Recent Trends of Integration of Blockchain Technology With the IoT by Analysing the Networking Systems: Future Research Prospects

Ahmad Anwar Zainuddin
International Islamic University Malaysia

Hariz Syahmi Hairo Rose Sidi
International Islamic University Malaysia

Muhammad Dini Aulia Shamsudin
International Islamic University Malaysia

Ahmad Jehad Esa Khaleel
International Islamic University Malaysia

Nur Athirah Mohd Abu Bakar
International Islamic University Malaysia

Nurain Sufi Sabreena Mohd Sukri
International Islamic University Malaysia

Nurul Salshabila Mustapa
International Islamic University Malaysia

Muhammad Nurzikry Mohd Sazali
International Islamic University Malaysia

In recent times, attention has surged towards entities with the potential to revolutionize various sectors. The integration of Internet of Things (IoT) and blockchain technologies, known as IoT-blockchain, offers numerous advantages, including heightened security, privacy, traceability, transparency, and reduced costs. This abstract delves into the taxonomy and prominent platforms of blockchain applications for IoT in networking systems, exploring recent advancements, obstacles, and future research avenues. IoT blockchain's crucial aspect lies in establishing decentralized networks, enabling secure collaboration and data interchange among diverse devices without a central governing entity. Platforms like Ethereum, Hyperledger, and IOTA facilitate the creation and management of these networks. Recent developments focus on enhancing security, scalability, and efficiency through novel consensus mechanisms and cryptographic techniques. Challenges persist, including the need for improved interoperability, integration with existing systems, efficient governance, regulatory structures, and the identification of use cases and business models for widespread adoption. The examination of successful governance, regulatory frameworks, and potential adoption catalysts completes the discourse on IoT blockchain technology.

Keywords: blockchain, security, Internet of Things (IoT), taxonomy, networking system

INTRODUCTION

The IoT (Internet of Things) has developed into an important part of the computing world in recent years, with the estimated value of the smart device market is billions pounds every year in the future (Farooq et al., 2023). While many companies use technology to enhance their business operations, the IoT is gaining prominence in sectors such as healthcare, among others. energy grids, cities, and finance, it confronts severe security and privacy issues. There has been increased attention from the research communities towards two significant developments. The emergence of Software Defined Networking (SDN) and Blockchain (BC) presents numerous prospects for secure and adaptable network administration, which are crucial attributes in the swiftly expanding realm of the IoT (Turner et al., 2023). A massive assault on the US internet in 2016 was traced back to the Mirai virus, which had infected a variety of IoT devices such as home routers, baby monitors, and webcams (USENIX Association, 2005). These sorts of assaults are growing more numerous and complex, emphasising the necessity for a strong response. Recently, technology will be worth billions of pounds every year, and every company will utilise it to improve its financial operations. Shrewd grids, shrewd cities, smart smarts and finance healthcare are just a few of the crucial IoT applications that face numerous security and privacy concerns as they develop. Previously, in October 2016 hackers shut down the US internet. The servers of Dyn, a business that oversees the domain name system's infrastructure, were the focus of these attacks (DNS) (Hathaway, 2021). According to Dyn, the assaults are becoming more widespread and emanate from tens of millions of IP addresses. The IoT devices used in these assaults, such as household routers and baby monitors, cameras, video recorders, too, were compromised by malicious software known as Mirai.

The combination of IoT with blockchain has created new prospects for the development of decentralised networks in which several devices may safely communicate and exchange data without the need for a centralised authority. As a result, numerous platforms and protocols, such as Ethereum, Hyperledger, and IOTA, have been developed to facilitate the establishment and control of decentralised IoT networks (Alfandi et al., 2021; Chowdhury et al., 2020; Makhdoom et al., 2019; Pustišek & Kos, 2018). Recent advances in IoT blockchain have focused on enhancing the security, scalability, and efficiency of these networks. For example, new consensus mechanisms and cryptographic techniques have been developed to improve the resilience of the network against attacks, while new data management and communication protocols have been proposed to enable efficient data sharing and processing among IoT devices.

