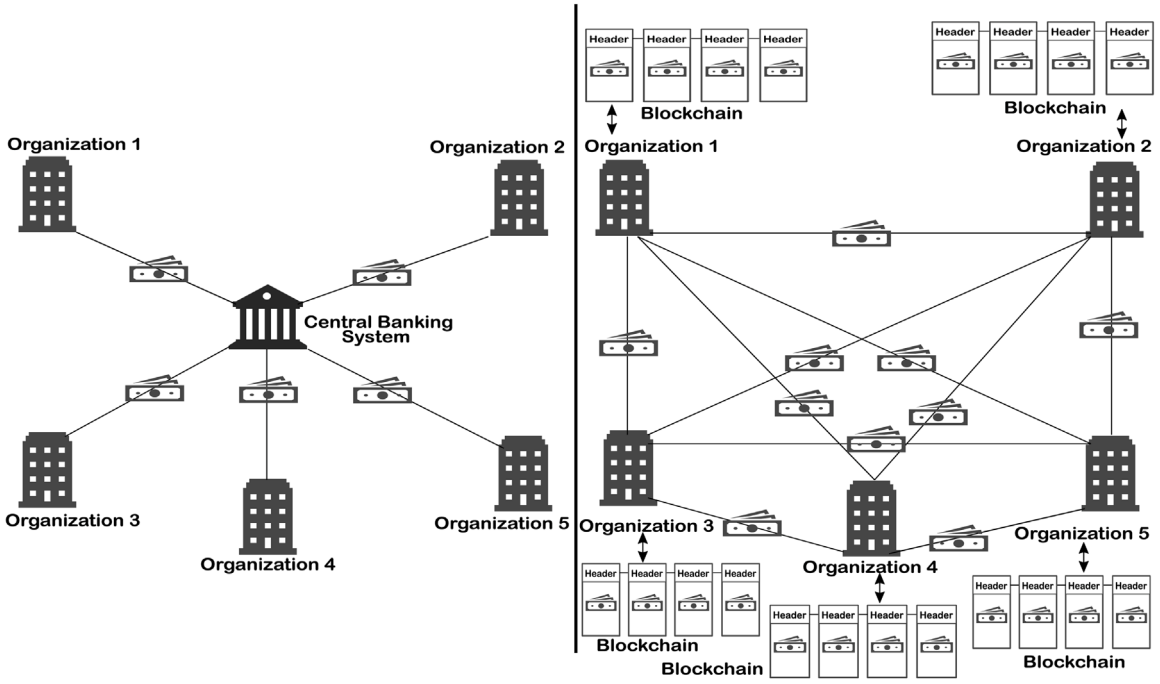


Fig. 8. An example showing the difference between current and Blockchain-based financial systems.

systems, the intermediary bank was entirely responsible for coordinating all transactions between multiple organisations. By eliminating the middleman, Blockchain technology allows the majority of network nodes to authenticate a transaction's legitimacy.

The integration of public Blockchain and distributed ledgers poses a significant potential challenge because stored transactions may leak *"sensitive and trading information"*. Another critical challenge for distributed ledgers is auditing or verifying recorded transactions since no central entity can afterwards. Wang and Kogan [117] proposed a Blockchain-based privacy preservation strategy to protect users' financial information to address the integration issues of distributed ledgers and Blockchain technology. Financial transactions on a private Blockchain network are secured using zero-knowledge proof and homomorphic encryption. Most Blockchain systems built for financial transactions suffer from *"high transaction costs", "propagation delays" and "latency"*. To efficiently utilise Blockchain-based financial system services, Zhong et al. [14] proposed a secure and lightweight payment scheme. The proposed scheme uses both digital signatures and a one-way hash function to provide system security and robustness. Off-chain storage is also used to store and access data from remote locations.

The notion of smart contracts allows users to communicate information and perform automated operations via a decentralised network without a trusted third party. However, users in a decentralised network confront a huge issue, as *"distributed privacy"* needs significant research effort from researchers. To achieve this, Kosba et al. [86] proposed a Blockchain-based cryptography model, known as the "Hawk". Hawk uses zero-knowledge proofs to record transactions on the Ethereum Blockchain in an inaccessible manner. The Hawk project is unique because the cryptography compiler develops the operations for the specific application at run time to protect the data inside the transaction. Kopp et al. [124] present another solution to the problem of *transactional privacy* in the payment system. The system protects users' privacy and financial transactions across a public Blockchain network by combining distributed system features such as cloud with privacy-enhancing strategies like ring signatures and one-time addressing.

To efficiently complete financial transactions, two clients are involved in Blockchain-based financial systems: full clients and lite clients. The full client is responsible for authenticating light clients with valid addresses. An attacker can easily detect and collect the entire clients' details by attacking the light clients. Kanemura et al. [200] fulfil the security requirement called *"deniability"* to achieve the light client's privacy in the Blockchain payment system. Aside from privacy, bloom filters prove deniability by using identical address patterns that meet metric criteria. Another critical requirement in the Blockchain-based finance system (primarily based on the principle of Know-your-Customer) is the *"validation"* of customers' transactions, where respective bank authorities can disclose customers' personal and confidential information. To address this issue, Bhaskaran et al. [201] suggested a public Blockchain-based data validation approach that uses smart contracts and double-blind sharing to protect client data. Biryukov et al. [202] presented a similar method to protect *"identity of customers"* in a decentralised public network. The proposed system used Ethereum smart contracts to overcome centralised system issues, including identity leakage and personal data disclosure.

Concerning privacy, most research aims to effectively solve transactional privacy in financial and payment systems. However, specific privacy-preserving solutions confront a trade-off; using expensive protocols slows down transactions. An efficient Blockchain-based approach called FPPP (Fast and Privacy Preserving Blockchain) is proposed by Li et al. [203] to achieve the performance of a system with guaranteed privacy of transactions. This approach uses an Ethereum Blockchain with an off-chain storage system to record multiple transactions, reducing computation time and transaction speed. To protect *"financial privacy"*, Ziegeldorf et al. [116] introduced the CoinParty technique, which used the distributed mixing method to merge many identities. Anonymity and scalability were preserved using the CoinParty technique using mix nets and threshold signatures. Another coin mixing scheme for Bitcoin and their related cryptocurrencies was proposed by Liu et al. [204], enabling the users to unlink their *"identities"* from the coins without the need of any central party. To ensure the privacy of the transactions, the approach uses cryptography primitives, including ring signatures and elliptic curve digital signatures.

5.2. Healthcare industry

Existing industrial healthcare models have discovered various vulnerabilities, including single-point failure and unauthorised alterations,

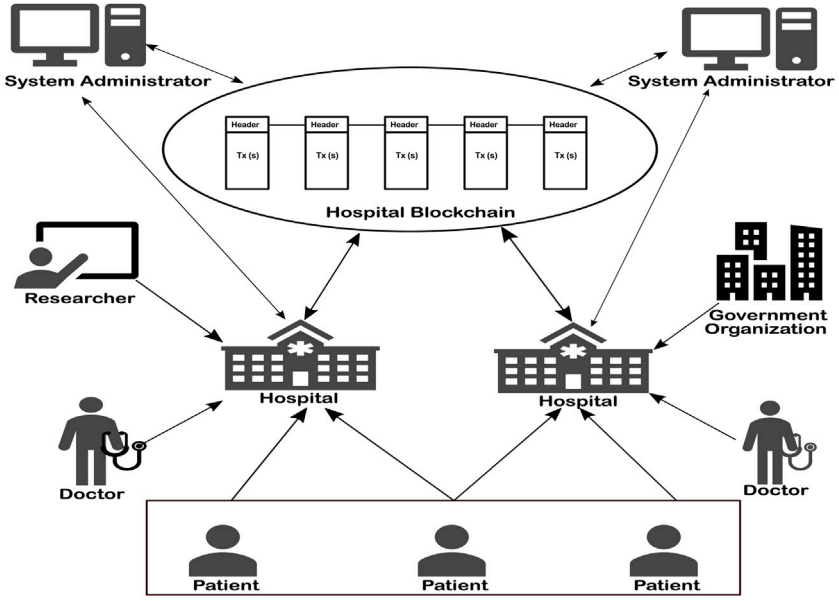


Fig. 9. An example of Blockchain-based healthcare industry model.

as well as other security and privacy issues [205]. Because traditional models are no longer dependable and stable, protecting patient data is crucial. In addition, effective health care management requires patient privacy [206]. Using Blockchain technology, Industry 4.0 can achieve data security, integrity, and privacy while eliminating a single point of failure [207].

Like other industries, Industry 4.0 is transforming the healthcare sector to accept innovative technologies. To help doctors and researchers better understand the diagnostic learning process, patient data is considered the most significant source of information in the healthcare industry. The healthcare industry uses IoT, cloud computing, and big data services to collect and store vast amounts of patient data, allowing doctors, researchers, and health workers worldwide to construct a digital global healthcare ecosystem called Healthcare 4.0 [208].

Blockchain technology has proved to be a promising technology due to its characteristics of transparency, immutability and security, and its ability to connect multiple organisations through the decentralised and distributed aspects of the network. The rise of Blockchain technology in the healthcare industry empowers electronic health records (EHRs) and telecare medicine by keeping patient data secure and anonymous while opening the door to medical researchers to perform reliable analysis. Moreover, Blockchain has made healthcare transactions more transparent and accessible, enabling patients to know more about their treatment options and providers [207,209].

The role of Blockchain in the healthcare industry is multifaceted. For example, the lack of a centralised network topology prevents a malicious user from targeting patient data stored in a single area. Furthermore, Blockchain technology allows patients to access their medical records securely. Medical records are frequently spread across numerous healthcare facilities, making accessing them challenging. However, Blockchain and distributed ledger technology can be used to securely access and trade patient medical records [210]. Using distributed ledger technology, doctors, researchers, and government organisations may securely exchange patient health records. This ledger also aids healthcare researchers in decoding the human genome. Blockchain can also improve the security and quality of mobile applications and remote surveillance systems used in healthcare. An example of a Blockchain-based healthcare industry model is shown in Fig. 9 in which patients, doctors, medical researchers, and government organisations can safely engage and communicate with each other utilising Blockchain technology features.

Zhang et al. [15] created the FHIRChain, a Blockchain-based scheme to meet the specific needs and requirements of national health infrastructure organisations who *"control and manage"* other health-related organisations and sectors. As a result, the proposed scheme carefully selects health organisations that can effectively connect patients with service providers (hospitals). To ensure that personal data is only accessible to the right people, *"access control"* is critical in EHR systems. A private Blockchain-based data-sharing network that allows doctors to access sensitive data of patients who have authorised access privileges was proposed by Hussein et al. [211]. This scheme uses discrete wavelet transformation to assure healthcare data privacy and anonymity. The proposed scheme additionally uses the query service interface to access and optimise Blockchain data. The experimental results show that the technique is scalable and resistant to various threats. Similar to the scheme [211], Dagher et al. [123] implemented Ancile, a Blockchain-based *"access control"* scheme of using patients' confidential and sensitive information without releasing it to outsiders. In addition to access control, the proposed approach ensures patient data privacy across numerous platforms.

Another significant contribution is put forward by Yue et al. [212] to solve the problems between patients and doctors about the *"controlling of sensitive information"*. The proposed scheme empowers patients by allowing them to send and receive data securely. With the help of Blockchain technology, Xia et al. [213] propose another *"'secure data sharing"* technique (MeDShare). Researchers must contribute significantly to electronic health data to provide secure solutions for presenting patients' data at multiple levels. With the help of machine learning, Kuo and Ohno-Machado [122] proposed a solution, called "ModelChain", to the problem of protecting patient data privacy. Sun et al. [214] developed the Blockchain-based privacy preservation approach that used patient attributes in attribute-based signatures to secure personal information. The proposed paradigm uses both on-chain and off-chain storage systems, with on-chain is used to store the original data while off-chain is used to store data indexes. Zhang and Lin [215] introduced BSPP (Blockchain-based safe and privacy-preserving) to *"protect the personal data"* from various health-related organisations involved in the process. The proposed approach uses both private and consortium Blockchains to store patient data securely.

Like in [215], Guo et al. [216] used an attribute-based signature scheme to provide *"validation of health record"*. Unless required by law, numerous authorities can sign and transfer data without disclosing patients' personal information. Azaria et al. [217] presented

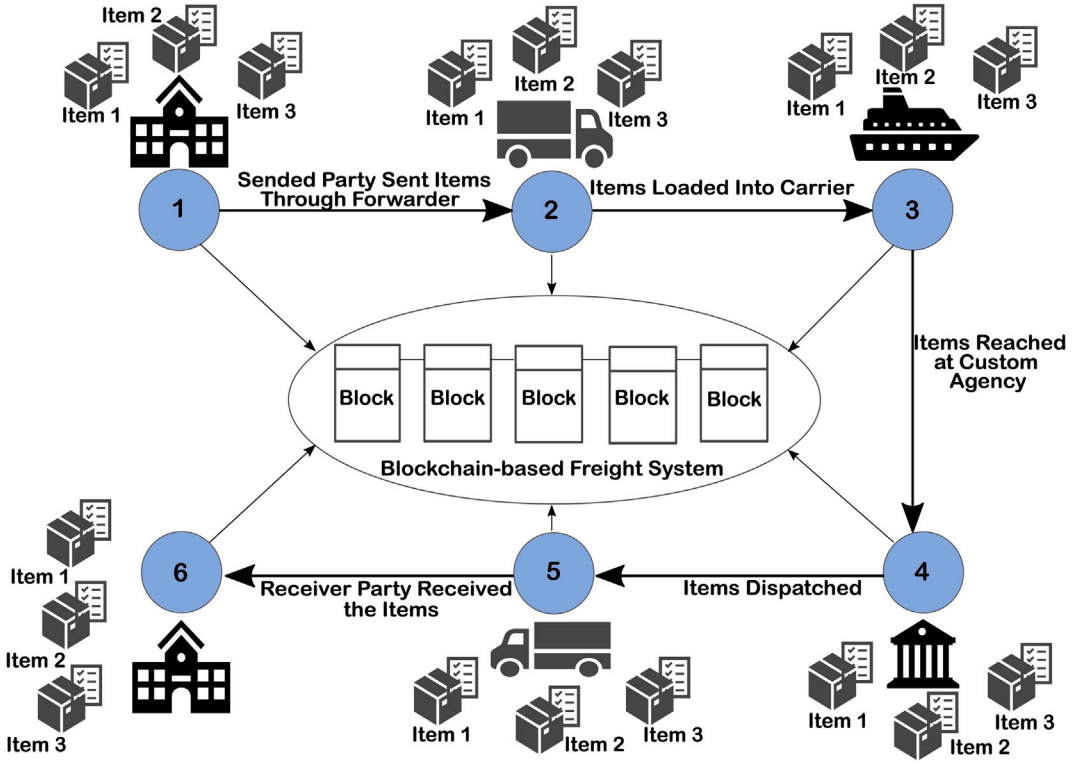


Fig. 10. An example of Blockchain-based transport and logistics – A complete process.

the MedRec, a unique Blockchain-based technology to secure patient medical data in a decentralised public environment. The proposed architecture enables doctors to control and view their data remotely. *"Location sharing problem"* in a Telecare Medical Information System is evaluated by Ji et al. [218]. Using a Merkle hash tree to store patient data hierarchically, a Blockchain-based location preserving technique called BMPLS was proposed to preserve multi-level location sharing. Aside from EHR security difficulties, there have been issues with distributed applications such as text *"retrieving, indexing and aggregating"* of data from several domains. Using the help of indexing and embedding technologies, Zhou et al. [219] introduced the distributed *"data vending"* framework that saves similar data into several locations with determined indexes.

5.3. Transport and logistics

Industry 4.0 is driving substantial and pervasive change within the transport and logistics sector because of a rise in supply chain demand and usage of modern and emerging technologies, as well as the potential to build the industry process's digital supply chain [220]. The transport and logistics sectors are increasingly automating to expand their market reach. New technologies and open standards enable firms to restructure their supply chains to support social and data-driven market dynamics, as well as innovation in traceability [221].

Flexible, sustainable, and online transportation ranging from a large container to a little box are becoming global industry standards in supply chains. These containers are constantly tracked and guided by the IoT [222]. The shipping business is vital in practically every industry and operation that handles large containers. If the contents of the container are not prohibited or mislabelled, the container is considered complete. However, due to bulk volumes and time constraints, the central agencies cannot inspect and audit each container's contents [223]. Moreover, the audit procedure includes tracking and selecting random items from the container with detailed information, such as item id, company name and addresses of both sending and receiving parties. Most auditing agencies kept all item data in one area or server, conveniently accessible to all auditing parties. However, unauthorised access or a single point of failure attack can compromise the security of shipping data. With the advent of Blockchain technology, decentralisation and immutability features allow the freight industry to transfer freight commodities securely.

The role of Blockchain technology in transportation and logistics is to maintain data integrity and security throughout the ecosystem. These systems also enable document exchange via a shared distributed ledger, eliminating the need for manual paper-based operations. Smart contracts cut processing times at customs checkpoints by automating and speeding up the customs clearance and approval procedure. The Blockchain-based transport and logistics framework, as an example, is shown in Fig. 10, which depicts the entire process of moving things from one location to another via shipping agents.

Vos et al. [16] proposed DEFEND, a secure decentralised Blockchain-based platform that achieves *"data privacy"* and anonymity of containers and store goods. The sending agency claims to transmit items, encrypts them, and sends them to other destination agencies. Only the destination customs agency can access and decrypt the claim. The suggested scheme's key contribution is data division among the many Blockchain parties. Aside from that, the proposed platform is efficient for both customs agencies and economic operators to undertake risk assessments on commodities without producing delays.

5.4. Energy industry

Industry 4.0 has paved the way for widespread grid-based utilisation of renewable energy sources by introducing a flexible framework called the smart grid (SG). Converging electricity networks and cutting-edge information and communication technologies (ICTs) such as smart metres, intelligent processing units and advanced communication protocols are used to address numerous barriers and vulnerabilities such as increased energy consumption, faulty transmission, increased construction costs and less efficient delivery in conventional meter systems. The

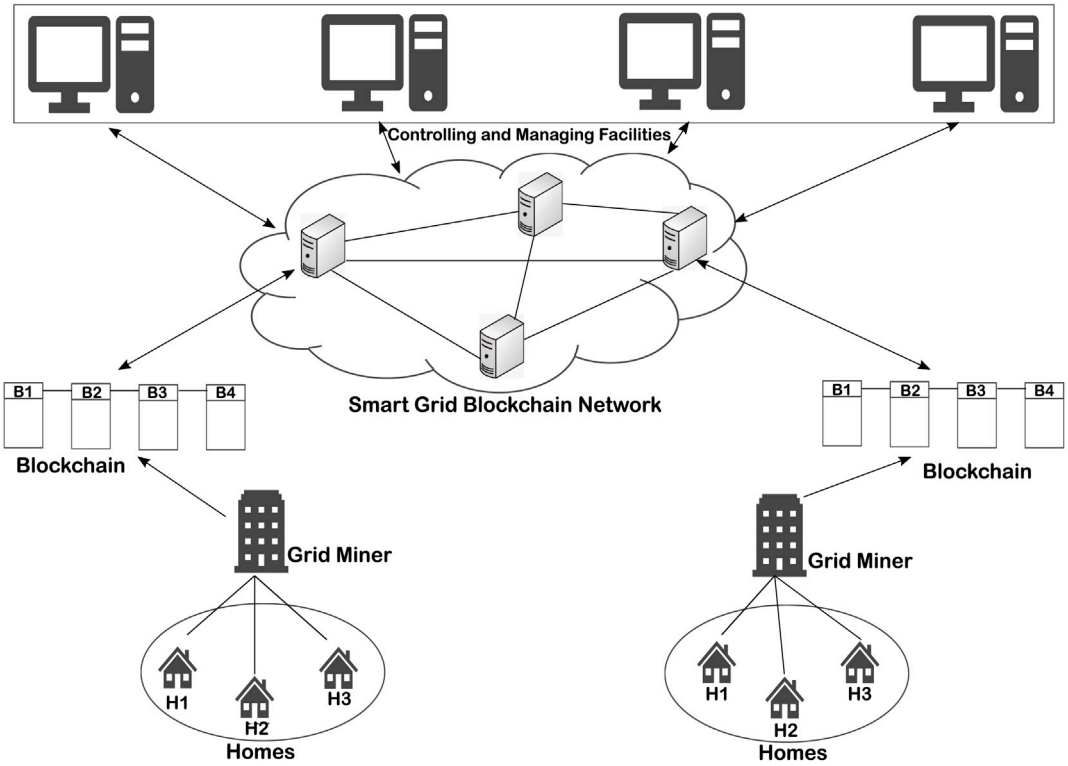


Fig. 11. An example of Blockchain-based smart grid system model.

SG is designed to control and track energy resources of consumers and suppliers more efficiently, accurately, functionally, scalable, safely, and economically [224,225].