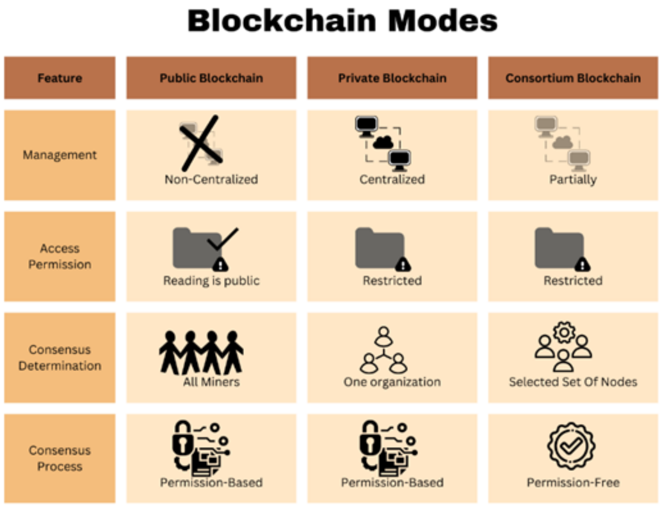
However, there are several obstacles that need to be overcome in order to fully utilise the potential of IoT block-chain. The issues encompass enhancing interoperability and interaction with pre-existing systems, establishing efficient governance and regulatory frameworks, and determining use cases and commercial models that might stimulate adoption (Anthony Jnr., 2022). In the following sections, we provide a more detailed overview of the taxonomy and key platforms for IoT block-chain, as well as go through some of the most recent developments, difficulties, and potential future research areas in this area. The literature review of IoT and Blockchain has been discussed in a previous publication (Zainuddin et al., 2023).

This paper emphasizes on the integration of IoT and blockchain in networking systems. The first section outlines the introduction of the IoT blockchain's advancement in security, scalability, and efficiency and Section 2 displays an overview of taxonomy in IoT blockchain. Section 3 contains the summary of the platforms in IoT blockchain. Section 4 explains recent advancements in IoT blockchain, Section 5 elaborates the challenges in IoT blockchain, Section 6 presents the future research of IoT blockchain and Section 7 includes the conclusion of the article.

Taxonomy in IOT Blockchain

The majority of recent survey research categorises blockchain approaches based on blockchain architecture elements and mode. Our classification is based on blockchain technologies and applications, and it is supported by literature that uses more pertinent blockchain methodologies. To date, a more thorough division of blockchain-based IoT applications. Figure 1 illustrates the categorization of various blockchain modes, protocols, technologies, and attributes that play a crucial role in delivering security and privacy solutions for IoT applications (Han et al., 2018; Pavithran et al., 2020; Wu et al., 2020).

FIGURE 1
THE CLASSIFICATION OF DIFFERENT BLOCKCHAIN FOR IOT



Blockchain Modes

Feature	Public Blockchain	Private Blockchain	Consortium Blockchain
Management	Non-Centralized	Centralized	Partially
Access Permission	Reading is public	Restricted	Restricted
Consensus Determination	All Miners	One organization	Selected Set Of Nodes
Consensus Process	Permission-Based	Permission-Based	Permission-Free

Blockchain Technology

The blockchain technology is a decentralised program that facilitates the exchange and distribution of data among participants in a peer-to-peer network (Zafar & Ben Slama, 2022). Blockchains can be classified into two main categories: totally decentralised, also known as non-permissioned blockchains, and partially decentralised, which encompass both permissioned and permissionless blockchains (Prashanth Joshi et al., 2018). In addition, the blockchain may be a consortium blockchain, a private blockchain, or a public blockchain depending on many guiding principles including access control and authentication methods.