One grid unit collects real-time data (sometimes referred to as metre reading) from smart metres put in various areas such as residences and industries. Most data collected is in low-level processes, allowing data analysts to find significant data outcomes and help coordinate subsequent utilisation, followed by more complicated analytics and planning [226]. The advanced countries are urging their power consumers to use smart metres to regulate and efficiently control power consumption. However, one major issue in the SG is the *"leakage of personal information"*. Personal information such as billing information, meter units, and addresses can pose serious security risks and privacy concerns for both consumers and suppliers [227].

Blockchain technology is an emerging technology that offers decentralised management and P2P energy trading, enabling secure, transparent, and efficient energy transactions. Blockchain technology is used to conduct network transactions in SG architectures. A transaction is a record of interactions between entities in the SG, such as producers, customers, distributors and managing authorities. Light nodes and full nodes are two common types of Blockchain-based SG entities. Light nodes are ordinary electricity users who pay their bills, while full nodes handle electricity and participate in Blockchain mining. A blockchain-based SG generally uses smart contracts to enforce transactions. These transactions include residual balances, balance deductions, grid benefit or loss, and so on [228]. Fig. 11 presents an example of a Blockchain-based SG model in which each grid acts as a miner to control and regulate the group of residences.

As previously stated, streaming data can reveal household users' personal information, causing significant security and privacy issues. An attacker can also collect power use history by following and analysing user behaviour patterns, such as turning off lights and charging smart metres. As a solution to these concerns, Guan et al. [229] presented a Blockchain-based *"privacy preserving"* and data aggregation technique for the SG, in which users are divided into subgroups, with each subgroup head recording the data of their sub-users. To protect users' data, each head uses pseudonyms to mask streaming data from other heads. Aitzhan and Svetinovic [17] designed a private Blockchain-based decentralised system that allows safe end-to-end communication between smart metres and SGs without the need for a trusted third party. A multi-signature technique and anonymous encrypted messaging are utilised to protect the anonymity of the trade transactions between end-users. Rottondi and Verticale [230] designed a Blockchain-based smart meter architecture in which public users can securely *"transform their data"* to the SG. The proposed system uses a secure multi-party protocol for encryption and authentication that ensures users' data is authentic without revealing it to the SG.

5.5. Technology industry

The technology industry includes internet-of-things, big data and cloud computing, crowdsensing, and E-Commerce as Blockchain-based Industry 4.0 applications.

5.5.1. Internet of Things

In Industry 4.0, practically all embedded equipment, such as robots, machines, and tools, include sensors to gather data from the environment and work accordingly. The IoT has revolutionised human life by enabling omnipresent applications that automate and streamline daily operations. In conjunction with Fog computing, IoT plays a significant role in offering time-sensitive services such as disaster-related services, smart transportation and smart health services [231,232]. However, improving the IoT's present paradigms requires ongoing technological research and development. Aside from the fact that this technology makes our lives easier and safer, it also raises many performance, security and privacy concerns. Due to its remarkable properties such as decentralisation, immutable ledger, transparency and data auditability, Blockchain technology has bridged the gap between IoT services and security challenges.

The use of Blockchain in IoT can help address security and performance issues. Using Blockchain technology in IoT applications adds

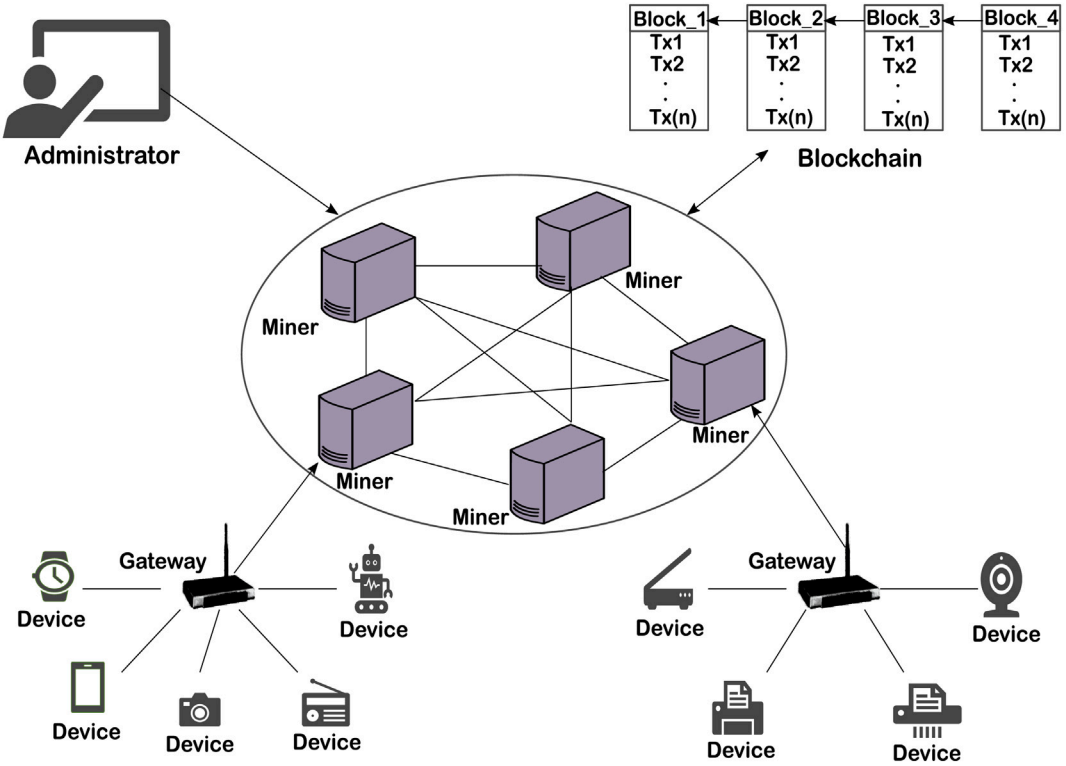


Fig. 12. An example of blockchain-based Internet of Things (IoT) network.

another layer of security, making it difficult for attackers to access the network. The overall contribution of Blockchain to IoT systems can be summed up as follows. An immutable distributed ledger in a Blockchain system makes it nearly hard to remove current data records. The decentralised network eliminates the requirement for a trusted third party. Furthermore, an accountability feature allows authorised users to access the network and analyse previous transactions. Blockchain removes the processing overhead associated with IoT gateways by promoting trust between parties. [233]. Fig. 12 presents an example of a decentralised IoT network using Blockchain technology. In this example, IoT devices are light nodes with limited resources, requiring identification and authorisation for security and scalability. The miners' nodes are full nodes that operate as gateways for IoT devices to interact with the Blockchain securely. Miner nodes are also responsible for validating and adding transactions to the Blockchain. The administrator authority is in charge of implementing the system and controlling network nodes.

Cha et al. [234] proposed a Blockchain-based system for IoT users that provides a secure gateway to achieve *"user privacy"* in the IoT network. The secure gateway prevents unauthorised access to users' data stored on the Blockchain in the proposed concept. To accomplish *"authentication of users"* in IoT, Wan et al. [235] proposed a Blockchain-based technique that utilises a digital signature method to provide *"security and privacy"* among various industrial processes. Le and Mutka [236] presented the CapChain, a novel access control scheme that allows IoT devices to *"store and manage their data"* on a public cloud without releasing any personal information. In this scheme, anonymisation protects sensitive information, such as identities, from unknown sources. To achieve *"protection of sensor data"* in the IoT network, Chanson et al. [237] presented a certification-based Blockchain approach. The certification authority permits users to undertake authentication in three stages to prevent malicious activity in the system.

Nowadays, many home appliances are connected to the internet to monitor and manage the home environment remotely. The growing demand for smart home devices presents issues of *"security privacy, efficiency, and scalability"*. Singh et al. [238] presented a Blockchain-based smart home network to achieve *secure communication* between IoT devices. The proposed system uses multi-correlation to analyse malicious network traffic. Dorri et al. [239] proposed another IoT-based smart home model to ensure *"security and privacy"* of users. The proposed Blockchain smart home design uses three primary components: cloud, overlay network, and home appliances. Cloud storage, for example, is used to store future data that can only be retrieved through separate transactions.

5.5.2. Big data and cloud computing

Big data analytics uses modern computing techniques to find important patterns in large datasets to assist organisations in detecting trends and consumer preferences. In Industry 4.0, smart factories use data analytics to forecast when maintenance and operations are required. For instance, using cloud computing and IoT technology, manufacturers can better manage their supply chains by identifying track patterns [240]. Cloud computing is a set of on-demand resources and services that customers can employ to do various tasks. Cloud Service Providers (CSPs) monitor and decide the applicability of on-demand access with the available resources. A growing number of industrial organisations use cloud computing services for data computation and storage.

The Cloud and Industry 4.0 are a winning combination, as both technologies took years to develop and earn industry acceptance. This integration allows organisations to rethink their entire digitisation process and adapt their current architectures to a larger industry market. By combining big data with cloud computing services, millions of users now have access to very complex data in an ever-changing technological environment—Cloud computing, big data, and the IoT all present new potential for connectivity and information sharing. However, such sensitive data must be managed and maintained consistently. Blockchain and cloud computing delivers new levels of data security and service availability to the industrial community. The decentralisation, immutability, and transparency of Blockchain can be used to tackle most cloud research issues.

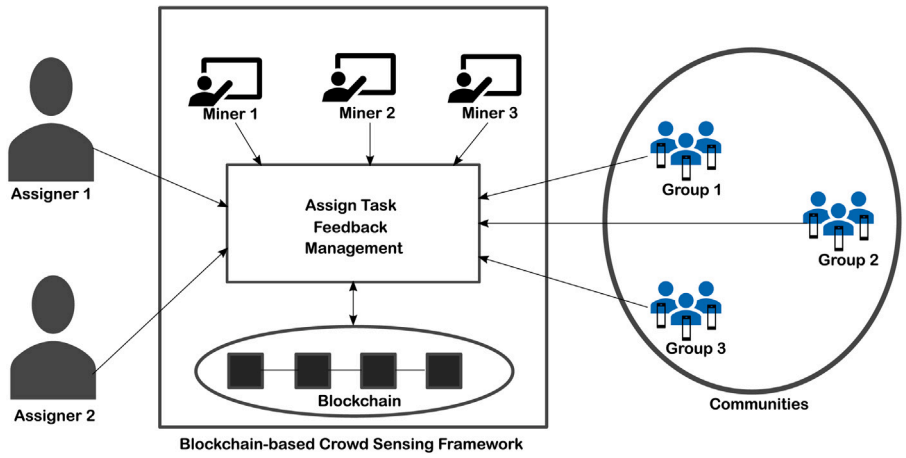


Fig. 13. An example of Blockchain-based crowdsensing framework.

Blockchain technology has various applications in cloud computing and big data. In the case of data management, there is no single point of failure. Aiming to provide immutable ledgers, Blockchain technology offers higher security than traditional providers. In terms of storage, nodes that help facilitate transactions can manage a cloud storage network, providing users access to storage on their devices. Cloud-based user data can also be divided into small chunks and distributed over the network using advanced cryptographic techniques.

CSPs are exclusively responsible for granting proper access to cloud users utilising various authentication and authorisation services in terms of security. Most cloud computing services have a single point of failure, exposing users' personal information. To address the issue of *"authentication"* in cloud computing, Lu. et al. [241] proposed a Blockchain-based decentralised authentication system for preserving an exhaustive list of users' access control permissions on the Blockchain. The proposed model integrates authorisation and accounting features that are often seen in digital currency systems. A simple one-way hash function is used to secure the ties between users' transactions to strengthen security. Another Blockchain-based approach for trusted *"data sharing"* with a cloud service provider is developed by Zheng et al. [49]. The suggested approach uses Paillier cryptography to protect data stored in distributed databases. Fan et al. [242] proposed a Blockchain-based privacy preservation strategy to *"secure users' information"* being communicated via a content-centric 5G mobile network. The proposed scheme effectively established a secure data transfer connection between service providers and users. The access control method ensures access to cloud resources as well as data protection.

5.5.3. Crowdsensing

Giving individuals access to important resources has been a popular approach for discovering new advances in information and communication technologies. Crowdsensing is a common approach of leveraging the public for authentic knowledge discovery [243]. Crowdsensing has shown to be beneficial in Industry 4.0, cutting human effort costs and increasing access to innovative ideas. Depending on the sector, from production to distribution, individuals' data in knowledge discovery platforms varies substantially. With the help of crowd-sourced information and experience, high-throughput computational frameworks help streamline organisational processes. Crowdsensing aids in monitoring ecosystems, mapping, and exchanging information with people. For example, crowdsensing can reduce energy use in the energy sector by monitoring user behaviour and thermal comfort. Crowdsensing can help industries reduce maintenance cycles and track environmental variables and machine failure [244]. Humans are equipped with sensing devices such as smartwatches or trackers to sense data from their surroundings and take action in the industrial process. The quality of data acquired by sensing devices depends on the number of individuals and their skill level. However, the crowdsensing method has a flaw that precludes new users from entering the network due to the leakage of personal information or data of participants. Moreover, crowdsensing also confronts issues in fact discovery, knowledge quality, and estimation quality [245].

Blockchain technology is used in crowdsensing to circumvent these limitations to allow the most significant number of highly qualified persons to participate. Crowdsensing uses a rewarding mechanism to attract and incentivise skilled users to participate in the data collection process. Interconnecting blockchain with existing crowd-sourcing systems aims to develop decentralised crowdsensing systems that eliminate single points of failure and allow all participants to collect data fairly and equally. Furthermore, the distributed ledger enables the immutability and traceability of users' data and feedback in various activities. Increasing worker efficiency, creating a fair remuneration system, preserving confidential data, and minimising deployment costs are all goals of Blockchain technology in crowdsensing [246]. Fig. 13 presents an example of a Blockchain-based crowdsensing framework, which consists of various nodes such as assigners, user groups, and miners that all contribute to and govern the overall crowdsensing process.

To demonstrate the concept of using Blockchain in crowdsensing, Wang et al. [247] proposed a Blockchain-based *"privacy-preserving"* incentive scheme for crowdsensing applications that enables highly skilled users to participate in the sensing process publicly and securely in exchange for high incentives. The proposed mechanism employs the k-anonymity scheme to preserve the privacy of skill users. Furthermore, Cai et al. [248] proposed another strategy for *"protecting the personal information"* by the use of knowledge discovery without releasing any personal information. The public Blockchain platform collects knowledge in this manner from diverse sensing users located in distributed locations. Finally, to guarantee the *"guaranteed privacy"* of mobile users and crowdsensing providers, Chatzopoulos et al. [249] developed a Blockchain-based crowdsensing method that specifies smart contracts to ensure a secure relationship between both. The proposed scheme combines a secure multi-party computation algorithm with smart contracts to protect users' privacy and incentive payments.

5.5.4. E-Commerce

Electronic commerce (E-Commerce) is widely regarded as a major trading platform for buying and selling online goods or services. However, these platforms do not secure client transactional privacy, such as content, addresses, account data, or trading information. Therefore, traditional E-Commerce platforms have been migrated to Blockchain technology to allow clients to conduct fair transactions without a

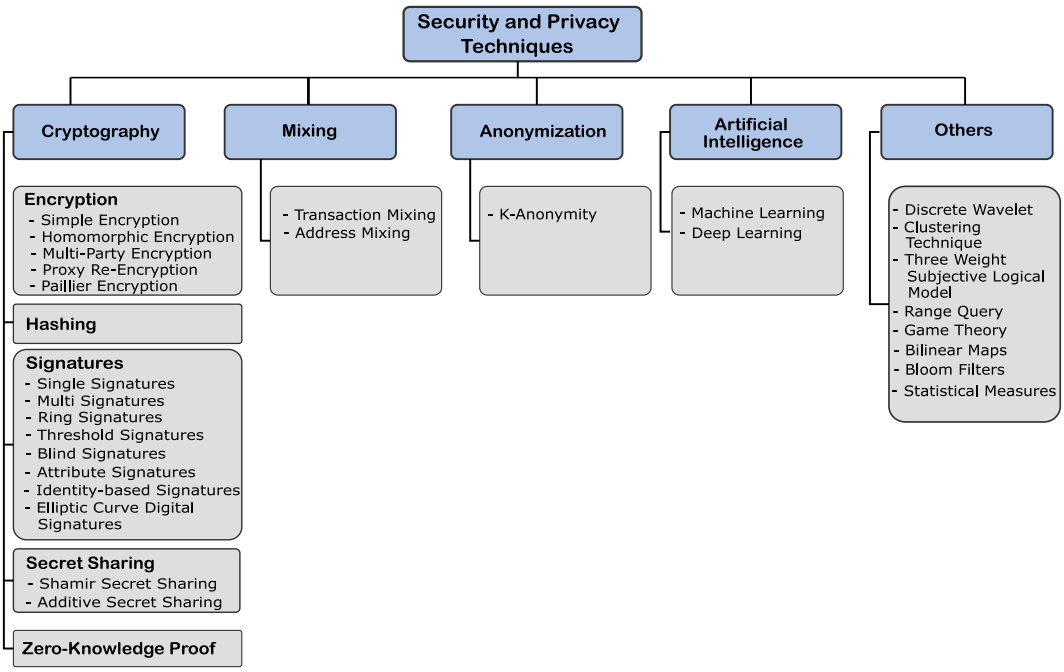


Fig. 14. A taxonomy of security and privacy techniques for Blockchain-based Industry 4.0 applications.

trusted intermediary. However, while numerous Blockchain-based security mechanisms have been proposed to protect financial transactions, privacy and speed are still challenging. To address this issue, Li and Wang [250] proposed RZKPB – a Blockchain-based *"Privacy Preservation"* technique that prevents financial data from being kept in plain-text on the Blockchain. The suggested solution uses cryptographic primitives like hashing and signatures to validate transactions and establish trust between trading partners.

6. Security and privacy techniques for Blockchain-based Industry 4.0 applications

This section describes the security and privacy techniques employed in various Blockchain-based Industry 4.0 applications. Techniques for security and privacy include cryptography, mixing, anonymisation, artificial intelligence and few others, such as discrete wavelet, clustering and bloom filters. These categories are further divided into sub-categories to comprehend security and privacy measures further. Fig. 14 shows a taxonomy of security and privacy techniques.

6.1. Cryptography

Cryptography is a method of securing communication between parties using a mathematical set of rules and logic. For example, a plaintext is converted into a hidden text using a secret key only known to the sender and receiver. Cryptography protects information from theft or modification, provides authentication, and ensures user and data access [251].

6.1.1. Encryption

Encryption is the most frequently used technique in cryptography for transforming plain text or data into an encoded version that can be decoded only by authorised parties holding the same secret key. Secret keys offer data security between end-to-end components and should not be shared with other network components. Encryption is commonly used in Blockchain applications to address security and privacy issues. In this section, we divide encryption into different sub-extensions.

- **Simple Encryption:** As stated previously, encryption converts plain text into a format that others cannot read. There are two forms of encryption: symmetric and asymmetric. In the symmetric method, two parties share a secret key to encrypt and decrypt data. In the asymmetric method, each party has two public and private keys to encode and decode data, respectively.
- **Homomorphic Encryption:** Simple encryption does not allow users to conduct meaningful computations on the ciphertext; therefore, this is an enhanced encryption version. The fundamental benefit of homomorphic encryption is that it allows users to perform sophisticated mathematical operations on encrypted data without losing the original data. Also, in cloud computing, homomorphic encryption is the most widely used method for analysing encrypted data stored in the public cloud. In Blockchain-based applications [49,117], homomorphic encryption protects the privacy of users by not revealing personal or sensitive information to others.
- **Multi-Party Encryption:** Multi-party encryption (or multi-party computation) is another encryption method in which numerous users work together to encrypt data. Using multi-party encryption in secure computations prevents an attacker from acquiring any targeted user's confidential information. For example, [169] uses multi-party computation to ensure user security and privacy in a decentralised Blockchain network.
- **Proxy Re-Encryption:** Proxy re-encryption is a third-party encryption mechanism that converts plaintext into ciphertext without knowing the content. For applications where users desire to share encrypted data without disclosing their secret key, proxy re-encryption is widely employed as a public-key cryptography solution. For example, proxy re-encryption is used in Blockchain-based IoT applications [10,17,123,215,216,218] to communicate private contracts between users to control and manage IoT devices.
- **Paillier Encryption:** Paillier encryption, also known as probabilistic asymmetric cryptography, is a key-pair based algorithm that uses two keys, public and private, to encrypt and decrypt data. In Paillier cryptography, additive homomorphic encryption applies to the given set of messages, and each message is encoded/decoded with the key pairs of respective users. Considering

the implementation of Blockchain in IoT [234] and cloud computing [49] domains, Paillier cryptography is used to achieve privacy and anonymity in such decentralised applications.

6.1.2. Hashing

The use of hash functions in cryptography ensures data integrity because any change in output value can be quickly identified. Apart from data integrity, cryptography hash functions are employed in digital signatures and authentication systems. The best cryptography hash function must have the properties listed below. First, it must be collision-resistant, meaning that two identical inputs must provide different outputs. Second, no one should be able to reproduce the identical input from output values. Finally, the hash function should easily detect minor data changes.

In Blockchain, cryptography hash functions are used to link and maintain the integrity of blocks so that the previous hash of the block is placed in the header of the following block to construct a complete hash chain.

6.1.3. Signatures

Historically, the signature method was used to authenticate documents by placing handwritten signatures at the bottom [252]. However, in a digital world, signatures are used to secure software ownership and digital communication by ensuring message authenticity, integrity, and non-repudiation [253]. The following types of signatures are used in Blockchain-based industrial 4.0 applications.

- **Digital Signature:** Digital Signature is a public-key cryptography approach that uses a private key (or secret key) to link the identity of users to their digital data. The digital signature method validates the authenticity of the data delivered from the sender to the receiver [254].
- **Multi-Signature:** Multi-signature is a digital signature technique used to confirm the validity of digital documents that allows multiple persons to sign one document instead of one user per document. For example, in government organisations, a document is authenticated and proven by numerous people of different ranks (bottom-up) [255]. In Blockchain, the amount of signatures required for a document is determined before the generation of addresses [29].
- **Threshold Signature:** Unlike multi-signature, threshold signatures require a defined number of persons to provide a valid signature for the document [256]. To illustrate the proof of threshold signatures, [116,257] proposed the Blockchain-based e-voting scheme to achieve the security and privacy of voters.
- **Ring Signature:** A ring signature is another essential digital signature that operates in a group pattern arranged in a ring shape to provide better security and privacy to group users. In a group, any member with a valid cryptographic key can generate the signature, making it difficult to verify who generated the signature with their public key [258]. In Blockchain-based applications, ring signatures are employed to protect the input transactions signatures with the public key of any node [124,204].
- **Blind Signature:** This signature algorithm treats the user as a blind person throughout the signature process, generating a blind signature without knowing the actual content. Blind signatures are usually employed in privacy-preserving protocols to achieve the anonymity of users (or signers) belonging to different parties [259]. In addition, blind signatures are extensively utilised in Blockchain e-voting applications to ensure voter and candidate anonymity [201,260].
- **Attribute-Based Signature:** Attribute-based signature (ABS) is a modern digital signature mechanism that allows users to sign documents with fine-grained access control policies. Each user in an attribute-based signature has unique attributes; hence the changing nature of attributes might result in unique signatures. The ABS is commonly used in Blockchain-based E-health applications that value the privacy of patients in a secure way [35,214].
- **Identity-Based Signature:** An identity-based signature (IBS) scheme has some advantages over other digital signature schemes in terms of implementation and computation. However, it has the disadvantage of increasing the signature length by combining two different signatures, one from the user and the other from the certification authority. Further, it requires two verifiers to validate the signatures. In Blockchain, the IBS method is frequently used in authentication systems in which users require authentication before using system resources [261].
- **Elliptic Curve Digital Signature Algorithm (ECDSA):** To generate a data signature, this approach combines elliptic curve cryptography with digital signature algorithms. It is the most powerful digital signature algorithm and is widely utilised in IoT applications [262]. Furthermore, the ECDSA is used in Blockchain applications to verify transaction integrity and authenticity.

6.1.4. Secret sharing

In cryptography, secret sharing is a common technique used in distributed computing. In this technique, one secret is shared equally among all group participants to build trust by fulfilling the following criteria: a sufficient number of participants and the conditions and types of shares to reconstruct the share later. The (n, m) - threshold scheme is utilised to build the secret in this scheme [263]. Using secret sharing with Blockchain-based applications reduces the costs of data exchange and storage on distributed ledgers.

- **Shamir Secret Sharing:** To keep the confidence between most participants, this security approach uses encryption to provide evidence from most community participants securely. For example, one person must be trusted in distributing private keys. In the Blockchain, the secret Shamir technique requires a number (or secret) to define the threshold value [264].
- **Additive Secret Sharing:** Like the Shamir secret sharing technique, additive secret sharing uses multi-party computing to provide privacy by ensuring that no one can retrieve the full value of a secret using their shared secrets [265]. The additive secret sharing approach is advantageous in Blockchain applications because it uses homomorphic encryption for bitwise transactions.

6.1.5. Zero-Knowledge Proof

The notion of Zero-Knowledge Proof (ZKP) is used in applied cryptography to ensure security properties such as anonymity, privacy, and transaction verification. In ZKP, a verifier party verifies the claimant's proof and gives proof of knowledge without revealing personal information [266]. Furthermore, ZKP has the advantage in Blockchain that any validator (or miner) can prove a shared secret challenge even if the claimant provides no information (zero-knowledge) [267].

6.2. Mixing

The mixing service is critical in establishing privacy by concealing both sender and receiver transactions so that no one knows what is inside. Using the mixing technique, both incoming and outgoing transactions are mixed. This method aims to segregate transaction details from sender/receiver identities. In Blockchain applications, there are two types of mixing: transaction mixing and address mixing.

6.2.1. Transaction mixing

In the Blockchain, transactions are stored in the distributed ledger and are open to everyone for graph analysis and other purposes; thus, an adversary can easily track individuals by knowing the information stored in the Blockchain. Transaction mixing services enable users to mix their financial transactions so that others cannot trace the original user who initiated the transactions. These services receive transactions from different users, mix or shuffle them, and transmit them to different addresses.

However, the fundamental difficulty noted in current mixing services is that it depends on third parties that keep the transactions (coins) for some time. As a result, malicious parties frequently target or operate these systems, stealing coins from both participants' accounts. CoinJoin and CoinShuffle are two commonly Blockchain-based mixing services proposed that remove the need for a third party to mix financial transactions between the sender and receiver to provide unlinkability against malicious servers, verifiability and resilience.

6.2.2. Address mixing

Address mixing (or address shuffling) is a mixing service where an input address and an output address are connected. Explicit and implicit address shuffling are two techniques to implement the address mixing service.

In explicit address shuffling, the mixing party knows the sender and their addresses. For example, CloakCoin [268] employed explicit address shuffling to link input and output addresses. In an implicit shuffling service, the mixing server cannot match sender and receiver addresses. Maxwell's CoinJoin cryptocurrency [269] utilises blind signatures to implement implicit address shuffling.

6.3. Anonymisation

Anonymisation is a data hiding technique that assures users remain anonymous throughout the process and makes it hard for others to identify them or their data saved in the database. The main aim of the anonymisation process is to protect users' privacy with cryptography or different generalisation methods.

6.3.1. K-anonymity

The most prevalent generalisation technique is K-anonymity, which performs complicated data operations on users' data to achieve anonymisation. For example, data must satisfy the k-anonymity property if it cannot be identified from the remaining k-1 users involved in the computing process. Furthermore, the k-anonymity property ensures that the chance of identifying users in a data set is not greater than 1/k [270].

The two most frequent methods for k-anonymity are generalisation and data suppression. However, in the Blockchain, k-anonymity is the primary approach for achieving public privacy [271].

6.4. Artificial Intelligence

Artificial Intelligence (AI) is a combination of distinct intelligence characteristics and techniques for utilising native hardware that can enhance thinking by utilising neural network concepts via machine learning and deep learning [272]. AI algorithms have also been utilised in Blockchain-based applications to evaluate user activity on the Blockchain network and employ various heuristic approaches in a predictable manner [273].

6.4.1. Machine Learning

Machine Learning (ML) is the most fundamental and frequently used technique in artificial intelligence. It enables the system to learn from experience and make an automatic decision to improve itself by providing input values to machine learning techniques, typically in the form of learning data, heuristic observations, and experiences.

The integration of blockchain technology and machine learning techniques enables the development of Blockchain-based applications, which fundamentally alters the way decentralised applications are considered [274]. Furthermore, using analytical learning methods, machine learning can help improve the security of Blockchain systems and create new privacy-preserving models for decentralised applications [272].

6.4.2. Deep learning

As a widely utilised artificial intelligence (AI) approach, Deep Learning can execute various tasks with high accuracy and has a substantial impact on many different industries. Like machine learning, deep learning instructs the computer through text, images, audio, and video. However, because deep learning uses massive data sets to deliver high-quality results, data security is a critical issue that demands considerable security and privacy solutions [275].

Using Blockchain technology, deep learning features can secure user data and meet application privacy requirements. Also, decentralised deep learning is utilised with Blockchain applications to provide data consistency and transparency [276].

6.5. Others

Many other approaches are available to respond to the security and privacy problems in the Blockchain-based Industry 4.0 applications. For example, a solution to privacy problems in the E-Health application [211] is a discrete wavelength transformation method in which a conversion strategy is utilised to convert the wavelets into discrete sampling in order to achieve accurate frequency and timing information of stored data. Blockchain security uses the discrete wavelength transformation with cryptography functions to generate the key pairs for encryption/decryption. To secure vehicle users' privacy, [10] employs a clustering technique in which each vehicle is linked to and tracked by its controlling unit, called the RSU (Road-Side Unit). The unit authenticates the vehicles using some asymmetric cryptography primitives. Another privacy preserving approach, called the three-weight subjective logical [120], is employed in the vehicular network to protect vehicles' data. This approach is purely based on a probabilistic logic model in which data is assigned a different weight to calculate the subjective logic in the decision-making process. There are also a few other methods, such as Range Query [121], Game Theory [249], Bilinear Maps [215], Bloom Filter [124] and Statistical Measures [277] which are used to deal with the problem of security and privacy in different Blockchain-based applications.

7. Security and privacy attacks on Blockchain-based Industry 4.0 applications

This section describes the various security and privacy attacks on Blockchain-based Industry 4.0 applications, in which an attacker uses different approaches to obtain data and information. The primary advantage of a Blockchain is that it is based on a decentralised P2P network, which provides a plethora of benefits, including trust, security, transparency, traceability, and accessibility. However, contrary to common opinion, the Blockchain's P2P architecture also contributes to many attacks against industrial blockchain applications. Since our survey paper aims to integrate Blockchain technology with various industrial applications, it is critical to note that the attack vectors covered in our paper include attacks on both the core P2P network and the subsequent industrial applications built on top of the Blockchain network.

We classify the security and privacy attacks discussed in our work into several categories, including layer category, attack nature, attacker's objective, security breaches occurred, exploited vulnerabilities, target applications, and countermeasures. The data layer, the network layer, the consensus layer, the incentive layer, the smart contract layer, and the application layer are all included in the layer category. The attack vectors fall into two categories: P2P networks and blockchain applications. A P2P network is a decentralised inter-process communication model comprised of a collection of individual devices (nodes) that collaboratively store and share files. P2P networks can be classified as structured, unstructured, or hybrid. Unstructured P2P networks are established by nodes randomly connecting, but structured P2P networks are organised, and every node may efficiently traverse

the network for the requested. For simplicity, we grouped attacks based on unstructured or structured P2P network models into one P2P system category. We also categorise the security breaches into three different primary branches: (i) breach of confidentiality, (ii) breach of integrity and (iii) breach of availability. In breach of confidentiality, an attacker tries to listen to the communication between two parties without the owner's consent of the data rights. In breach of integrity, an attacker aims to change or modify the original data into another form after listening to the communication channel. Undoubtedly, breach of availability is one of the most severe breaches because an attacker intends to disrupt the network or data services using malicious attacks, such as a DoS, to make these services unavailable to legitimate users. Moreover, we explain each attack with the goals and objectives to expose vulnerabilities and threats in the system. We also sort attacks and targeted applications whereby some attacks, such as 51% attacks, double spending attacks and selfish mining attacks, are specially designed for Bitcoin and Ethereum applications. However, most attacks can also be targeted generally to the other domains, including IoT, SG, medical and vehicles. We also present state-of-the-art solutions and techniques to protect the applications and their underlying systems against a subset of such malicious attacks.

Table 4 presents a summary of the reviewed attacks along with their layer categories, attack nature, attacker goals and objectives, security breaches and vulnerabilities, as exploited in the system or network. In addition, we also include the targeted applications suffering from the potential threats and vulnerabilities and discussed prevention methods to overcome them.

7.1. Data layer

The main functionality of the data layer is to define the physical structure and underlying attributes of a single block, followed by encapsulating the data and specifying the chaining structure of connecting blocks in the Blockchain. In addition, the data layer is also responsible for handling data stored on the Blockchain (on-chain) and in the database (off-chain). Below is a detailed explanation of the various attacks that have targeted the data layer of Blockchain architecture.

7.1.1. Malleability attack

A malleability attack is a type of double-spending attack that frequently occurs in Blockchain-based systems due to the malleability of signatures. In this attack, an attacker is able to broadcast two transactions to the Blockchain network, resulting in the appearance of double-spending [278].

Numerous countermeasures have been proposed to this attack, including segregated witness [279], specification modification [280] and time commitment approaches [281].

7.1.2. Time hijacking attack

A time hijacking attack primarily results from a vulnerability discovered in the timestamp protocol used by Bitcoin and the majority of other comparable cryptocurrencies. The aim of an attacker in this attack is to modify the time counters of all nodes and the network on which they are located.

One approach to resolve this issue is to build hardware-oriented systems that benefit from replacing outdated network time technologies. Additionally, time hijacking attacks can be avoided through the use of tolerance range restrictions and enhanced network time protocols [282].

7.1.3. Quantum attack

Quantum attacks are typically directed towards the cryptographic component of the Blockchain, with the primary goal of resolving the mathematical problem of cryptographic dependency. For example, attackers may execute quantum attacks on Blockchain to cause problems with multiple consensus protocols such as PoW.

Khalifa et al. [283] presented a few security measures for quantum elastic Blockchain networks through the use of a quantum post-signature technique to mitigate quantum attacks.

7.1.4. Replay attack

A replay attack is a widespread problem in Blockchain systems, as it can result in a significant delay in communication between two parties. In such attacks, the adversary retains certain transactions on the network without submitting them to the miners for verification.

Recent work has demonstrated that this problem can be solved through a variety of measures, including adding a nonce to each transaction, mixing techniques, and employing digital signature methods [284].

7.1.5. Modification attack

An adversary always tries to change the broadcasted transactions in the Blockchain network before sending them to the miners for verification. As a result, an attacker can breach the integrity of the system to launch harmful activities and take complete control of the underlying system.

To address this issue, several techniques [35,122,169] based on cryptographic operations are proposed, such as attribute-based signatures and consensus procedures in order to ensure that Blockchain systems are resistant to modification attacks.

7.1.6. Fault injection attack

In Blockchain-based systems, the adversary always attempts to impersonate the Blockchain by adding fake data or blocks to the existing Blockchain, using fault injection methods. The purpose of the fault injection is to either stop the execution of specific transactions or disrupt the complete set of code (or transactions). This vulnerability generally exists in the system due to insufficient code validation, for example, the avoidance of integer flow conditions in smart contracts.

To illustrates the idea of a fault injection attack, [121] proposed the Blockchain-based vehicular system in which different cryptography methods, such as hashing and digital signatures, were used to protect the system from injection attacks.

7.1.7. Upgraded attack

An upgraded attack is a type of data attack in which an adversary changes the trust values, also referred to as threshold values, of the participants in the system. In an upgraded attack, the Blockchain miners, acting as the fake miners, can control the overall network to launch the upgraded attack. In addition, multiple fake miners can change the current threshold value to perform malicious activities in the network.

A possible solution to overcome this problem is proposed in [285], in which digital signatures are utilised to verify the defined threshold values in the vehicular network.

7.2. Network layer

The network layer is primarily responsible for information transmission between Blockchain nodes. As we all know, Blockchain operates on a network known as a P2P network, in which peers exchange knowledge about the state of the network. For example, any node in the public Blockchain may enter the network. That node can be any ordinary home computer or mobile device; therefore, network layer protection must be implemented to prevent further network attacks. As discussed in detail below, the network layer is vulnerable to the following attacks.

7.2.1. 51% Attack

One of the common vulnerabilities found in the Blockchain network, especially in Bitcoin and Ethereum applications, is the 51% attack. A group of miners wants to control the network with more than 50% mining (or computing) power [286]. In this case, the 51% controlling group controls the overall Blockchain and creates wrong decisions to dispute the reputation of a network. Additionally, with the successful execution, 51% of miners will be able to move all bitcoins from various user accounts to their targeted accounts.

One approach to solve this problem involves selecting random miners and restricting them from recycling their bitcoins to participate in the consensus process [287].

Table 4
Security and privacy attacks on Blockchain-based Industry 4.0 applications.

Layer	Attack name	Attack nature	Attacker objectives	Security breaches occurred	Vulnerabilities exploited	Target applications	Countermeasures
Data	Malleability attack	Blockchain application	Duplication of signatures to exacerbate the problem of double spending	Breach of integrity	Modify a few signature bytes	Financial applications (e.g., Bitcoin and other cryptocurrencies)	Segregated witness, Changes to the bitcoin specification, Time commitment methods
	Time Hijacking attack	P2P System	Modification of time stamps	Breach of integrity	Incorrect time stamps broadcasted to nodes	Financial applications (e.g., Bitcoin and other cryptocurrencies)	Hardware oriented systems, Network time protocol, Time constraints
	Quantum attack	P2P System	Utilisation of quantum computing to resolve the Blockchain's cryptography problems	Breach of integrity, Breach of availability	Performed hash collisions	All applications	Quantum post-signature scheme
	Replay attack	P2P System	To keep valid transactions out of the Blockchain	Breach of integrity, Breach of availability	Delay in a P2P network	Online digital platforms, Vehicular-based networks	Add nonce in all transactions Mixing techniques, Digital signatures
	Modification attack	P2P System	To perform modification in transmitted data	Breach of confidentiality, Breach of integrity	Caused the system or network malfunctions	SG, IoT, Medical	Consensus algorithms, Cryptography techniques
	Fault injection attack	P2P System	To counterfeit a Blockchain by inserting fake data or blocks	Breach of Integrity	Making the reputation (or performance) of the system worse	Vehicular-based networks	Digital signatures, Hashing
	Upgraded attack	P2P System	To modify the threshold values to impersonate the miners	Breach of integrity	Intentional maliciousness by the fake miners	Vehicular-based networks	Digital signatures
Network	51% attack	Blockchain application	To gain control of the network by collaborating with more than 50% of the devices	Breach of integrity	Made wrong decisions, Sent bitcoins into accounts targeted	Financial applications (e.g., Bitcoin, Ethereum)	Random selection of miners
	DDoS attack	P2P System	To collectively disrupt or overwhelm network resources	Breach of Availability	Unavailability of legitimate services	All applications	Consensus algorithms
	Eclipse attack	P2P System	To attack a specific node in a P2P network rather than the entire network	Breach of integrity	Hijack and bypass the entire network communication at once	Financial applications (e.g., Bitcoin, Ethereum)	Setting up a private network, Randomly selection of miners,Limiting inbound/outbound connections
	Sybil attack	P2P System	To create fake accounts to exploit a network	Breach of integrity	Personal information of leakage	Bitcoin, Online digital platforms, IoT, Medical, Vehicular-based networks, Cloud	Limit network identity creation, Assign users reputations
	BGP Hijacking attack	P2P System	To determine network data path from source to destination	Breach of integrity	All network traffic directed to the malicious server	Financial applications (e.g., Bitcoin, Ethereum)	Analysing network traffic, BGPsec protocol
	Phishing attack	P2P System	Obtaining a network user's personal information	Breach of confidentiality	Inappropriately use personal data	All applications	Anti-spyware software, Firewalls up-gradation
	Liveness attack	P2P System	To hold the transaction longer than their confirmation time	Breach of availability	A timely transaction verification is impossible	Financial applications (e.g., Bitcoin, Ethereum)	Round trip time (RTT)

(*continued on next page*)

7.2.2. Distributed Denial of Services (DDoS) attack

Despite the fact that blockchain technology is based on a P2P system, it is still susceptible to DDoS attack, which is the most common type of attack on online applications. The types of DDoS attacks range greatly based on the nature of the application, the system architectures, and the behaviour of other network participants. Recently, the most prominent blockchain-based applications, such as Bitcoin and Ethereum, have been regularly targeted by similar attacks, owing to their financial nature [288–290]

However, there is still considerable debate about preventing DDoS attacks on P2P systems through the use of prominent Blockchain technology features such as decentralisation and consensus mechanisms.

Table 4 (*continued*).