Public Blockchain

Public blockchain is an open-source, non-permissioned network where anyone can join and engage in mining or transactional operations regardless of their entity. The greatest ability to write, read, inspect, or analyse blockchain records, including bitcoin records, belongs to any blockchain node. To obtain the required output, users can gather transaction records and launch mining activities on a public peer-to-peer

(P2P) blockchain network. Once the miner nodes, who gather data on transactions in blocks and confirm their veracity, have agreed to a consensus, the existing blockchain is updated by the result and block. In public blockchains, Proof-of-Work (PoW) is a potent solution to such issues. In this procedure, half of the mining power of the blockchain network is required if a rival wants to control the blockchain (Yadav et al., 2023). Cryptographic keys secure blockchain transactions, and the public key of each user is hashed to form their address. A node has the ability to engage in a transaction and transfer an additional node asset by affixing its signature to a hash, so validating its capacity to access information. This transaction also involves the inclusion of the public keys of the new owners (Peres et al., 2023). In order to confirm the chain of ownership, the current owner must also confirm the signature. In the context of finance and banking applications, both the Proof of Work (PoW) protocol and the public blockchain method are deemed unsuitable due to the substantial data volume and intricate processing infrastructure involved.

Private Blockchain

With the use of private blockchain technology, a company or group of people can privately exchange and disseminate a lot of data through a centralised network with rights. Due to the centralised nature of a private blockchain mining operation, wherein a specific individual or corporation assumes control, the utilisation of the blockchain by a novel or unfamiliar user necessitates a formal request to the governing authority for the addition of said user (Bhushan et al., 2020). The Hyperledger is often regarded as a prominent element within the realm of private blockchain technology. A proposal has been put up to utilise a deterministic shared consensus process in private blockchains, with the aim of ensuring stability and anonymity throughout the planning, preparation, and interaction stages (Lai & Lee Kuo Chuen, 2018). In the context of a private blockchain, the exclusive authority to append new transactions or modify pre-existing ones lies solely with the nodes responsible for network management (*Blockchains Unchained*, 2018). Private blockchains seem to be centralised because of this. Private blockchains are suited for use by banks and other financial organisations due to other characteristics including consensus and distributed ledgers.

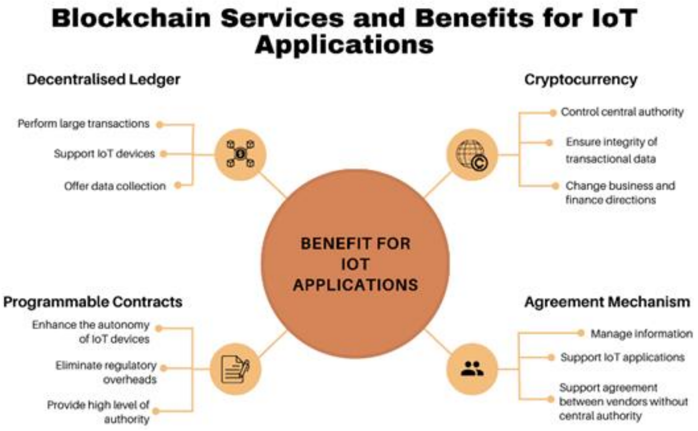
Consortium Blockchain

Private and public blockchain combines are used in the consortium blockchain strategy. A group of businesses or individuals decide on block verification and consensus. The alliance of numerous entities recognises the network and its mining nodes as existing. The network block generated using a multi-signature strategy is deemed valid if it is acknowledged and endorsed by the governing nodes. This criterion must be met for the block to be considered legitimate (Qureshi & Megías Jiménez, 2020). The consortium blockchain facilitates the validation of blocks by a collective of individuals or organizations who are its members. An instance of a framework that can be employed by a consortium utilising blockchain technology is known as Hyperledger Fabric. The Byzantines' error is in their approach to tolerance and other forms of consensus, which are employed in the process of verifying transactions on the consortium blockchain.

Blockchain Technologies and Advantages

The advantages of IoT-Blockchain encompass various elements, including distributed ledger technology, cryptocurrency integration, smart contract functionality, and consensus protocol implementation as depicted in Figure 2.