Layer	Attack name	Attack nature	Attacker objectives	Security breaches occurred	Vulnerabilities exploited	Target applications	Countermeasures
	Routing attack	P2P System	To modify data packets before sending them to other network nodes	Breach of integrity	The malicious server receives all traffic from the targeted server	All applications	Audit and verification protocols, Round trip time, Cryptography techniques
	Man-in-the-middle (MITM) Attack	P2P System	To circumvent the communication route to access confidential information	Breach of confidentiality, Breach of integrity	The attackers get access to private keys and personal identities	Online digital platforms, Medical, Vehicular-based networks, Financial applications, IoT	Authentication schemes
	Blockchain ingestion attack	Blockchain application	To analyse the publicly available data of Blockchain	Breach of confidentiality, Breach of availability	The attackers get access to personal information in the user's wallet	Financial applications (i.e., Bitcoin, Ethereum)	Use of private and consortium Blockchain networks
Consensus	Double spending attack	Blockchain application	To send the same bitcoins to several users	Breach of Integrity	Copies of digital transactions	Financial applications (e.g., Bitcoin, Digital currencies)	Consensus protocols, Digital signatures
	Stake bleeding attack	Blockchain application	To own new blocks uploaded to the Blockchain	Breach of integrity	Increase the stakes	Incentives-based applications	Perspective transaction validity
	Cryptojacking attack	Blockchain application	To exploit the consensus process of the Blockchain to execute unlawful mining	Breach of integrity, Breach of availability	Consensus protocols are used to consume system resources	Financial applications (i.e., Bitcoin, Ethereum)	A software called "MineGuard" is developed to overcome this issue
Incentive	Selfish mining attack	Blockchain application	To keep the valid block from broadcasting to other nodes	Breach of Integrity, Breach of availability	High resource usage, Claim more awards than other nodes	Financial applications(e.g., Bitcoin, Ethereum)	Define scale and height for miner detection
	Bribery attack	Blockchain application	To create fake mining capacity	Breach of availability	To get additional network power	Incentive-based applications	Consensus mechanism (PoW)
	Refund attack	Blockchain application	To reclaim user payments	Breach of availability	Refunding user payments	Financial applications (Bitcoin and related cryptocurrencies)	A payment request method with enough evidence
	Block withholding attack	Blockchain application	To change the puzzle hash rather than returning it to the mining pool	Breach of Availability, Breach of Integrity	Wastage of computing resources affects mining pool revenue	Incentives-based Applications	Silent time stamps, Zero determinant methods, Contribution of smaller pools, Game-theoretic models and Nash equilibrium
	Balance attack	Blockchain application	To slow down communication between nodes with similar mining power (balance) on the Blockchain network	Breach of Integrity	Some miners can improve their balance by disturbing others' communication	Financial applications (e.g., Bitcoin, Ethereum)	Limiting the number of miners with more network balance
	Integer overflow attack	Blockchain application	To exceed the set limits	Breach of Integrity	Memory overflow and system halting issues	Ethereum-based applications	Code analysis and testing approaches
	Re-Entrancy attack	Blockchain application	To write malicious smart contracts with calling of re-entrance functions	Breach of Integrity	Steal ethers from other people's wallets	Ethereum-based applications	Dynamic fuzzing of smart contract data flows
	Short address attack	Blockchain application	To enter a short address to execute malicious code	Breach of Integrity, Breach of Availability	Smart contract code exploitation	Ethereum-based applications	Validation and synthesis of code

(*continued on next page*)

For instance, the blockchain and Bitcoin systems are entirely decentralised in their construction, management and maintenance [23]. Further, the consensus protocol for new block creation and inclusion to the blockchain guarantees that blockchain transactions can continue to be processed even if many other blockchain nodes go offline [291]. Therefore, to successfully take down a blockchain, an attacker needs to require sufficient computational resources to target a surprisingly high number of the blockchain nodes throughout the whole Blockchain network.

Table 4 (*continued*).

Layer	Attack name	Attack nature	Attacker objectives	Security breaches occurred	Vulnerabilities exploited	Target applications	Countermeasures
	Criminal smart contract attack	Blockchain application	To access personal information by exploiting smart contract vulnerabilities	Breach of integrity, Breach of availability	Stolen personal information of the users	Ethereum-based applications	Use of Intel SGX, HTTPS
Smart contract	Transaction ordering dependency attack	Blockchain application	To disrupt the Blockchain transaction execution order	Breach of integrity, Breach of availability	Disrupted the execution order of the Blockchain transaction	Ethereum-based applications	Utilisation of synchronised and state-locked functions
	Timestamp dependency attack	Blockchain application	To modify the timestamps of smart contracts	Breach of integrity	Complicated the Blockchain systems in a variety of ways	Ethereum-based applications	Oyente tool
	Gas cost attack	Blockchain application	To erroneously configure the gas costs associated with the execution of smart contracts	Breach of integrity	Infected smart contracts, causing DoS	Ethereum-based applications	An adaptive gas cost association method
	Mishandling exceptions attack	Blockchain application	To modify the specific conditions in smart contracts, leading to exceptions mishandling	Breach of integrity, Breach of availability	Caused the error handling issues	Ethereum-based applications	Proper code analysis and testing
	Location cheating attack	P2P System	To misdirect the road side unit (RSU)	Breach of integrity	Usage of the entire system's resources	Vehicular-based networks	Calculate the new location from saved locations each time
	Ballot stuffing attack	P2P System	To make numerous entries instead of one in the system	Breach of integrity	Took over the entire network to perform harmful acts	E-Commerce, E-Voting	Digital signatures
Application	Badmouthing attack	P2P System	To destroy someone 's reputation by giving negative feedback	Breach of confidentiality Breach of integrity	Performed malicious activities in the system by single or group of attackers	E-Commerce	Self-organising maps
	Guess attack	P2P System	To guess the keyword via brute force or matching	Breach of confidentiality, Breach of Integrity	Disclose the system secret	Medical	Cryptographic techniques (Encryption, Hashing)
	Chosen ciphertext attack	P2P System	To get the secret key to decode the ciphertext	Breach of Confidentiality, Breach of Integrity	Obtained the personal data	Medical	Order-Preserving Encryption
	Impersonation attack	P2P System	To create a fake node profile to maximise benefit	Breach of integrity	Control the network by maximising others' benefits	Vehicular-based networks, Crowd Sensing	Verification techniques, Cryptography
	Linking attack	P2P System	To link the stored data using various linking techniques	Breach of confidentiality, Breach of integrity	Extracted some helpful data to violate users' privacy	Financial-based applications (e.g., Bitcoin), Online digital platforms, IoT, Vehicular-based networks,	Encrypt the data with a new key pair each time.
	Collusion attack	P2P System	To combine inputs to disclose node secrets	Breach of Confidentiality, Breach of Integrity	Revealed personal information	Medical, E-Commerce	Pseudo-random approaches
	Private key compromise attack	Blockchain application	To compromise the private key of network users	Breach of availability	Performed unauthorised modifications on behalf of a user	All applications	Choosing non-dictionary seeds, Storing the private key
	Money laundering attack	Blockchain application	To transfer funds illegally	Breach of availability	Illegally transferred funds through foreign banks or legitimate businesses	Blockchain-based cryptocurrency applications	Selection of trusted cryptocurrencies e.g., Bitcoin

7.2.3. Eclipse attack

In an eclipse attack, an attacker targets a specific node rather than capture all the P2P network nodes. Thus, an attacker can prevent the targeted node from receiving new updates from other nodes in the Blockchain network, forcing it to subvert the computing power of the target for malicious purposes. The significant difference between the eclipse and Sybil attacks is that the eclipse attack only targets the specific node. In contrast, the Sybil attack captures and takes control of all network nodes at once. Thus, if an attacker successfully launches the eclipse attack, he can govern his own rules in the network.

Several possible solutions can resist the eclipse attack by applying the following methodologies, such as using the private network, a

random selection of miners, static IP address and limiting the number of incoming/outgoing connections [292,293].

7.2.4. Sybil attack

Sybil attack refers to the most important issue of the P2P network. In this attack, an adversary exploits the network's performance by creating multiple fake identities of the same user. In Blockchain-based applications, this attack is used to separate a target node from the rest of the trustworthy network, which is then utilised to launch other attacks. When a Sybil attack occurs on a blockchain, honest nodes within the network cannot identify fraudulent behaviour and appear to accept transactions from other honest nodes within the network.

There are many solutions available to reduce the risk of Sybil attack in Blockchain-based applications such as E-Health [122], smart vehicles [285], trusted computing [294] and online digital platforms [295]. However, a straightforward technique that can restrict the access of a malicious user is to apply some identity-based mechanisms in the systems. Further, consensus algorithms, such as PoW can also be used in many cryptocurrencies to protect the Sybil attack.

7.2.5. BGP (Border Gateway Protocol) hijacking attack

In a BGP hijacking attack, an adversary takes advantage of a vulnerability found in network operators to intercept and manipulate the network traffic routing through gateways [296]. In a Blockchain system, the BGP attack can control the mining power of miners (or mining pool servers) by splitting them into different groups to cause the propagation delay of blocks in the network. Thus, all traffic from the Blockchain nodes is directed towards the malicious server to gain all the bitcoins.

The common strategy used to tackle the BGP hijacking is the use of BGPsec protocol that prevents the malicious traffic from gaining access to the system [297]. Moreover, monitoring and verifying network traffic after some time can also be a helpful solution.

7.2.6. Phishing attack

Phishing is a type of social engineering activity frequently employed in Blockchain-based applications to get financial benefits, such as miner incentives and bitcoins, by stealing user personal information, login passwords, and banking information such as credit card numbers.

The most successful way to prevent phishing attacks on the system is to install anti-spyware software and periodically upgrade firewall settings. Furthermore, firewall security can prevent unauthorised file access by blocking malicious attempts [298].

7.2.7. Liveness attack

This attack happens in Bitcoin and Ethereum applications when an attacker can hold the broadcasted transactions longer than their confirmation time to cause a delay in the network. As a result, an attacker can build a single chain consisting of targeted transactions that are not transferred to honest miners on the network [299].

The round-trip time (RTT) is used to solve the liveness attacks in Blockchain-based applications to overcome this problem.

7.2.8. Routing attack

An attacker in a routing attack aims to temper the data values inside a block before transmitting them to miner nodes for verification in the network. The adversary in the routing attack routes the data transactions towards the malicious server by changing their destination addresses. This attack is a common attack on those applications that are based on a P2P network. As Blockchain technology follows the idea of a P2P network, an attacker can change the destination address of broadcasted transactions to get the maximum reward from the system [300–302].

In Blockchain-based applications, a standard solution used to detect routing attacks is simply discarding those updates that do not match the other received updates. Moreover, the network parameters, such as round-trip time (RTT) and irregular patterns, can also help users identify and detect routing attacks.

7.2.9. Man-in-the-Middle (MITM) attack

The MITM is one of the common vulnerabilities found in network-based systems such as Blockchain. In a MITM attack, an attacker plays the role of a middleman to bypass the network traffic to obtain users' personal information or secrets. For example, in Blockchain-based cryptocurrency systems, an attacker uses the MITM attack to steal money from victims' wallets by changing the destination address with their fake wallet address.

The most significant way to overcome the MITM attack is to use an advanced authentication mechanism that does not allow the adversary to enter the system.

7.2.10. Blockchain ingestion attack

A Blockchain ingestion attack takes advantage of the vulnerability of public Blockchain networks. Since public Blockchains lack a strong notion of anonymity and provide open data access to the public, analysing the available data in public Blockchains can reveal valuable information to an adversary. Fleder et al. [303] employed graph analysis to highlight the possible exploitation of public Blockchain data by constructing the directed relationships between related wallet user IDs and associated Bitcoin transaction data.

One of the efficient ways to circumvent the Blockchain ingestion attack is to utilise private and consortium blockchain networks in the supported applications.

7.3. Consensus layer

The consensus layer is regarded as the foundation layer of the layered architecture of Blockchain. Further, it contains numerous consensus algorithms essential to the operation of all Blockchain networks. For example, these consensus algorithms allow Blockchain nodes to agree on the validity of newly generated data blocks. The security of the Blockchain is based on the participation of each node in the network. For example, the security of Bitcoin depends on the high hash power of the nodes that participated in the PoW. There are several distinct consensus protocols, for example, PoW, PoS, PBFT and DPoS. The attacks on consensus layers are described below, including the double-spending attack and the stake bleeding attack.

7.3.1. Double spending attack

In Blockchain-based cryptocurrencies, especially in Bitcoin, an attacker with some bitcoins tries to collude with the network by sending a transaction of already consumed bitcoins to others, with the intention of a newly generated transaction. In this case, the attacker can use and spend the double bitcoins to collude with someone in the network.

Therefore, recently proposed cryptocurrencies and different Blockchain systems [14,17,304] are trying to overcome the double-spending attack by using the latest consensus protocols and cryptography mechanisms, such as digital signatures.

7.3.2. Stake bleeding attack

As the name implies, a stake-bleeding attack is a type of attack on the PoS consensus mechanism. An attacker used transaction fees and processed transactions out of context in this attack, enabling attackers to track the newly added block to the Blockchain.

To address this problem in Blockchain networks, Gazi et al. [305] suggested a protocol focused on perspective transactions for validating low-growth chains in order to avoid stake-bleeding attacks.

7.3.3. Cryptojacking attack

Cryptojacking is a type of attack that uses several publicly available web and cloud-based services to get access to the consensus mechanism that runs on Blockchain-based systems. For instance, an attacker can gain unauthorised access to PoW consensus methods for Blockchain-based cryptocurrencies without the approval of miners in order to engage in illicit mining. While in-browser cryptojacking is the most common type of cryptojacking, it utilises websites instead of other tools to mine cryptocurrencies. This attack is referred to as covert mining in cloud-based cryptojacking when malevolent users conducted covert mining activities on available virtual machines and depleted cloud resources.

Tahir et al. [306] developed a solution to circumvent cloud-based cryptojacking attacks in the form of software called "MineGuard" that effectively detects and prevents covert cloud mining operations.

7.4. Incentive layer

The incentive layer in the Blockchain architecture is intended to provide rewards to nodes for participating in the mining process to ensure security and verification of blocks added to the Blockchain. The security of the Blockchain is determined by a few factors such as the number of miner nodes, the consensus protocol and the mining method. Following are the possible attacks on the incentive layer of the Blockchain architecture.

7.4.1. Selfish mining attack

In a selfish mining attack, an adversary plays the role of a miner and acts selfishly by retaining confirmed blocks without broadcasting them to the other miners in the pool network. Thus, selfish miners accumulating validated blocks can demonstrate and claim a higher reward than other honest miners in the mining pool.

Recently, one solution is proposed to tackle the selfish mining attack when a fair mining mechanism is adapted to determine the scale and height of the block. It also allows the network to block the selfish miners in the event of a discrepancy in the blocks [307].

7.4.2. Bribery attack

Bribery attacks attempt to gain temporary control of a majority of miners to increase the mining capacity in the network. As a result, the attackers may initiate a transaction first, forcing the supplier to wait for confirmation. Attackers bribed miners in various ways, including direct payment, fraudulent mining pools, and internal payouts via tokens.

An efficient strategy to alleviate this problem is using the PoW consensus mechanism as attackers have to pay considerable costs to discredit the miner [308].

7.4.3. Refund attack

In a refund attack, an attacker attempts to recover from honest users the transactions (or payments) made to illegitimate users and then fairly denies them participation in the refund transaction phase. In this attack, the intruder impersonates unauthorised traders to exploit the entire network by rejecting all sent transactions.

McCorry et al. [309] suggest an effective solution to this problem in which users are asked to include payment request messages along with a few verifiable pieces of evidence such as a delivery address, which reduces an incentive of the attacker for profitable attacks.

7.4.4. Block withholding attack

A block withholding attack is a form of resource squandering attack in which miners violate the mining rules by disguising the hash of the puzzle rather than returning it to the mining pool for a greater self-reward. However, block withholding attacks waste a significant portion of computing resources and reduce the pool's overall mining income, as only malicious miners profit from this attack and collect additional rewards.

A wide range of solutions to this problem have been suggested, including silent time stamps [310], zero determinant methods [311], the contribution of smaller pools [312] and a game model based on the consensus protocol and Nash equilibrium [313].

7.4.5. Balance attack

As the name suggests, a balance attack is an attack on some consensus mechanism to increase the balance by using unfair means. Thus, a balance Attack is a particular type of attack on a PoW-based consensus protocol. For example, an attacker with low balance or power attempts to delay communication between those subgroups of miners who have the same hashing power (or balance) [314]. This type of attack is most common in financial-based applications such as Bitcoin and Ethereum that have coins and ethers to spend, respectively.

A balance attack can be mitigated by prohibiting miners from mining other blocks with more balance in the network.

7.5. Smart contract layer

The contract layer comprises three major components: the smart contract itself, scripting code and an algorithm or logic. These three elements represent the key logic and conditions in the executed contract. These logics are generally written in Solidity, a programming language. The following summarises the various types of attacks that could be launched against the smart contract layer.

7.5.1. Integer overflow attack

Integer overflow is a common security vulnerability in many applications, mainly based on ethereum smart contracts, which occurred primarily due to a lack of code validations. Smart contracts are a series of programme codes in which unique numbers determine an integer's upper and lower limits. An integer overflow problem occurs when the value executed reaches its prescribed limits, causing the machine to halt specific errors.

A few solutions have been suggested to mitigate the risk of integer overflow attack in smart contracts; however, most of them focus on careful analysis, rewriting, verification of codes writing [304,315].

7.5.2. Re-entrancy attack

Re-entrancy attacks are usually triggered by those functions that are not meant to be re-entered by developers. In this attack, attackers can create malicious contracts that call these functions reentrantly with the intent of stealing Ether from an honest user's account, causing the user to lose his credentials and all Ethers. An example of this type of attack is the DAO attack on smart contracts, which occurred in 2016 and resulted in the loss of 60 million Ether.

Many solutions have been suggested to overcome the re-entrancy attack on smart contracts. For example, one approach called Sereum [316] is proposed to solve the re-entrance attack, allowing for dynamic taint tracking of smart contract data flows. In addition, ReGuard [317] is an automatic detection system that conducts fuzzing tests in order to fix the issue of re-entry attacks.

7.5.3. Short address attack

A short address attack is a bug in developer-side code that causes users to enter a short address instead of the full address. For example, if a user uses the transfer method to withdraw coins and is needed to enter a short address. In addition, if the user's size entered by the address is not checked due to a lack of validation measures, a short address attack may occur.

A solution to this problem is suggested by a technique called SmartScopy [318]—automatically synthesising adversarial contracts to achieve smart contract stability.

7.5.4. Criminal smart contract attack

A criminal smart contract attack occurs due to the misuse of smart contracts, which results in data leaking, cryptographic key theft, and a variety of other real-world crimes. For example, Jules et al. [319] presents an example of PwdTheft: a method in which passwords can be stolen without relying on a third party trusted authority by utilising a criminal smart contract attack. In PwdTheft process, contractors and perpetrators use fair exchange smart contracts in Blockchain, which do not have access to the network in the entire process.

A practical solution to overcome this attack is the use of trusted hardware technologies, such as Intel SGX (Software Guard eXtension), in conjunction with HTTPS (Hypertext Transfer Protocol Secure) to verify the validity of credentials [320].

7.5.5. Transaction ordering dependency attack

In Ethereum smart contracts, a transaction ordering attack is often referred to as a race condition attack. In Blockchain, when a block contains many transactions and the blockchain state changes multiple times inside an epoch, a transaction ordering dependency attack is triggered. For instance, when a new block is generated that has two transactions such as T_1 and T_2 that invoke the same smart contract, the execution order of T_1 and T_2 affects the ultimate state and thus causes the reason for transaction ordering to be disturbed [321].

Synchronised and state locking facility functions could be the best solution for overcoming this attack in Ethereum-based applications.

7.5.6. Timestamp dependency attack

Smart contracts that need the block timestamp to perform important operations (such as transmitting Ether) or to generate random numbers are vulnerable to the timestamp dependency attack. While a miner has the flexibility to adjust the timestamp of a block within a short period span smaller than a few seconds in a distributed system such as Blockchain. Therefore, if a smart contract transfers Ether depending on the timestamp, an attacker can manipulate block timestamps to execute the security vulnerabilities.

Oyente [322] is an excellent tool for detecting timestamp dependency attacks on Ethereum smart contracts.

7.5.7. Gas cost attack

When a smart contract executes in the Ethereum Virtual Machine (EVM), it uses gas (also known as computational resources) to ensure that the contract eventually terminates. Unfortunately, gas cost misconfiguration allows an attacker to mount a denial-of-service attack on the contracts, terminating the smart contracts.

To prevent the gas cost attack on smart contracts, Chen et al. [323] presented an adaptive gas cost method that can change DoS gas prices. Although Ethereum has made the necessary adjustments to prevent exploitation, the flaws are still present and exploitable.

7.5.8. Mishandling exceptions attack

An attacker uses a mishandled exception attack to exploit vulnerabilities in smart contract implementation. For instance, when multiple smart contracts are invoked simultaneously, in some circumstances, the smart contracts that were supposed to supply output to other smart contracts cease to function, thereby aborting the specific condition or entire system.

This problem can be overcome by ensuring that the function call was executed successfully by explicitly checking the return value. While smart contracts need to have exception checking built-in, they may be insecure if not implemented appropriately.