FIGURE 2
SERVICES AND BENEFITS THAT BLOCKCHAIN TECHNOLOGY OFFERS FOR IOT APPLICATIONS


Blockchain Services and Benefits for IoT Applications
Decentralised Ledger
Perform large transactions
Support IoT devices
Offer data collection
Cryptocurrency
Control central authority
Ensure integrity of transactional data
Change business and finance directions
BENEFIT FOR IOT APPLICATIONS
Programmable Contracts
Enhance the autonomy of IoT devices
Eliminate regulatory overheads
Provide high level of authority
Agreement Mechanism
Manage information
Support IoT applications
Support agreement between vendors without central authority

Decentralised or Distributed Ledger

The decentralised ledger relies on the collective agreement of numerous entities, whether locations, institutions, or sovereign entities, to operate independently and without a central controlling body. These participants provide data that is subject to processes of replication, dissemination, and synchronisation (Namasudra & Akkaya, 2023). Today, many IoT devices are capable of carrying out a variety of transactions. Advocates stress the technology's potential in the IoT context, highlighting its ability to improve linked device cybersecurity, streamline automated payments, and strengthen supply chain processes. Distributed ledger integration helps users develop trust with one another. A distributed ledger can be operated by each peer couple since they are each connected to a peer-to-peer (P2P) network and have the necessary hardware and storage capacity. The interconnection of sensors and peers is made possible by this connectivity layer. In addition, the distributed ledger stratum provides resources for thorough data aggregation.

Programmable Contracts

A programmable contract (smart contract) is a piece of executable code that functions within a blockchain architecture and is dependent on certain predetermined criteria. The execution of programable contracts is postponed until a new block combines the transactions that activate them. To eliminate nondeterminism, which can otherwise affect the output outcomes of transactions, blocks are used to group transactions. Blockchain-based contracts enable IoT devices to directly evaluate agreement conformity with contractual norms, increasing their autonomy (Tang et al., 2019). The convergence of blockchain technology and the Internet of Things (IoT) harbors the capability to enhance application performance by streamlining the processes of transaction recording, validation, and activation, all of which are orchestrated by interconnected devices. The implementation of business logic in a blockchain-based IoT system is automated through the use of smart contracts, which serves to safeguard the fundamental mechanism against potential threats such as denial-of-service attacks (Taherdoost, 2023). A programmable contract guarantees strong cooperation and retains cohesiveness when handling connections and transactions. As a result, a smart contract makes it possible for the ledger's service to incorporate the terms of the transaction's lexicon as well as calculations that determine whether those requirements have been met.

Cryptocurrency

A brand-new digital asset that was built on a network spanning numerous platforms called cryptocurrency. A cryptocurrency's decentralised architecture allows it to function independently of governmental control. The phrase "cryptocurrency" is a result of the encryption techniques applied to secure the network. Many cryptocurrencies, including the organisation's strategies to ensure transactional data transparency, employ blockchain technology as a fundamental component. Cryptocurrencies have drawn criticism for their use in criminal operations, fluctuating exchange rates, and underlying technological flaws. Blockchain, on the other hand, encourages openness, portability, tolerance for inflation, and divisibility. The course of business and finance will undoubtedly shift as a result of blockchain technology, thus its legal and regulatory implications must be taken into account.

Agreement Mechanism

The agreement mechanism (consensus protocols) utilised play a crucial role in the blockchain methodology since they are responsible for the organisation and consolidation of data on the blockchain. Most suppliers and participants must support and concur on consensus methods over a dispersed network without the requirement for a centralised authority. The most prevalent types of consensus protocols are proof-of-stake (PoS), proof-of-authority (PoA), delegated proof-of-stake (DPoS), and proof-of-work (PoW). Proof of operation is used on the Bitcoin Network. PoS focuses on forgers as opposed to miners. Depending on chance, these forgers possess enough cryptocurrency to function as a block validator. The proper block transaction fees are given to the good craftsman. A forger has the chance to try to trick the network by including a block of its own cryptocurrency because it stands to lose money if the network's transactions are applied incorrectly. The DPoS methodology functions similarly to PoS. Investors in cryptocurrencies are able to choose witnesses by voting with money given according to their stake rather than by chance. With merely votes, these witnesses can safeguard and validate the blockchain. They do not need any cryptocurrency. In contrast to the majority of PoA protocols that specify block validators, this consensus method is more centralised. Similar to the PoS system, new blocks in a blockchain can only be made if a majority of validators agree on them. Validators are in charge of figuring out who is eligible and what the state of Point of Sale validation is. In the Ethereum environment, testnet and PoA blockchains are used by Elysian, a new blockchain platform.