7.6. Application layer

The application layer is responsible for executing applications used by end-users to communicate with the Blockchain network. Application layer security refers to the protection of this layer and the users who communicate with it. Since this layer is a combination of different Blockchain components and third-party technologies to develop an application, it is vulnerable to a wide range of attacks. The application layer attacks and their accompanying mitigation strategies are explored in detail below.

7.6.1. Location cheating attack

A location cheating attack is a prevalent type of attack against the majority of Blockchain-based vehicular network applications. Both passengers and drivers engage in location cheating activities by broadcasting fake locations to respective authorities known as a roadside unit (RSU). In the case of passengers, an adversary initiates a location cheating attack by transmitting a fictitious and long-distance location to a RSU to pick up the passengers at some point. On the other hand, the driver may be complicit in the location cheating attack by impersonating a RSU to mislead passengers.

To rectify the issue of location cheating in vehicular networks, Li et al. [203] proposed a robust and secure Blockchain-based method to calculate the authenticity of both drivers and passengers.

7.6.2. Ballot stuffing attack

Ballot stuffing (or ballot-box stuffing) is a specific type of attack against a Blockchain-based electronic voting system. An adversary attempts to carry out this unauthorised action by persuading network miners to vote in multiple illegal decisions (or ballots). This fraudulent behaviour exploits the integrity of a system to increase the number of votes for one miner, thus reducing others' credibility.

One technique to address this issue is to incorporate digital signatures into the voting process to verify the validity of voters and candidates. Additionally, a range of e-voting programmes built on the Blockchain is designed to identify ballot-stuffing attempts in the systems [260,324,325].

7.6.3. Badmouthing attack

A badmouthing attack is a common type of attack that occurs in Blockchain-based systems. It is based on the concept of rating or feedback, in which an attacker attempts to respond negatively to legal miners in order to lower their system reputation. In this attack, the main objectives of an attacker are twofold: (i) to degrade the reputation of a particular miner in the system by making the scale system negative (ii) to increase the rating of a favourable miner.

To address this issue, a method called self-organising maps [326] is utilised to detect and prevent malicious user behaviour.

7.6.4. Guess attack

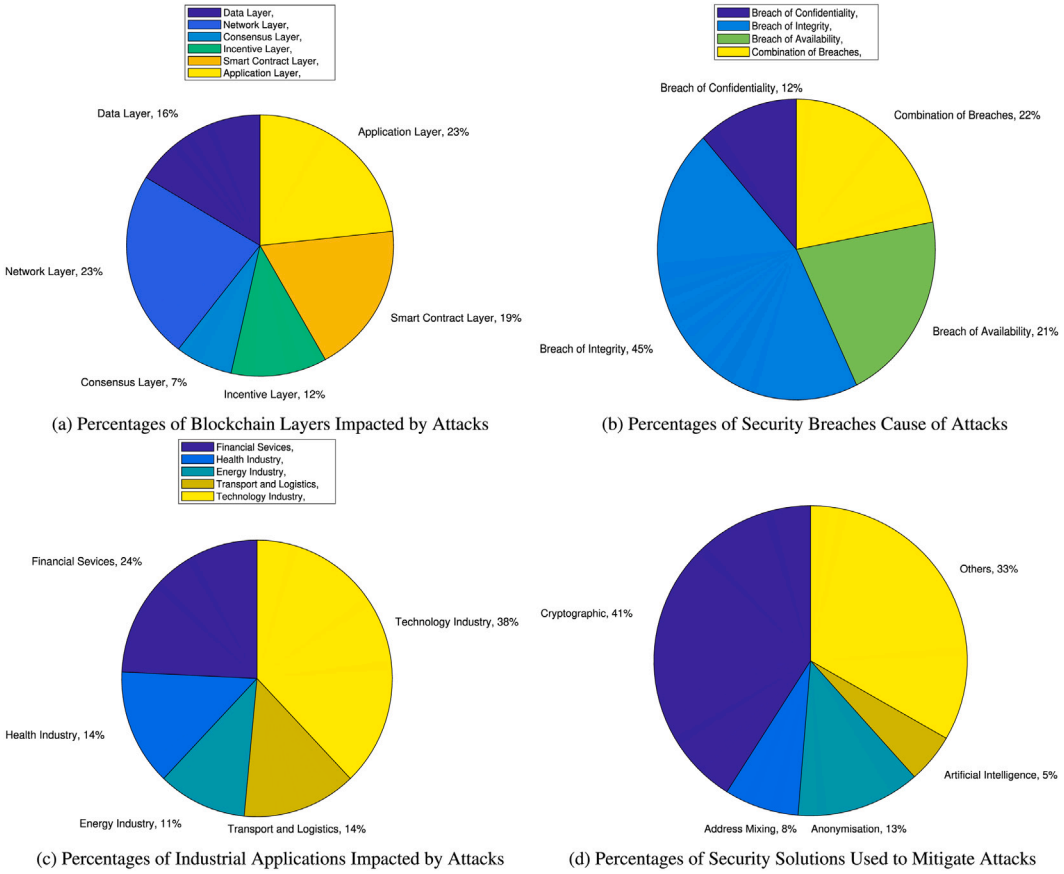
A guess attack in Blockchain-based systems aims to find personal information about the targeted users, such as their private keys, by brute force or other matching approaches. Generally, a guess attack occurs during the search process, when an attacker randomly matches input terms with stored data.

To address this issue, [215] presented a Blockchain-based E-health scheme that uses cryptography primitives such as encryption and hashing to protect the personal information of both patients and doctors.

7.6.5. Chosen ciphertext attack

In Blockchain-based systems, the chosen ciphertext attack aims to get secrets of users, such as private keys from their wallets that are used to generate transactions, by analysing the various chosen ciphertexts obtained over the communication channel [327].

This issue can be resolved by employing advanced cryptography techniques, such as order-preserving encryption across several systems to transmit the secret key securely [218].



(a) Percentages of Blockchain Layers Impacted by Attacks

(b) Percentages of Security Breaches Cause of Attacks

(c) Percentages of Industrial Applications Impacted by Attacks

(d) Percentages of Security Solutions Used to Mitigate Attacks

Fig. 15. A graphical representations of performed analysis of security and privacy attacks in terms of layers, security breaches, applications and security solutions.

7.6.6. Private key compromise attack

A private key is an important security credential in Blockchain-based applications since it is generated and managed by users rather than third-party entities. For instance, in the Bitcoin application, digital wallets contain a private key used exclusively by the wallet owner and must be kept secret from other network users. This is also referred to as a wallet theft attack. In Blockchain, Hartwig et al. [328] discovered a vulnerability in ECDSA in which the signature process lacks sufficient randomisation, allowing an attacker to retrieve the private key of a user.

This issue can be mitigated by emphasising the importance of users selecting non-dictionary seeds and securely storing their private keys rather than making them freely accessible. Since Blockchain has no centralised trusted third party, if the private key is taken, it is nearly impossible to follow criminal activities and identify which blockchain information has been updated.

7.6.7. Money laundering attack

With the emergence of Bitcoin and numerous other associated cryptocurrencies, the attackers have begun engaging in fraudulent operations. Money laundering is a sort of fraudulent behaviour in which the origins of illegally obtained funds are concealed, generally through transfers engaging foreign banks or legitimate enterprises. For example, Cody and Amir [329] developed a cryptocurrency application called Dark Wallet that conceals all Bitcoin transactions in an entirely private and undetectable manner. However, in contrast to most cryptocurrencies, the risk of Bitcoin being used for money laundering is among the lowest [330].

7.6.8. Impersonation attack

An attacker creates a fake profile of a valid network user in an impersonation attack and then uses social engineering techniques such as email and links to access the targeted system. For instance, in Blockchain systems, malicious attackers employ various common approaches to access the systems of miners involved in the consensus process to obtain incentives to reward their malicious peers.

To minimise the possibility of impersonation attacks on Blockchain systems, such as transportation and crowdsensing applications, [35,247,261] proposed a security mechanism that protects miners from impersonation attacks and validates only those miners with the required attributes to log in to the system.

7.6.9. Linking attack

In a linking attack, the goal of an adversary is to create the link between the external data and stored data by using some de-anonymisation techniques to expose the personal information of users. The linking attack is a severe type of attack that is applied over many Blockchain systems such as Bitcoin [204], online digital platform [295], IoT and vehicular networks [10], in order to extract the secret data from stored transactions.

This problem has been widely discussed, and several approaches have been proposed to resolve a link attack, but the most accurate approach is to create a new key pair each time encrypt the data.

7.6.10. Collusion attack

A collusion attack on a Blockchain network aims to gather user secrets, such as personal information, through packet sniffing tools and merging various copies of transactional data to obtain some collective benefits. For example, on the Blockchain network, numerous miners attempt to collude with the network in order to maximise their reward for mining.

To address collusion in Blockchain-based E-Health and E-Commerce applications, pseudo-random approaches are utilised [216,260]. In such approaches, the random seed is exchanged between two users to withstand N-1 additional fictitious users.

7.7. Analysis and discussion on attacks

We undertake a thorough analysis of the security and privacy attacks discussed in this survey paper. We examined the attacks against the numerous criteria in the table, such as layers, security breaches, impacted applications, and security solutions, for analysis. Fig. 15 illustrates multiple graphical representations of security and privacy attacks in percentages based on our selected criteria.

Fig. 15a shows the percentage of each Blockchain layer affected by security and privacy attacks included in the paper. The layers of the Blockchain are as follows: network, data, consensus, incentive, smart contract, and application. By and large, it is evident that the network and application layers of Blockchain architecture are the target of a significant amount of attacks, accounting for 26% of all attacks. It is also worth mentioning that the data and smart contract layers are the second and third most affected layers, with only a 3% difference between them. These layers are the targets of 16% and 19% of all attacks, respectively. Further, attacks have a 12% influence on the incentive layer, but only a small number of attacks, around 7%, are targeted at the consensus layer.

The percentage of various security breaches that result in the security and privacy attacks mentioned in our paper is depicted in Fig. 15b. We focused on three types of security breaches in our work: breaches of confidentiality, integrity, and availability. Additionally, attacks may arise as a result of a combination of the aforementioned security breaches. By and large, it is evident that a considerable number of attacks on various Blockchain and industrial applications are the consequence of a breach of integrity, which is referred to in this study as a potential security breach. Additionally, it is worth mentioning that roughly half of the integrity breaches are the consequence of a combination of multiple security vulnerabilities. Combinations of security breaches may include a breach of confidentiality, breach of integrity and breach of availability. On the other hand, there is only a 9% difference between the last two breaches (confidentiality and integrity).

Fig. 15c illustrates the percentage of various industrial applications susceptible to security and privacy attacks explored in our work. Financial services, health industry, energy industry, transport and logistics and technology industry are among the industrial applications covered by our research. At first look, it appears that the technology industry-related applications such as IoT, big data and cloud computing, crowdsensing, and E-Commerce are the most affected applications by the security attacks. For instance, 38% of technology-related industry applications are impacted in our analysis results, more than a third of the total numbers. However, the financial industry is the second most impacted industry, accounting for 24% of all attacks. Additionally, the health industry and transportation and logistics have been vulnerable to these attacks, accounting for 14% of all attacks. Finally, the energy industry is also impacted by attacks, accounting for 11% of the total attacks.

The percentages of various security solutions utilised to minimise security and privacy threats on Blockchain-based Industry 4.0 applications are represented in Fig. 15d. Cryptographic-based approaches, address mixing, anonymisation, artificial intelligence and few other solutions utilised in available applications. By and large, the most successful method of securing industrial applications against attacks is to employ various cryptographic approaches such as encryption, hashing, and digital signatures, which account for 41% of all other security solutions. As a result, roughly a third portion of security solutions combine different security solutions such as bilinear maps, three weight models, time ranks, and consensus mechanisms to mitigate the risk of attacks on Blockchain-based applications. Anonymisation techniques, which account for 13% of the total, also contribute significantly to the security of those applications. Address mixing and artificial intelligence-based solutions also address security concerns, accounting for 8% and 5% of the total, respectively.

8. Open issues

Although potential Blockchain features could greatly benefit industry users, various issues must be addressed before developing more industrial applications. This section highlights open issues regarding incorporating Blockchain technology into industrial applications, restricting its applicability to broader industry adoption. Fig. 16 summarises the open issues related to designing and integrating Industry 4.0 applications with Blockchain technology.

8.1. Interoperability and governance

Industry 4.0 encompasses a wide range of applications and businesses that can communicate and share essential data or assets. Interoperability is described as a network infrastructure or capacity that allows industry partners to exchange information over the network. Similarly, Blockchain interoperability allows different Blockchain systems to communicate by exchanging messages and trustworthy values [331]. The challenges that arise during the interoperability of Blockchain systems include data security and industry guidelines for regulating and controlling applications [136]. Thus, it is necessary to build a mechanism that can ensure interoperability between Blockchain platforms and define rules and laws that align with industry principles and guidelines [147].

8.2. Legal and compliance issues

Using a different standard, agreement rules, and some uncertainties about government regulatory agencies are significant obstacles to implementing Blockchain technology in larger industrial domains. For example, industries require Blockchain solutions to guarantee their internal processes and commodities comply with legal and regulatory standards [332]. In addition, contracts between industry users and government regulations relating to negotiation, execution, administration, and Blockchain management are required by commercial law. If a contract is miscoded and is not performed as intended, the parties are liable for the miscoded contract [333].

Another crucial problem between the parties' legal and compliance arrangements is to adhere to substantive law, effective governance, jurisdiction and settlement, and ensuring the privacy of both consumers and the product. The sharing of production data across platforms can also cause issues for manufacturers and their products. Thus, when creating industrial platforms, users' privacy and data must be protected [334]. Governments should consider a specific government obligation in the public interest while making new laws, rules, recommendations, and applying laws in industries. Using a private Blockchain can help stop illegal activities like money laundering and regulatory evasion. Additionally, fake miners should be prevented from creating new blocks.

8.3. Scalability

The decentralisation of blockchain technology has emerged as a promising alternative in reforming existing centralised structures. It allows P2P network nodes to mine blocks in a dynamic environment and frequently updates transactions to other network nodes. Bitcoin and Ethereum Blockchain systems can handle users and transactions, but scalability issues prevent widespread adoption and implementation. For example, VISA [335] can process 2000 transactions per second, while Bitcoin [336] can only process seven transactions per second. Moreover, as Blockchain technology is adopted and applied in Industry 4.0, the size of a system expands, and thousands of nodes are required to join the network for block creation and mining. Thus, the scalability of Blockchain is in question, posing a severe challenge to network security systems and applications [337,338].

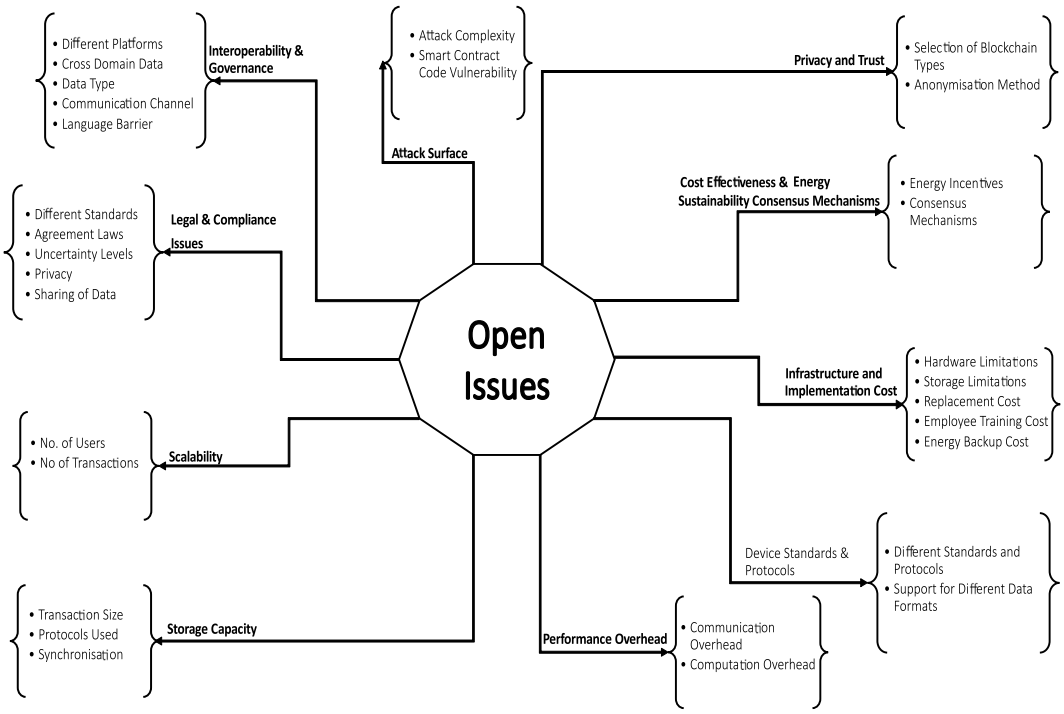


Fig. 16. Open issues of Blockchain adoption in Industry 4.0-based applications.

8.4. Storage capacity

Many Blockchain-based applications have questioned the storage constraint for keeping data on a secure distributed ledger. As in Bitcoin, the chain increases by one megabyte every 10 min and each node in the network has a copy of the full chain. While a full node can hold all blocks, the total storage requirements grow exponentially with transaction size, increasing system capacity. Because manufacturing data is extensive, integrating Blockchain technology into many industrial processes is problematic [339]. The underlying Blockchain protocols also cause significant system traffic congestion, increasing the system's need for overall Blockchain storage space [340]. Oversized chains also cause synchronisation overload for new users. In the industrial IoT setting, the problem is exacerbated by the expanding number of sensors and data produced [341]. As of now, resource-restricted IoT solutions are too immature to appreciate more industrial applications, even though Ethereum-inspired frameworks have recently been established [342].

8.5. Performance overhead

Like most industrial applications, E-Health, SG and IoT are simple and require little computing, storage, and energy capabilities. However, these applications demand significant computation to mine blocks and perform intensive cryptographic operations as hashing, encryption/decryption, and digital signatures [343]. Many solutions have been proposed that identify mining nodes and simple nodes as complete nodes and simple nodes in Blockchain-based IoT applications, respectively [344]. Another performance concern in industrial applications is communication overhead, as each mining node is responsible for mining, updating Blockchain, and communicating updated blocks to other peer nodes over the network [345]. This issue adds network overhead, affecting network capacity and performance. Thus, computation and communication overheads in Blockchain-based Industry 4.0 applications create barriers to their adoption at a wider industry level [346].

8.6. Device standards and protocols

Various heterogeneous IoT devices are used in industrial setups to monitor and regulate the environment to take future measures continuously. However, device standards and protocols have become another challenge for IoT and Industry 4.0. Because they all capture data in different forms and use separate protocols, integrating them into industrial setups is costly and difficult [347]. Companies like Bosch and the Eclipse Foundation are working to standardise data formats and communication protocols like MQTT [348]. The primary goal is to help smart devices interact effortlessly by providing popular data formats. However, more data formats mean more complexity in establishing a single data model [349].

8.7. Cost-effectiveness and energy sustainable consensus mechanisms

Consensus algorithms like PoW and PoS are considered energy-intensive since they utilise more energy and computational resources [350]. DPoS [351] and Proof of Trust (PoT) [352] have recently been proposed as energy-efficient consensus protocols to conduct this procedure cost-effectively as the size of Blockchain grows. Since enormous volumes of data surround energy and resource-constrained industrial IoT devices, more efficient consensus algorithms are required [353].

8.8. Infrastructure/implementation cost

Blockchain technology generally requires specialised infrastructure, such as additional storage and computationally intensive hardware resources to store the Blockchain. Blockchain storage is based on Distributed Ledger Technology (DLT) and acts as a shared database of information about transactions. Between April 2019 and March 2021, Bitcoin is estimated to have grown by 340 GB; however, this growth varies with the rate of new block discovery [354]. Because of this, when using Blockchain technology in industrial settings, numerous cost scenarios must be considered. These costs can include: (i) implementing and establishing the Blockchain setup, (ii) replacing the current industrial infrastructure, (iii) training staff on Blockchain technology and (iv) energy maintaining resources as a backup [2].

8.9. Privacy and trust

One of the benefits of using Blockchain technology in industrial applications is to achieve anonymity of users' identities and their transactions, using pseudo-anonymity methods [23]. However, using a public Blockchain type and pseudo-anonymous approaches in Blockchain applications may link users' identities such as public keys with transactions that can increase the risk of personal data leakage [355]. Therefore, complete and anonymous pseudo-anonymity approaches are required to achieve privacy and trust amongst Blockchain users [356].

8.10. Attack surface

As more industrial applications adopt Blockchain technology, several attack surfaces have been targeted. These attacks exploit numerous application vulnerabilities to get access to the resources and modify user data [357]. For example, with Bitcoin, the double-spending attack can combine with other attacks, such as a Sybil attack, to gain access to user wallets, coins, and private keys [358]. In addition, the vulnerabilities identified in the smart contract code and, in some cases, open source applications have made Blockchain systems more vulnerable to other malicious users [359]. Thus, carefully designed Blockchain applications with appropriate principles and secure cryptography procedures across layers can reduce the risk of attacks [82].

9. Conclusion and future work

Blockchain integration with different Industry 4.0-based applications such as IoT, banking, SG, E-Health, transport and logistics, and the cloud is rapidly expanding, and it has positively impacted human life. Considering the design of secure Blockchain-based Industry 4.0 applications and limitations identified in the existing survey studies, we present a detailed study that achieved significant contributions regarding security and privacy for Blockchain-based Industry 4.0 applications. First, we present an application-oriented overview of Blockchain technology, including its features, evolution, layered architecture, types, storage structures, and transaction model, which serve as a map and motivate the design of secure Blockchain applications. Second, we define the application, security, and privacy requirements necessary to satisfy the need for secure Blockchain-based Industry 4.0 applications. Third, we discuss how various security measures meet the various security and privacy requirements of Blockchain-based Industry 4.0 applications. Furthermore, we extend our survey to include various security and privacy attacks on Blockchain applications, classifying them according to their attack type, the attacker's aims, attack nature, security breaches, exploited vulnerabilities, and targeted applications. Then, we examine various security and privacy enhancement techniques that have been employed to meet security and privacy requirements in Industry 4.0 applications built on the Blockchain. Finally, we discuss open design issues that provide fuel to researchers and developers to design secure Industry 4.0. applications.

In the concluding section of the paper, we give numerous future recommendations for handling different design and security requirements and some open issues, guiding both researchers and developers in the design of secure, scalable, efficient, and flexible Blockchain-based applications. Currently, most Blockchain-based schemes do not meet critical requirements such as scalability, interoperability, usability, adaptability, modularity, and transparency. Scalability is the most critical requirement for developing Blockchain applications, particularly in the industrial area, where systems perform poorly as the number of users and their real-time transactions increases. Furthermore, the scalability of various systems (like [60] and Hyperledger [61]) is impacted by mining and transaction validation constraints. Thus, researchers and developers must address scalability issues when developing Blockchain applications. Another design requirement issue that has been identified in Blockchain applications is the divergence between the various system's internal and external components, often known as an interoperability issue. Additionally, interoperability of system components enables the administrator to take immediate security measures in response to hostile activity occurring within the system. As a result, the interoperability issue must be addressed throughout the development of secure Blockchain applications.

Blockchain technology is composed of numerous supporting and underlying characteristics that facilitate the execution of numerous tasks. However, not all ordinary users are familiar with the technical details and operation of Blockchain technology. As a result, they are unable to utilise Blockchain solutions in a variety of organisations and industries. While developing Industry 4.0 applications and business domains, the blockchain model must adhere to usability and adaptability criteria. Moving on to the modularity design requirement, developers must construct application code that is more applicable across Blockchain applications and supports a wide range of services that efficiently deliver network resources. As blockchain applications acquire community acceptance, researchers and developers must establish a safe environment where users may efficiently exchange resources and interact transparently.

CRediT authorship contribution statement

Khizar Hameed: Problem investigation, Conceptualization, Methodology, Writing – original draft, Writing – review & editing. **Mutaz Barika:** Methodology, Conceptualization, Writing – review & editing. **Saurabh Garg:** Supervision, Methodology, Writing – review & editing. **Muhammad Bilal Amin:** Supervision, Methodology, Writing - review & editing. **Byeong Kang:** Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] B. Oberer, A. Erkollar, Leadership 4.0: Digital leaders in the age of industry 4.0, Int. J. Organ. Leadersh. (2018).
[2] J. Lee, M. Azamfar, J. Singh, A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems, Manuf. Lett. 20 (2019) 34–39.
[3] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, M. Alazab, Blockchain for industry 4.0: A comprehensive review, IEEE Access 8 (2020) 79764–79800.
[4] N. Mohamed, J. Al-Jaroodi, Applying blockchain in industry 4.0 applications, in: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2019, pp. 0852–0858.
[5] M. Swan, Blockchain: Blueprint for a New Economy, " O'Reilly Media, Inc.", 2015.
[6] S. Wang, J. Wan, D. Li, C. Zhang, Implementing smart factory of industrie 4.0: An outlook, Int. J. Distrib. Sens. Netw. 12 (1) (2016) 3159805, http://dx.doi.org/10.1155/2016/3159805.
[7] Y. Guo, C. Liang, Blockchain application and outlook in the banking industry, Financ. Innov. 2 (1) (2016) 24.
[8] K. Fanning, D.P. Centers, Blockchain and its coming impact on financial services, J. Corp. Account. Finance 27 (5) (2016) 53–57.
[9] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, C. Weinhardt, A blockchain-based smart grid: towards sustainable local energy markets, Comput. Sci. Res. Dev. 33 (1–2) (2018) 207–214.
[10] A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak, Blockchain: A distributed solution to automotive security and privacy, IEEE Commun. Mag. 55 (12) (2017) 119–125.
[11] M. Mettler, Blockchain technology in healthcare: The revolution starts here, in: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, 2016, pp. 1–3.
[12] Y. Cai, D. Zhu, Fraud detections for online businesses: a perspective from blockchain technology, Financ. Innov. 2 (1) (2016) 20.
[13] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, Blockchain technology innovations, in: 2017 IEEE Technology & Engineering Management Conference (TEMSCON), IEEE, 2017, pp. 137–141.

[14] L. Zhong, Q. Wu, J. Xie, J. Li, B. Qin, A secure versatile light payment system based on blockchain, Future Gener. Comput. Syst. 93 (2019) 327–337.

[15] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom, FHIRChain: applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.

[16] D. Vos, L. Overweel, W. Raateland, J. Vos, M. Bijman, M. Pigmans, Z. Erkin, DEFenD: A secure and privacy-preserving decentralized system for freight declaration, 2018, arXiv preprint arXiv:1803.09257.

[17] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Trans. Dependable Secure Comput. 15 (5) (2016) 840–852.

[18] D. Yang, J. Gavigan, Z. Wilcox-O'Hearn, Survey of Confidentiality and Privacy Preserving Technologies for Blockchains, R3, Zcash Company, Res. Rep, 2016.

[19] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. (2017).

[20] Q. Feng, D. He, S. Zeadally, M.K. Khan, N. Kumar, A survey on privacy protection in blockchain system, J. Netw. Comput. Appl. (2018).

[21] M.C.K. Khalilov, A. Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2543–2585.

[22] M. Conti, E.S. Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3416–3452.

[23] R. Zhang, R. Xue, L. Liu, Security and privacy on blockchain, 2019, arXiv preprint arXiv:1903.07602.

[24] A.P. Joshi, M. Han, Y. Wang, A survey on security and privacy issues of blockchain technology, Math. Found. Comput. 1 (2) (2018) 121–147.

[25] M.U. Hassan, M.H. Rehmani, J. Chen, Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions, Future Gener. Comput. Syst. 97 (2019) 512–529.

[26] S.V. Akram, P.K. Malik, R. Singh, G. Anita, S. Tanwar, Adoption of blockchain technology in various realms: Opportunities and challenges, Secur. Priv. (2020) e109.

[27] F. Casino, T.K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: current status, classification and open issues, Telemat. Inform. 36 (2019) 55–81.

[28] T.M. Fernandez-Carames, P. Fraga-Lamas, A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories, IEEE Access 7 (2019) 45201–45218.

[29] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey, IEEE Commun. Surv. Tutor. 21 (1) (2018) 858–880.

[30] D. Dasgupta, J.M. Shrein, K.D. Gupta, A survey of blockchain from security perspective, J. Bank. Financ. Technol. 3 (1) (2019) 1–17.

[31] B.K. Mohanta, D. Jena, S.S. Panda, S. Sobhanayak, Blockchain technology: A survey on applications and security privacy challenges, Internet Things 8 (2019) 100107.

[32] D.D.F. Maesa, P. Mori, Blockchain 3.0 applications survey, J. Parallel Distrib. Comput. 138 (2020) 99–114.

[33] S. Perera, S. Nanayakkara, M. Rodrigo, S. Senaratne, R. Weinand, Blockchain technology: Is it hype or real in the construction industry? J. Ind. Inf. Integr. 17 (2020) 100125.

[34] D. Wang, J. Zhao, Y. Wang, A survey on privacy protection of blockchain: the technology and application, IEEE Access (2020).

[35] C. Lin, D. He, X. Huang, K.-K.R. Choo, A.V. Vasilakos, BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, J. Netw. Comput. Appl. 116 (2018) 42–52.

[36] W. Viriyasitavat, L. Da Xu, Z. Bi, A. Sapsomboon, Blockchain-based business process management (BPM) framework for service composition in industry 4.0, J. Intell. Manuf. (2018) 1–12.

[37] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Bus. Inf. Syst. Eng. 59 (3) (2017) 183–187.

[38] S. Underwood, Blockchain beyond bitcoin, 2016.

[39] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, et al., Blockchain technology: Beyond bitcoin, Appl. Innov. 2 (6–10) (2016) 71.

[40] Bitcoinwiki. Proof of work, 2020, Available: https://en.bitcoin.it/wiki/Proof_of_work. Accessed: 2020-08-19.

[41] Bitcoinwiki. Proof of stake, 2020, Available: https://en.bitcoin.it/wiki/Proof_of_Stake. Accessed: 2020-08-19.

[42] M. Castro, B. Liskov, et al., Practical Byzantine fault tolerance, in: OSDI, Vol. 99, 1999, pp. 173–186.

[43] D. Larimer, Delegated proof-of-stake (dpos), in: Bitshare Whitepaper, 2014.

[44] D. Puthal, S.P. Mohanty, Proof of authentication: IoT-friendly blockchains, IEEE Potentials 38 (1) (2018) 26–29.

[45] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, W. Shi, On security analysis of proof-of-elapsed-time (poet), in: International Symposium on Stabilization, Safety, and Security of Distributed Systems, Springer, 2017, pp. 282–297.

[46] Bitcoinwiki. Proof of space, 2020, Available: https://en.wikipedia.org/wiki/Proof_of_space. Accessed: 2020-08-19.

[47] Proof of importance, 2020, Available: https://golden.com/wiki/Proof-of-importance_(PoI). Accessed: 2020-08-19.

[48] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, 2017, pp. 557–564.

[49] B.-K. Zheng, L.-H. Zhu, M. Shen, F. Gao, C. Zhang, Y.-D. Li, J. Yang, Scalable and privacy-preserving data sharing based on blockchain, J. Comput. Sci. Tech. 33 (3) (2018) 557–567, http://dx.doi.org/10.1007/s11390-018-1840-5.

[50] M. Muzammal, Q. Qu, B. Nasrulin, Renovating blockchain with distributed databases: An open source system, Future Gener. Comput. Syst. 90 (2019) 105–117.

[51] M. Conoscenti, A. Vetro, J.C. De Martin, Blockchain for the Internet of Things: A systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), IEEE, 2016, pp. 1–6.

[52] L. Lotti, Contemporary art, capitalization and the blockchain: On the autonomy and automation of art's value, Finance Soc. 2 (2) (2016) 96–110.

[53] Z. Wang, J. Lin, Q. Cai, Q. Wang, D. Zha, J. Jing, Blockchain-based certificate transparency and revocation transparency, IEEE Trans. Dependable Secure Comput. (2020).

[54] S. Nakamoto, et al., Bitcoin: A peer-to-peer electronic cash system, 2008.

[55] Bitcoin cash, 2017, https://bitcoincash.org/.

[56] Litecoin - open source p2p digital currency, 2018, "https://litecoin.org/". (Online; accessed on 12-Dec-2018).

[57] Ripple, 2012, https://ripple.com/.

[58] M. Xu, X. Chen, G. Kou, A systematic review of blockchain, Financ. Innov. 5 (1) (2019) 1–14.

[59] R. Colomo-Palacios, M. Sánchez-Gordón, D. Arias-Aranda, A critical review on blockchain assessment initiatives: A technology evolution viewpoint, J. Softw.: Evol. Process 32 (11) (2020) e2272.

[60] G. Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, Ethereum Proj. Yellow Pap. 151 (2014) (2014) 1–32.

[61] Hyperledger, 2016, "https://www.hyperledger.org//".

[62] Codius, 2013, "https://www.codius.org//".

[63] M. Swan, Anticipating the economic benefits of blockchain, Technol. Innov. Manage. Rev. 7 (10) (2017) 6–13.

[64] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P.K. Singh, W.-C. Hong, A survey on decentralized consensus mechanisms for cyber physical systems, IEEE Access 8 (2020) 54371–54401.

[65] Y. Lu, Industry 4.0: A survey on technologies, applications and open research issues, J. Ind. Inf. Integr. 6 (2017) 1–10.

[66] S. Omohundro, Cryptocurrencies, smart contracts, and artificial intelligence, AI Matters 1 (2) (2014) 19–21.

[67] A. Berentsen, F. Schär, The fallacy of a cashless society, in: C. Beer, E. Gnan, U.W. Birchler (Eds.), Cash on Trial, SUERF Conference Proceedings, Vol. 1, 2016, pp. 14–19.

[68] T. Don, T.A.B. Revolution, How the technology behind bitcoin is changing money, business, and the world, Inf. Syst. (2016) 100–150.

[69] R. Böhme, N. Christin, B. Edelman, T. Moore, Bitcoin: Economics, technology, and governance, J. Econ. Perspect. 29 (2) (2015) 213–238.

[70] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi, Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab, in: International Conference on Financial Cryptography and Data Security, Springer, 2016, pp. 79–94.

[71] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. Kishigami, Blockchain contract: Securing a blockchain applied to smart contracts, in: 2016 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2016, pp. 467–468.

[72] M. Khazraee, I. Magaki, L.V. Gutierrez, M. Taylor, ASIC clouds: Specializing the datacenter, IEEE Micro (2017).

[73] http://www.genaro.network/. (2018). (2018).

[74] M. Chung, J. Kim, The internet information and technology research directions based on the fourth industrial revolution, KSII Trans. Internet Inf. Syst. 10 (3) (2016).

[75] A. Bahga, V.K. Madisetti, Blockchain platform for industrial internet of things, J. Softw. Eng. Appl. 9 (10) (2016) 533.

[76] S.A. Abeyratne, R.P. Monfared, Blockchain ready manufacturing supply chain using distributed ledger, 2016.

[77] J. Basden, M. Cottrell, How utilities are using blockchain to modernize the grid, Harv. Bus. Rev. 23 (2017).

[78] P.K. Sharma, S.Y. Moon, J.H. Park, Block-VN: A distributed blockchain based vehicular network architecture in smart city, JIPS 13 (1) (2017) 184–195.

[79] A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data, in: Proceedings of IEEE Open & Big Data Conference, Vol. 13, 2016, p. 13.

[80] Relictum Pro, URL https://relictumpro.medium.com/.

[81] H. Wang, Y. Wang, Z. Cao, Z. Li, G. Xiong, An overview of blockchain security analysis, in: China Cyber Security Annual Conference, Springer, Singapore, 2018, pp. 55–72.

[82] Y. Wen, F. Lu, Y. Liu, X. Huang, Attacks and countermeasures on blockchains: A survey from layering perspective, Comput. Netw. (2021) 107978.

[83] C. Fromknecht, D. Velicanu, S. Yakoubov, A decentralized public key infrastructure with identity retention, IACR Cryptol. ePrint Arch. 2014 (2014) 803.

[84] J.A. Garay, Blockchain-based consensus (keynote), in: 19th International Conference on Principles of Distributed Systems (OPODIS 2015), Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

[85] K. Heires, The risks and rewards of blockchain technology, Risk Manage. 63 (2) (2016) 4.

[86] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: 2016 IEEE Symposium on Security and Privacy (SP), IEEE, 2016, pp. 839–858.

[87] Monero project, 2018, "https://getmonero.org/" (Online; accessed on 12-Dec-2018).

[88] V. Gramoli, On the danger of private blockchains, in: Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16), 2016.

[89] W. Suberg, We don't need blockchain: R3 consortium after $59 million research, Cointelegr. 22 (2017).

[90] E. Maras, R3 consortium's blockchain initiative: What makes 'Corda'different, Cryptocoins News (2016).

[91] J. Eberhardt, S. Tai, On or off the blockchain? Insights on off-chaining computation and data, in: European Conference on Service-Oriented and Cloud Computing, Springer, 2017, pp. 3–15.

[92] K. Wüst, A. Gervais, Do you need a blockchain? in: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2017, pp. 45–54.

[93] S. Ali, G. Wang, B. White, R.L. Cottrell, A blockchain-based decentralized data storage and access framework for pinger, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 1303–1308.

[94] J. Zahnentferner, Chimeric ledgers: Translating and unifying UTXO-based and account-based cryptocurrencies, IACR Cryptol. ePrint Arch. 2018 (2018) 262.

[95] S. Delgado-Segura, C. Pérez-Sola, G. Navarro-Arribas, J. Herrera-Joancomartí, Analysis of the bitcoin UTXO set, in: International Conference on Financial Cryptography and Data Security, Springer, 2018, pp. 78–91.

[96] L. Shin, The first government to secure land titles on the bitcoin blockchain expands project, Forbes 7 (2017) February.

[97] N. Chalaemwongwan, W. Kurutach, State of the art and challenges facing consensus protocols on blockchain, in: 2018 International Conference on Information Networking (ICOIN), IEEE, 2018, pp. 957–962.

[98] M. Sanchez, E. Exposito, J. Aguilar, Autonomic computing in manufacturing process coordination in industry 4.0 context, J. Ind. Inf. Integr. 19 (2020) 100159.

[99] N. Xie, W. Tan, X. Zheng, L. Zhao, L. Huang, Y. Sun, An efficient two-phase approach for reliable collaboration-aware service composition in cloud manufacturing, J. Ind. Inf. Integr. 23 (2021) 100211.

[100] D.G. Broo, U. Boman, M. Törngren, Cyber-physical systems research and education in 2030: Scenarios and strategies, J. Ind. Inf. Integr. 21 (2021) 100192.

[101] Z. Jiang, Y. Chang, X. Liu, Design of software-defined gateway for industrial interconnection, J. Ind. Inf. Integr. 18 (2020) 100130.

[102] M. Ghobakhloo, N.T. Ching, Adoption of digital technologies of smart manufacturing in SMEs, J. Ind. Inf. Integr. 16 (2019) 100107.

[103] E. Oztemel, S. Gursev, Literature review of Industry 4.0 and related technologies, J. Intell. Manuf. 31 (1) (2020) 127–182.

[104] ConsenSys codefi, 2021, "https://consensys.net/codefi/blog/" (Online; accessed on 13-Apr-2021).

[105] MedRec, 2021, "https://medrec.media.mit.edu/, 2016" (Online; accessed on 13-Apr-2021).

[106] MedicalChain, 2021, "Medicalchain, " https://medicalchain.com/en/, 2019" (Online; accessed on 13-Apr-2021).

[107] P. Ledger, Power Ledger White Paper, Power Ledger Pty Ltd, Australia, 2017, pp. 16–21, White Paper.

[108] Bankymooon - blockchain powered solutions and services, 2021, "http://bankymoon.co.za/, 2019" (Online; accessed on 13-Apr-2021).

[109] Q. Lin, H. Wang, X. Pei, J. Wang, Food safety traceability system based on blockchain and EPCIS, IEEE Access 7 (2019) 20698–20707.

[110] OriginTrail, 2021, "https://origintrail.io/, 2019" (Online; accessed on 13-Apr-2021).

[111] IBM Watson IoT platform, 2021, "https://www.ibm.com/docs/en/watson-iot-platform" (Online; accessed on 13-Apr-2021).

[112] P. Veena, S. Panikkar, S. Nair, P. Brody, Empowering the Edge-Practical Insights on a Decentralized Internet of Things, Vol. 17, IBM Institute for Business Value, 2015.

[113] K. Korpela, J. Hallikas, T. Dahlberg, Digital supply chain transformation toward blockchain integration, in: Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.

[114] E. Gökalp, U. Şener, P.E. Eren, Development of an assessment model for industry 4.0: industry 4.0-MM, in: International Conference on Software Process Improvement and Capability Determination, Springer, 2017, pp. 128–142.

[115] I. Kremenova, M. Gajdos, Decentralized networks: The future internet, Mob. Netw. Appl. (2019) 1–8.

[116] J.H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, K. Wehrle, Secure and anonymous decentralized Bitcoin mixing, Future Gener. Comput. Syst. 80 (2018) 448–466.

[117] Y. Wang, A. Kogan, Designing confidentiality-preserving blockchain-based transaction processing systems, Int. J. Account. Inf. Syst. 30 (2018) 1–18.

[118] Z. Ma, M. Jiang, H. Gao, Z. Wang, Blockchain for digital rights management, Future Gener. Comput. Syst. 89 (2018) 746–764.

[119] Y. Amoussou-Guenou, A. Del Pozzo, M. Potop-Butucaru, S. Tucci-Piergiovanni, Correctness and fairness of tendermint-core blockchains, 2018, arXiv preprint arXiv:1805.08429.

[120] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, Y. Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks, IEEE Internet Things J. (2018).

[121] M. Li, L. Zhu, X. Lin, Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing, IEEE Internet Things J. (2018).

[122] T.-T. Kuo, L. Ohno-Machado, Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks, 2018, arXiv preprint arXiv:1802.01746.

[123] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable Cities Soc. 39 (2018) 283–297.

[124] H. Kopp, D. Mödinger, F. Hauck, F. Kargl, C. Bösch, Design of a privacy-preserving decentralized file storage with financial incentives, in: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2017, pp. 14–22.

[125] P. Ellis, J. Hubbard, Flexibility trading platform—Using blockchain to create the most efficient demand-side response trading market, in: Transforming Climate Finance and Green Investment with Blockchains, Elsevier, 2018, pp. 99–109.

[126] N. Mohamed, J. Al-Jaroodi, S. Lazarova-Molnar, Leveraging the capabilities of industry 4.0 for improving energy efficiency in smart factories, IEEE Access 7 (2019) 18008–18020.

[127] https://komodoplatform.com/. 2008.

[128] W. Viriyasitavat, D. Hoonsopon, Blockchain characteristics and consensus in modern business processes, J. Ind. Inf. Integr. 13 (2019) 32–39.

[129] D.D.F. Maesa, P. Mori, L. Ricci, A blockchain based approach for the definition of auditable Access Control systems, Comput. Secur. 84 (2019) 93–119.

[130] W. Hao, J. Zeng, X. Dai, J. Xiao, Q.-S. Hua, H. Chen, K.-C. Li, H. Jin, Towards a trust-enhanced blockchain P2P topology for enabling fast and reliable broadcast, IEEE Trans. Netw. Serv. Manag. 17 (2) (2020) 904–917.

[131] Q. Lu, A. Binh Tran, I. Weber, H. O'Connor, P. Rimba, X. Xu, M. Staples, L. Zhu, R. Jeffery, Integrated model-driven engineering of blockchain applications for business processes and asset management, Softw. - Pract. Exp. (2020).

[132] Y. Lu, The blockchain: State-of-the-art and research challenges, J. Ind. Inf. Integr. 15 (2019) 80–90.

[133] X. Xu, H. Bandara, Q. Lu, I. Weber, L. Bass, L. Zhu, A decision model for choosing patterns in blockchain-based applications, in: 18th IEEE Int. Conf. on Software Architecture (ICSA 2021), 2021.

[134] S. Kalra, S. Goel, M. Dhawan, S. Sharma, ZEUS: Analyzing safety of smart contracts, in: Ndss, 2018, pp. 1–12.

[135] C. Zhang, Z. Ni, Y. Xu, E. Luo, L. Chen, Y. Zhang, A trustworthy industrial data management scheme based on redactable blockchain, J. Parallel Distrib. Comput. (2021).

[136] M. Madine, K. Salah, R. Jayaraman, Y. Al-Hammadi, J. Arshad, I. Yaqoob, Application-level interoperability for blockchain networks, 2021.

[137] A. Mavridou, A. Laszka, Designing secure ethereum smart contracts: A finite state machine based approach, in: International Conference on Financial Cryptography and Data Security, Springer, 2018, pp. 523–540.

[138] X. Cheng, F. Chen, D. Xie, H. Sun, C. Huang, Design of a secure medical data sharing scheme based on blockchain, J. Med. Syst. 44 (2) (2020) 1–11.

[139] G. Governatori, F. Idelberger, Z. Milosevic, R. Riveret, G. Sartor, X. Xu, On legal contracts, imperative and declarative smart contracts, and blockchain systems, Artif. Intell. Law 26 (4) (2018) 377–409.

[140] X. Xu, G. Sun, L. Luo, H. Cao, H. Yu, A.V. Vasilakos, Latency performance modeling and analysis for hyperledger fabric blockchain network, Inf. Process. Manage. 58 (1) (2021) 102436.

[141] L. Stoykov, K. Zhang, H.-A. Jacobsen, Vibes: fast blockchain simulations for large-scale peer-to-peer networks, in: Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos, 2017, pp. 19–20.

[142] M. Jin, X. Chen, S.-J. Lin, Reducing the bandwidth of block propagation in bitcoin network with erasure coding, IEEE Access 7 (2019) 175606–175613.

[143] X. Min, Q. Li, L. Liu, L. Cui, A permissioned blockchain framework for supporting instant transaction and dynamic block size, in: 2016 IEEE Trustcom/BigDataSE/ISPA, IEEE, 2016, pp. 90–96.

[144] N. Singh, M. Vardhan, Multi-objective optimization of block size based on CPU power and network bandwidth for blockchain applications, in: Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems, Springer, 2021, pp. 69–78.

[145] H.-Y. Paik, X. Xu, H.D. Bandara, S.U. Lee, S.K. Lo, Analysis of data management in blockchain-based systems: From architecture to governance, IEEE Access 7 (2019) 186091–186107.

[146] J. Sedlmeir, H.U. Buhl, G. Fridgen, R. Keller, The energy consumption of blockchain technology: beyond myth, Bus. Inf. Syst. Eng. 62 (6) (2020) 599–608.

[147] R. Belchior, A. Vasconcelos, S. Guerreiro, M. Correia, A survey on blockchain interoperability: Past, present, and future trends, 2020, arXiv preprint arXiv: 2005.14282.

[148] J. Chang, J. Ni, J. Xiao, X. Dai, H. Jin, SynergyChain: A multichain-based data sharing framework with hierarchical access control, IEEE Internet Things J. (2021).

[149] T. Hardjono, A. Lipton, A. Pentland, Toward an interoperability architecture for blockchain autonomous systems, IEEE Trans. Eng. Manage. 67 (4) (2019) 1298–1309.

[150] W.J. Gordon, C. Catalini, Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability, Comput. Struct. Biotechnol. J. 16 (2018) 224–230.

[151] B. Sundarakani, A. Ajaykumar, A. Gunasekaran, Big data driven supply chain design and applications for blockchain: An action research using case study approach, Omega (2021) 102452.

[152] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?—a systematic review, PLoS One 11 (10) (2016) e0163477.

[153] Z. Li, R.Y. Zhong, Z. Tian, H.-N. Dai, A.V. Barenji, G.Q. Huang, Industrial blockchain: A state-of-the-art survey, Robot. Comput.-Integr. Manuf. 70 (2021) 102124.

[154] J. Leng, D. Yan, Q. Liu, K. Xu, J.L. Zhao, R. Shi, L. Wei, D. Zhang, X. Chen, ManuChain: Combining permissioned blockchain with a holistic optimization model as bi-level intelligence for smart manufacturing, IEEE Trans. Syst. Man Cybern.: Syst. 50 (1) (2019) 182–192.

[155] F. Werner, M. Basalla, J. Schneider, D. Hays, J. Vom Brocke, Blockchain adoption from an interorganizational systems perspective–a mixed-methods approach, Inf. Syst. Manage. (2020) 1–16.

[156] S.K. Das, The measurement of flexibility in manufacturing systems, Int. J. Flex. Manuf. Syst. 8 (1) (1996) 67–93.

[157] L. D'Oriano, G. Mastandrea, G. Rana, G. Raveduto, V. Croce, M. Verber, M. Bertoncini, Decentralized blockchain flexibility system for smart grids: Requirements engineering and use cases, in: 2018 International IEEE Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE), IEEE, 2018, pp. 39–44.

[158] G. Fragapane, D. Ivanov, M. Peron, F. Sgarbossa, J.O. Strandhagen, Increasing flexibility and productivity in Industry 4.0 production networks with autonomous mobile robots and smart intralogistics, Ann. Oper. Res. (2020) 1–19.

[159] B. Fahimnia, C.S. Tang, H. Davarzani, J. Sarkis, Quantitative models for managing supply chain risks: A review, European J. Oper. Res. 247 (1) (2015) 1–15.

[160] S. Goel, A. Singh, R. Garg, M. Verma, P. Jayachandran, Resource fairness and prioritization of transactions in permissioned blockchain systems (industry track), in: Proceedings of the 19th International Middleware Conference Industry, 2018, pp. 46–53.

[161] P. Danzi, M. Angjelichinoski, Č. Stefanović, P. Popovski, Distributed proportional-fairness control in microgrids via blockchain smart contracts, in: 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2017, pp. 45–51.

[162] M. Li, D. Hu, C. Lal, M. Conti, Z. Zhang, Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things, IEEE Trans. Ind. Inf. 16 (10) (2020) 6564–6574.

[163] N. Pathak, A. Mukherjee, S. Misra, Aerialblocks: Blockchain-enabled UAV virtualization for industrial IoT, IEEE Internet Things Mag. (2021).

[164] W. Sun, A.T. Dedahanov, H.Y. Shin, W.P. Li, Using extended complexity theory to test SMEs' adoption of Blockchain-based loan system, PLoS One 16 (2) (2021) e0245964.

[165] M.A. Engelhardt, Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector, Technol. Innov. Manage. Rev. 7 (10) (2017).

[166] J. Leng, G. Ruan, P. Jiang, K. Xu, Q. Liu, X. Zhou, C. Liu, Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey, Renew. Sustain. Energy Rev. 132 (2020) 110112.

[167] Y. Lu, Blockchain and the related issues: a review of current research topics, J. Manage. Anal. 5 (4) (2018) 231–255.

[168] S. Porru, A. Pinna, M. Marchesi, R. Tonelli, Blockchain-oriented software engineering: challenges and new directions, in: 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), IEEE, 2017, pp. 169–171.

[169] G. Zyskind, O. Nathan, A. Pentland, Enigma: Decentralized computation platform with guaranteed privacy, 2015, arXiv abs/1506.03471.

[170] H.D. Chang, Blockchain: Disrupting data protection?, 2017.

[171] D. Nasonov, A.A. Visheratin, A. Boukhanovsky, Blockchain-based transaction integrity in distributed big data marketplace, in: International Conference on Computational Science, Springer, 2018, pp. 569–577.

[172] H. Subramanian, Decentralized blockchain-based electronic marketplaces, Commun. ACM 61 (1) (2017) 78–84.

[173] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, V. Sassone, Blockchain-based database to ensure data integrity in cloud computing environments, 2017.

[174] A. Iftekhar, X. Cui, M. Hassan, W. Afzal, Application of blockchain and Internet of Things to ensure tamper-proof data availability for food safety, J. Food Qual. 2020 (2020).

[175] H.G. Do, W.K. Ng, Blockchain-based system for secure data storage with private keyword search, in: 2017 IEEE World Congress on Services (SERVICES), IEEE, 2017, pp. 90–93.

[176] I. Weber, V. Gramoli, A. Ponomarev, M. Staples, R. Holz, A.B. Tran, P. Rimba, On availability for blockchain-based systems, in: 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 2017, pp. 64–73.

[177] A. Yastrebova, R. Kirichek, Y. Koucheryavy, A. Borodin, A. Koucheryavy, Future networks 2030: Architecture & requirements, in: 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), IEEE, 2018, pp. 1–8.

[178] K. Hameed, S. Garg, M.B. Amin, B. Kang, A formally verified blockchain-based decentralised authentication scheme for the internet of things, J. Supercomput. (2021) 1–41.

[179] G.D. Putra, V. Dedeoglu, S.S. Kanhere, R. Jurdak, A. Ignjatovic, Trust-based blockchain authorization for IoT, IEEE Trans. Netw. Serv. Manag. (2021).

[180] C. Esposito, M. Ficco, B.B. Gupta, Blockchain-based authentication and authorization for smart city applications, Inf. Process. Manage. 58 (2) (2021) 102468.

[181] A. Ahmad, M. Saad, M. Bassiouni, A. Mohaisen, Towards blockchain-driven, secure and transparent audit logs, in: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2018, pp. 443–448.

[182] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, R. Sirdey, Towards better availability and accountability for iot updates by means of a blockchain, in: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2017, pp. 50–58.

[183] L. Yang, X.-Y. Liu, W. Gong, Secure smart home systems: A blockchain perspective, in: IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2020, pp. 1003–1008.

[184] M.S. Al-Rakhami, M. Al-Mashari, A blockchain-based trust model for the internet of things supply chain management, Sensors 21 (5) (2021) 1759.

[185] F. Dewanta, M. Mambo, BPT scheme: Establishing trusted vehicular fog computing service for rural area based on blockchain approach, IEEE Trans. Veh. Technol. 70 (2) (2021) 1752–1769.

[186] D.J. Bernstein, T. Lange, et al., SafeCurves: choosing safe curves for elliptic curve cryptography, 2015, URL: https://safecurves.cr.yp.to. Citations in this document 9 (2014).

[187] U. Chohan, The Cryptocurrency Tumblers: Risks, Legality and Oversight, SSRN, 2017.

[188] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, Springer, 2017, pp. 164–186.

[189] S.N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, A. Bani-Hani, Blockchain smart contracts: Applications, challenges, and future trends, Peer-to-Peer Netw. Appl. (2021) 1–25.

[190] N. Popper, A hacking of more than $50 million dashes hopes in the world of virtual currency, N.Y. Times 17 (2016).

[191] F.J. de Haro-Olmo, A.J. Varela-Vaca, J.A. Álvarez-Bermejo, Blockchain from the perspective of privacy and anonymisation: a systematic literature review, Sensors 20 (24) (2020) 7171.

[192] D.W. Kravitz, J. Cooper, Securing user identity and transactions symbiotically: IoT meets blockchain, in: 2017 Global Internet of Things Summit (GIoTS), IEEE, 2017, pp. 1–6.

[193] D. Ron, A. Shamir, Quantitative analysis of the full bitcoin transaction graph, in: International Conference on Financial Cryptography and Data Security, Springer, 2013, pp. 6–24.

[194] A. Pfitzmann, M. Hansen, A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, 2010, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, v0.34.

[195] D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of things security: A top-down survey, Comput. Netw. 141 (2018) 199–221.

[196] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, FairAccess: a new Blockchain-based access control framework for the Internet of Things, Secur. Commun. Netw. 9 (18) (2016) 5943–5964.

[197] S.S. Feshina, O.V. Konovalova, N.G. Sinyavsky, Industry 4.0—transition to new economic reality, in: Industry 4.0: Industrial Revolution of the 21st Century, Springer, 2019, pp. 111–120.

[198] D. Mhlanga, Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion, Int. J. Financ. Stud. 8 (3) (2020) 45.
[199] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, M. Arami, How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees, Technol. Forecast. Soc. Change 158 (2020) 120166.
[200] K. Kanemura, K. Toyoda, T. Ohtsuki, Design of privacy-preserving mobile Bitcoin client based on γ-deniability enabled bloom filter, in: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2017, pp. 1–6.
[201] K. Bhaskaran, P. Ilfrich, D. Liffman, C. Vecchiola, P. Jayachandran, A. Kumar, F. Lim, K. Nandakumar, Z. Qin, V. Ramakrishna, et al., Double-blind consent-driven data sharing on blockchain, in: 2018 IEEE International Conference on Cloud Engineering (IC2E), IEEE, 2018, pp. 385–391.
[202] A. Biryukov, D. Khovratovich, S. Tikhomirov, Privacy-preserving KYC on Ethereum, 2018.
[203] B. Li, Y. Wang, P. Shi, H. Chen, L. Cheng, FPPB: a fast and privacy-preserving method based on the permissioned blockchain for fair transactions in sharing economy, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 1368–1373.
[204] Y. Liu, X. Liu, C. Tang, J. Wang, L. Zhang, Unlinkable coin mixing scheme for transaction privacy enhancement of bitcoin, IEEE Access 6 (2018) 23261–23270.
[205] J.J. Hathaliya, S. Tanwar, An exhaustive survey on security and privacy issues in Healthcare 4.0, Comput. Commun. 153 (2020) 311–335.
[206] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2) (2019) 326.
[207] H.M. Hussien, S.M. Yasin, N.I. Udzir, M.I.H. Ninggal, S. Salman, Blockchain technology in the healthcare industry: Trends and opportunities, J. Ind. Inf. Integr. (2021) 100217.
[208] G. Aceto, V. Persico, A. Pescapé, Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0, J. Ind. Inf. Integr. 18 (2020) 100129.
[209] T. McGhin, K.-K.R. Choo, C.Z. Liu, D. He, Blockchain in healthcare applications: Research challenges and opportunities, J. Netw. Comput. Appl. (2019).
[210] K. Fan, S. Wang, Y. Ren, H. Li, Y. Yang, Medblock: Efficient and secure medical data sharing via blockchain, J. Med. Syst. 42 (8) (2018) 1–11.
[211] A.F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J.M.R. Tavares, V.H.C. de Albuquerque, A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform, Cogn. Syst. Res. 52 (2018) 1–11.
[212] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. 40 (10) (2016) 1–8.
[213] Q. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: Trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767.
[214] Y. Sun, R. Zhang, X. Wang, K. Gao, L. Liu, A decentralizing attribute-based signature for healthcare blockchain, in: 2018 27th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2018, pp. 1–9.
[215] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, J. Med. Syst. 42 (8) (2018) 140.
[216] R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, IEEE Access 6 (2018) 11676–11686.
[217] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in: 2016 2nd International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25–30.
[218] Y. Ji, J. Zhang, J. Ma, C. Yang, X. Yao, BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems, J. Med. Syst. 42 (8) (2018) 147.
[219] J. Zhou, F. Tang, H. Zhu, N. Nan, Z. Zhou, Distributed data vending on blockchain, in: 2018 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, 2018, pp. 1100–1107.
[220] W. Viriyasitavat, D. Hoonsopon, Z. Bi, Augmenting cryptocurrency in smart supply chain, J. Ind. Inf. Integr. 21 (2021) 100188.
[221] A.A. Vieira, L.M. Dias, M.Y. Santos, G.A. Pereira, J.A. Oliveira, Supply chain data integration: A literature review, J. Ind. Inf. Integr. (2020) 100161.
[222] H. Golpîra, S.A.R. Khan, S. Safaeipour, A review of logistics internet-of-things: Current trends and scope for future research, J. Ind. Inf. Integr. (2021) 100194.
[223] C.S. Tang, L.P. Veelenturf, The strategic role of logistics in the industry 4.0 era, Transp. Res. E 129 (2019) 1–11.
[224] M. Faheem, S.B.H. Shah, R.A. Butt, B. Raza, M. Anwar, M.W. Ashraf, M.A. Ngadi, V.C. Gungor, Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges, Comp. Sci. Rev. 30 (2018) 1–30.
[225] R. Khan, S.U. Khan, Design and implementation of UPnP-based energy gateway for demand side management in smart grid, J. Ind. Inf. Integr. 8 (2017) 8–21.
[226] N. Dragicevic, A. Ullrich, E. Tsui, N. Gronau, A conceptual model of knowledge dynamics in the industry 4.0 smart grid scenario, Knowl. Manage. Res. Pract. 18 (2) (2020) 199–213.
[227] F. Al-Turjman, M. Abujubbeh, IoT-enabled smart grid via SM: An overview, Future Gener. Comput. Syst. 96 (2019) 579–590.
[228] A.A.G. Agung, R. Handayani, Blockchain for smart grid, J. King Saud Univ.-Comput. Inf. Sci. (2020).
[229] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, Y. Ma, Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities, IEEE Commun. Mag. 56 (7) (2018) 82–88.
[230] C. Rottondi, G. Verticale, A privacy-friendly gaming framework in smart electricity and water grids, IEEE Access 5 (2017) 14221–14233.
[231] K. Ujjwal, S. Garg, J. Hilton, J. Aryal, N. Forbes-Smith, Cloud computing in natural hazard modeling systems: Current research trends and future directions, Int. J. Disaster Risk Reduct. (2019) 101188.
[232] S.K. Battula, S. Garg, R.K. Naha, P. Thulasiraman, R. Thulasiram, A micro-level compensation-based cost model for resource allocation in a fog environment, Sensors 19 (13) (2019) 2954.
[233] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in IoT: The challenges, and a way forward, J. Netw. Comput. Appl. (2018).
[234] S.-C. Cha, J.-F. Chen, C. Su, K.-H. Yeh, A blockchain connected gateway for BLE-based devices in the internet of things, IEEE Access 6 (2018) 24639–24649.
[235] J. Wan, J. Li, M. Imran, D. Li, et al., A blockchain-based solution for enhancing security and privacy in smart factory, IEEE Trans. Ind. Inf. (2019).
[236] T. Le, M.W. Mutka, CapChain: A privacy preserving access control framework based on blockchain for pervasive environments, in: 2018 IEEE International Conference on Smart Computing (SMARTCOMP), IEEE, 2018, pp. 57–64.
[237] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, F. Wortmann, Privacy-preserving data certification in the internet of things: Leveraging blockchain technology to protect sensor data, J. Assoc. Inf. Syst. (2019).
[238] S. Singh, I.-H. Ra, W. Meng, M. Kaur, G.H. Cho, SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology, Int. J. Distrib. Sens. Netw. 15 (4) (2019) 1550147719844159.
[239] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, 2017, pp. 618–623.
[240] S.B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai, D. Trentesaux, A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0, Sustainability 12 (21) (2020) 9179.
[241] P.J. Lu, L.-Y. Yeh, J.-L. Huang, An privacy-preserving cross-organizational authentication/authorization/accounting system using blockchain technology, in: 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1–6.
[242] K. Fan, Y. Ren, Y. Wang, H. Li, Y. Yang, Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G, IET Commun. 12 (5) (2018) 527–532, http://dx.doi.org/10.1049/iet-com.2017.0619.
[243] L. Shu, Y. Chen, Z. Huo, N. Bergmann, L. Wang, When mobile crowd sensing meets traditional industry, IEEE Access 5 (2017) 15300–15307.
[244] F.R.P.M. Vianna, A.R. Graeml, J. Peinado, The role of crowdsourcing in industry 4.0: a systematic literature review, Int. J. Comput. Integr. Manuf. 33 (4) (2020) 411–427.
[245] A. Capponi, C. Fiandrino, B. Kantarci, L. Foschini, D. Kliazovich, P. Bouvry, A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2419–2465.
[246] Z. Chen, C. Fiandrino, B. Kantarci, On blockchain integration into mobile crowdsensing via smart embedded devices: A comprehensive survey, J. Syst. Archit. (2021) 102011.
[247] J. Wang, M. Li, Y. He, H. Li, K. Xiao, C. Wang, A blockchain based privacy-preserving incentive mechanism in crowdsensing applications, IEEE Access 6 (2018) 17545–17556.
[248] C. Cai, Y. Zheng, C. Wang, Leveraging crowdsensed data streams to discover and sell knowledge: A secure and efficient realization, in: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2018, pp. 589–599.
[249] D. Chatzopoulos, S. Gujar, B. Faltings, P. Hui, Privacy preserving and cost optimal mobile crowdsensing using smart contracts on blockchain, in: 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), IEEE, 2018, pp. 442–450.
[250] B. Li, Y. Wang, RZKPB: A privacy-preserving blockchain-based fair transaction method for sharing economy, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), 2018, pp. 1164–1169.
[251] L. Wang, X. Shen, J. Li, J. Shao, Y. Yang, Cryptographic primitives in blockchains, J. Netw. Comput. Appl. 127 (2019) 43–58.

[252] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.
[253] L. Lamport, Constructing Digital Signatures from a One-Way Function, Tech. rep., Technical Report CSL-98, SRI International Palo Alto, 1979.
[254] D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures, J. Cryptol. 13 (3) (2000) 361–396.
[255] L. Harn, Group-oriented (t, n) threshold digital signature scheme and digital multisignature, IEE Proc.-Comput. Digit. Tech. 141 (5) (1994) 307–313.
[256] A. Boldyreva, Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme, in: International Workshop on Public Key Cryptography, Springer, 2003, pp. 31–46.
[257] Z. Bao, B. Wang, W. Shi, A privacy-preserving, decentralized and functional bitcoin e-voting protocol, in: 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), IEEE, 2018, pp. 252–256.
[258] F. Zhang, K. Kim, ID-based blind signature and ring signature from pairings, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2002, pp. 533–547.
[259] D. Chaum, Blind signatures for untraceable payments, in: Advances in Cryptology, Springer, 1983, pp. 199–203.
[260] E. Owiyo, Y. Wang, E. Asamoah, D. Kamenyi, I. Obiri, Decentralized privacy preserving reputation system, 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC) (2018) 665–672.
[261] N. Malik, P. Nanda, A. Arora, X. He, D. Puthal, Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 674–679.
[262] A. Khalique, K. Singh, S. Sood, Implementation of elliptic curve digital signature algorithm, Int. J. Comput. Appl. 2 (2) (2010) 21–27.
[263] C.-C. Yang, T.-Y. Chang, M.-S. Hwang, A (t, n) multi-secret sharing scheme, Appl. Math. Comput. 151 (2) (2004) 483–490.
[264] H. Chen, H.-L. Wu, C.-C. Chang, L.-S. Chen, Light repository blockchain system with multisecret sharing for industrial big data, Secur. Commun. Netw. 2019 (2019).
[265] M.C. Doganay, T.B. Pedersen, Y. Saygin, E. Savaş, A. Levi, Distributed privacy preserving k-means clustering with additive secret sharing, in: Proceedings of the 2008 International Workshop on Privacy and Anonymity in Information Society, ACM, 2008, pp. 3–11.
[266] C. Rackoff, D.R. Simon, Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack, in: Annual International Cryptology Conference, Springer, 1991, pp. 433–444.
[267] O. Goldreich, A. Kahan, How to construct constant-round zero-knowledge proof systems for NP, J. Cryptol. 9 (3) (1996) 167–189.
[268] A trustless, anonymous transaction system for CloakCoin, 2016.
[269] CoinJoin: Bitcoin privacy for the real world (someday!) bitcoin forum, 2016..
[270] L. Sweeney, K-anonymity: A model for protecting privacy, Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10 (05) (2002) 557–570.
[271] N. Li, T. Li, S. Venkatasubramanian, T-closeness: Privacy beyond k-anonymity and l-diversity, in: 2007 IEEE 23rd International Conference on Data Engineering, IEEE, 2007, pp. 106–115.
[272] M.A. Maloof, Machine Learning and Data Mining for Computer Security: Methods and Applications, Springer, 2006.
[273] D. Zeng, H. Chen, R. Lusch, S.-H. Li, Social media analytics and intelligence, IEEE Intell. Syst. 25 (6) (2010) 13–16.
[274] C.M. Bishop, Pattern Recognition and Machine Learning, springer, 2006.
[275] R. Shokri, V. Shmatikov, Privacy-preserving deep learning, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM, 2015, pp. 1310–1321.
[276] H.B. McMahan, E. Moore, D. Ramage, S. Hampson, et al., Communication-efficient learning of deep networks from decentralized data, 2016, arXiv preprint arXiv:1602.05629.
[277] D.B. Rawat, L. Njilla, K.A. Kwiat, C.A. Kamhoua, Ishare: Blockchain-based privacy-aware multi-agent information sharing games for cybersecurity, in: 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 425–431.
[278] C. Decker, R. Wattenhofer, Bitcoin transaction malleability and MtGox, in: European Symposium on Research in Computer Security, Springer, 2014, pp. 313–326.
[279] Segregated witness (consensus layer), https://github.com/codeshark/bips/blob/segwit/bip-codeshark-jl2012-segwit.mediawiki.
[280] M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek, Fair two-party computations via bitcoin deposits, in: International Conference on Financial Cryptography and Data Security, Springer, 2014, pp. 105–121.
[281] M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek, How to deal with malleability of bitcoin transactions, 2013, arXiv preprint arXiv:1312.3230.
[282] G. Ma, C. Ge, L. Zhou, Achieving reliable timestamp in the bitcoin platform, Peer-to-Peer Netw. Appl. 13 (2020) 2251–2259.
[283] A.M. Khalifa, A.M. Bahaa-Eldin, M.A. Sobh, Quantum attacks and defenses for proof-of-stake, in: 2019 14th International Conference on Computer Engineering and Systems (ICCES), IEEE, 2019, pp. 112–117.
[284] E. Androulaki, A. De Caro, T. Kramp, D.W. Kravitz, A. Sorniotti, M. Vukolic, Resisting replay attacks efficiently in a permissioned and privacy-preserving blockchain network, 2019, US Patent 10, 230, 756.
[285] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles, IEEE Trans. Intell. Transp. Syst. 19 (7) (2018) 2204–2220.
[286] N. Hajdarbegovic, Bitcoin miners ditch ghash. io pool over fears of 51% attack, 2014.
[287] M. Bastiaan, Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin, 2015, Available at http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-oftwo-phase-proof-of-work-in-bitcoin.pdf.
[288] M. Saad, M.T. Thai, A. Mohaisen, POSTER: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization, in: Proceedings of the 2018 on Asia Conference on Computer and Communications Security, 2018, pp. 809–811.
[289] M. Saad, L. Njilla, C. Kamhoua, J. Kim, D. Nyang, A. Mohaisen, Mempool optimization for defending against ddos attacks in pow-based blockchain systems, in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2019, pp. 285–292.
[290] M. Vasek, M. Thornton, T. Moore, Empirical analysis of denial-of-service attacks in the bitcoin ecosystem, in: International Conference on Financial Cryptography and Data Security, Springer, 2014, pp. 57–71.
[291] A. Feder, N. Gandal, J. Hamrick, T. Moore, The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox, J. Cybersecur. 3 (2) (2018) 137–144.
[292] A. Singh, et al., Eclipse attacks on overlay networks: Threats and defenses, in: IEEE INFOCOM, Citeseer, 2006.
[293] E.A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on bitcoin's peer-to-peer network, in: 24th USENIX Security Symposium (USENIX Security 15)., 2015.
[294] G. Zyskind, O. Nathan, et al., Decentralizing privacy: Using blockchain to protect personal data, in: 2015 IEEE Security and Privacy Workshops, IEEE, 2015, pp. 180–184.
[295] S. Friebe, I. Sobik, M. Zitterbart, DecentID: Decentralized and privacy-preserving identity storage system using smart contracts, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 37–42.
[296] Z. Zhang, Y. Zhang, Y.C. Hu, Z.M. Mao, Practical defenses against BGP prefix hijacking, in: Proceedings of the 2007 ACM CoNEXT Conference, ACM, 2007, p. 3.
[297] M. Lepinski, K. Sriram, Bgpsec Protocol Specification, RFC8205, 2017.
[298] J. Hong, The state of phishing attacks, Commun. ACM 55 (1) (2012) 74–81.
[299] A. Kiayias, G. Panagiotakos, On trees, chains and fast transactions in the blockchain, in: International Conference on Cryptology and Information Security in Latin America, Springer, 2017, pp. 327–351.
[300] M. Apostolaki, A. Zohar, L. Vanbever, Hijacking bitcoin: Routing attacks on cryptocurrencies, in: 2017 IEEE Symposium on Security and Privacy (SP), IEEE, 2017, pp. 375–392.
[301] J.C. Song, M.A. Demir, J.J. Prevost, P. Rad, Blockchain design for trusted decentralized iot networks, in: 2018 13th Annual Conference on System of Systems Engineering (SoSE), IEEE, 2018, pp. 169–174.
[302] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future for internet of things security: A position paper, Digit. Commun. Netw. 4 (3) (2018) 149–160.
[303] M. Fleder, M.S. Kester, S. Pillai, Bitcoin transaction graph analysis, 2015, arXiv preprint arXiv:1502.01657.
[304] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, K. Ren, A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks, IEEE Netw. 32 (6) (2018) 184–192.
[305] P. Gaži, A. Kiayias, A. Russell, Stake-bleeding attacks on proof-of-stake blockchains, in: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, 2018, pp. 85–92.
[306] R. Tahir, M. Huzaifa, A. Das, M. Ahmad, C. Gunter, F. Zaffar, M. Caesar, N. Borisov, Mining on someone else's dime: Mitigating covert mining operations in clouds and enterprises, in: International Symposium on Research in Attacks, Intrusions, and Defenses, Springer, 2017, pp. 287–310.
[307] M. Saad, L. Njilla, C. Kamhoua, A. Mohaisen, Countering selfish mining in blockchains, in: 2019 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2019, pp. 360–364.
[308] A. Judmayer, N. Stifter, A. Zamyatin, I. Tsabary, I. Eyal, P. Gazi, S. Meiklejohn, E.R. Weippl, Pay-to-win: Incentive attacks on proof-of-work cryptocurrencies, IACR Cryptol. ePrint Arch. 2019 (2019) 775.
[309] P. McCorry, S.F. Shahandashti, F. Hao, Refund attacks on Bitcoin's payment protocol, in: International Conference on Financial Cryptography and Data Security, Springer, 2016, pp. 581–599.

[310] S.-Y. Chang, Y. Park, Silent timestamping for blockchain mining pool security, in: 2019 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2019, pp. 1–5.
[311] Q. Hu, S. Wang, X. Cheng, A game theoretic analysis on block withholding attacks using the zero-determinant strategy, in: Proceedings of the International Symposium on Quality of Service, 2019, pp. 1–10.
[312] S. Elliott, Nash equilibrium of multiple, non-uniform bitcoin block withholding attackers, in: 2019 2nd International Conference on Data Intelligence and Security (ICDIS), IEEE, 2019, pp. 144–151.
[313] W. Li, M. Cao, Y. Wang, C. Tang, F. Lin, Mining pool game model and Nash equilibrium analysis for pow-based blockchain networks, IEEE Access 8 (2020) 101049–101060.
[314] C. Natoli, V. Gramoli, The balance attack against proof-of-work blockchains: The R3 testbed as an example, 2016, arXiv preprint arXiv:1612.09426.
[315] C.F. Torres, J. Schütte, R. State, Osiris: Hunting for integer bugs in ethereum smart contracts, in: Proceedings of the 34th Annual Computer Security Applications Conference, 2018, pp. 664–676.
[316] M. Rodler, W. Li, G.O. Karame, L. Davi, Sereum: Protecting existing smart contracts against re-entrancy attacks, 2018, arXiv preprint arXiv:1812.05934.
[317] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen, B. Roscoe, Reguard: finding reentrancy bugs in smart contracts, in: 2018 IEEE/ACM 40th International Conference on Software Engineering: Companion (ICSE-Companion), IEEE, 2018, pp. 65–68.
[318] Y. Feng, E. Torlak, R. Bodik, Precise attack synthesis for smart contracts, 2019, arXiv preprint arXiv:1902.06067.
[319] A. Juels, A. Kosba, E. Shi, The ring of gyges: Investigating the future of criminal smart contracts, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 283–295.
[320] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town crier: An authenticated data feed for smart contracts, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 270–282.
[321] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254–269.
[322] enzymefinance/oyente: An Analysis Tool for Smart Contracts, URL https://github.com/enzymefinance/oyente.
[323] T. Chen, X. Li, Y. Wang, J. Chen, Z. Li, X. Luo, M.H. Au, X. Zhang, An adaptive gas cost mechanism for ethereum to defend against under-priced dos attacks, in: International Conference on Information Security Practice and Experience, Springer, 2017, pp. 3–24.
[324] G.G. Dagher, P.B. Marella, M. Milojkovic, J. Mohler, BroncoVote: Secure voting system using ethereum's blockchain, 2018.
[325] S. Heiberg, I. Kubjas, J. Siim, J. Willemson, On trade-offs of applying block chains for electronic voting bulletin boards, 2018, p. 259, E-Vote-ID 2018.
[326] Z. Banković, J.C. Vallejo, D. Fraga, J.M. Moya, Detecting bad-mouthing attacks on reputation systems using self-organizing maps, in: Computational Intelligence in Security for Information Systems, Springer, 2011, pp. 9–16.
[327] A. Biryukov, Chosen plaintext and chosen ciphertext attack, in: Encyclopedia of Cryptography and Security, Springer, 2011, p. 205.
[328] H. Mayer, ECDSA security in bitcoin and ethereum: a research survey, CoinFaabrik 28 (2016) 126, June.
[329] W. Cody, T. Amir, Darkwallet, 2017.
[330] E. Fletcher, C. Larkin, S. Corbet, Countering money laundering and terrorist financing: A case for bitcoin regulation, Res. Int. Bus. Finance 56 (2021) 101387.
[331] S. Saxena, B. Bhushan, M.A. Ahad, Blockchain based solutions to secure IoT: Background, integration trends and a way forward, J. Netw. Comput. Appl. (2021) 103050.
[332] M. Zachariadis, G. Hileman, S.V. Scott, Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services, Inf. Organ. 29 (2) (2019) 105–117.
[333] F. Amato, G. Cozzolino, F. Moscato, V. Moscato, F. Xhafa, A model for verification and validation of law compliance of smart-contracts in IoT environment, IEEE Trans. Ind. Inf. (2021).
[334] P. Yeoh, Regulatory issues in blockchain technology, J. Financ. Regul. Compliance (2017).
[335] J. Vermeulen, Bitcoin and Ethereum vs Visa and PayPal–Transactions per Second, Vol. 22, My Broadband, 2017.
[336] T. Alladi, V. Chamola, R.M. Parizi, K.-K.R. Choo, Blockchain applications for industry 4.0 and industrial IoT: A review, IEEE Access 7 (2019) 176935–176951.
[337] Q. Zhou, H. Huang, Z. Zheng, J. Bian, Solutions to scalability of blockchain: A survey, IEEE Access 8 (2020) 16440–16455.
[338] P.A. Shukla, S. Samet, Systematization of knowledge on scalability aspect of blockchain systems, in: Future of Information and Communication Conference, Springer, 2020, pp. 130–138.
[339] F. Tian, An agri-food supply chain traceability system for China based on RFID & blockchain technology, in: 2016 13th International Conference on Service Systems and Service Management (ICSSSM), IEEE, 2016, pp. 1–6.
[340] A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in internet of things: challenges and solutions, 2016, arXiv preprint arXiv:1608.05187.
[341] M. Azeem, A. Haleem, S. Bahl, M. Javaid, R. Suman, D. Nandan, Big data applications to take up major challenges across manufacturing industries: A brief review, Mater. Today: Proc. (2021).
[342] B. Farahani, F. Firouzi, M. Luecking, The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions, J. Netw. Comput. Appl. 177 (2021) 102936.
[343] G. Rathee, M. Balasaraswathi, K.P. Chandran, S.D. Gupta, C. Boopathi, A secure IoT sensors communication in industry 4.0 using blockchain technology, J. Ambient Intell. Humaniz. Comput. 12 (1) (2021) 533–545.
[344] R. Yang, F.R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated blockchain and edge computing systems: A survey, some research issues and challenges, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1508–1532.
[345] J. Kang, Z. Xiong, C. Jiang, Y. Liu, S. Guo, Y. Zhang, D. Niyato, C. Leung, C. Miao, Scalable and communication-efficient decentralized federated edge learning with multi-blockchain framework, 2020, arXiv preprint arXiv:2008.04743.
[346] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, Y. Yang, A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling, ACM Comput. Surv. 53 (1) (2020) 1–32.
[347] U. Majeed, L.U. Khan, I. Yaqoob, S.A. Kazmi, K. Salah, C.S. Hong, Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges, J. Netw. Comput. Appl. (2021) 103007.
[348] B. Mishra, A. Kertesz, The use of MQTT in M2M and IoT systems: A survey, IEEE Access 8 (2020) 201071–201086.
[349] J.N.S. Rubí, P.R. de Lira Gondim, IoT-based platform for environment data sharing in smart cities, Int. J. Commun. Syst. 34 (2) (2021) e4515.
[350] J. Mendling, I. Weber, W.V.D. Aalst, J.V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C.D. Ciccio, M. Dumas, S. Dustdar, et al., Blockchains for business process management-challenges and opportunities, ACM Trans. Manage. Inf. Syst. (TMIS) 9 (1) (2018) 1–16.
[351] F. Yang, W. Zhou, Q. Wu, R. Long, N.N. Xiong, M. Zhou, Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism, IEEE Access 7 (2019) 118541–118555.
[352] J. Zou, B. Ye, L. Qu, Y. Wang, M.A. Orgun, L. Li, A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services, IEEE Trans. Serv. Comput. 12 (3) (2018) 429–445.
[353] S. Bouraga, A taxonomy of blockchain consensus protocols: A survey and classification framework, Expert Syst. Appl. 168 (2021) 114384.
[354] Blockchain charts, 2021, https://www.blockchain.com/charts/blocks-size (Accesses on 2021-03-25).
[355] M. Swarnkar, R.S. Bhadoria, N. Sharma, Security, privacy, trust management and performance optimization of blockchain technology, in: Applications of Blockchain in Healthcare, Springer, 2021, pp. 69–92.
[356] Y. Ma, Y. Sun, Y. Lei, N. Qin, J. Lu, A survey of blockchain technology on security, privacy, and trust in crowdsourcing services, World Wide Web 23 (1) (2020) 393–419.
[357] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, Z. Zou, A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things, J. Ind. Inf. Integr. 21 (2021) 100190.
[358] S. Zhang, J.-H. Lee, Double-spending with a Sybil attack in the Bitcoin decentralized network, IEEE Trans. Ind. Inf. 15 (10) (2019) 5715–5722.
[359] T. Hu, X. Liu, T. Chen, X. Zhang, X. Huang, W. Niu, J. Lu, K. Zhou, Y. Liu, Transaction-based classification and detection approach for Ethereum smart contract, Inf. Process. Manage. 58 (2) (2021) 102462.