Byzantine fault tolerance in practice (PBFT). Regarding energy consumption and latency expenses, it is designed to exhibit greater efficiency compared to a Proof of Work (PoW) system. However, its resilience is limited to countering a maximum of 33% of malicious nodes. Practical Byzantine Fault Tolerance (PBFT) is often regarded as a resource-intensive protocol due to the significant volume of messages essential for achieving consensus. The PBFT methodology provides liveness based on dubious timing hypotheses. Operating within a framework where replicas traverse diverse configurations denominated as perspectives, it operates as a foundational backup mechanism. Istanbul Byzantine Fault Tolerance (IBFT), the inaugural consensus algorithm integrated into Quorum, has subsequently gained significant popularity as a consensus protocol suitable for establishing enterprise-grade permissioned networks that mandate both Byzantine fault tolerance and conclusive finality.

While applications employing blockchain technology and protocols exhibit robust security and privacy attributes, a myriad of challenges and complexities persist, necessitating resolution. In practice, the consensus protocol engenders substantial computational expenditure and resource consumption during real-time transactions, resulting in sluggish system throughput and protracted latency. Conversely, the blockchain framework necessitates heightened operational and platform harmonization. An imperative advancement entails the establishment of a communicative modality within the blockchain realm, one that can effectively harness the collective wisdom of distributed consensus nodes (Shackelford & Myers, 2016).

Furthermore, the essential incorporation of trusted oracles as reliable sources of factual data becomes imperative when interfacing with agreement mechanism. The evaluation of these intelligent contracts may face potential jeopardy due to the inherent volatility inherent in the IoT. Additionally, the deployment of these contracts could potentially encounter strain in scenarios involving simultaneous access to multiple data sources. Notwithstanding their present state of decentralization and distribution, smart contracts presently lack the capacity to pool resources for task distribution and the management of extensive computational workloads. The inherent variability and limitations intrinsic to the IoT must also be meticulously factored into the considerations of smart contracts. Applications should possess the capacity to effectively address IoT intricacies based on contextual cues and requisites, achieved through the symbiotic employment of agreement mechanism and discerning filtering and grouping mechanisms. The effectiveness of these applications could be further enhanced through the implementation of an on-the-fly device inclusion mechanism facilitated by a discovery process. Lastly, the integration of actuation methodologies rooted in agreement mechanism could bestow expeditious responsiveness to IoT stimuli. Nevertheless, the application of blockchain protocols to IoT domains is not devoid of challenges, potentially giving rise to a novel array of predicaments owing to the formidable computational burdens posed by IoT devices. As the quantity of interconnected devices burgeons, the dimensions of the underlying blockchain correspondingly swell, culminating in the real-time generation of substantial data volumes. Consequently, the validation of an IoT-oriented blockchain becomes a formidable endeavour. Although the prevailing cryptocurrency market boasts a plethora of extant blockchain implementations, a significant proportion of these frameworks are marred by insufficient scalability to adequately address emerging demands.

IoT-Blockchain Characteristics

IoT-Blockchain is characterised by several key features, namely decentralisation, immutability, transparency, security, and trust.

The Concept of Decentralisation

The server-client paradigm is commonly employed to delineate the integrated and intermediated communication patterns that constitute the focal point of contemporary IoT systems. Present-day IoT solutions incur considerable costs due to the substantial financial outlays associated with networking infrastructure, extensive server clusters, and centralized cloud resources (Chard et al., 2018). This is especially crucial as the IoT becomes more and more relevant to activities like human survival and wellbeing. IoT services actually lack a single authority and are decentralised. The system may either permit transactions or provide particular guidelines for their approval. There is a great deal of confidence involved because every network node wants to agree to approve transactions. The decentralised, autonomous, and trustless features of the blockchain make it a crucial part of IoT application solutions. The blockchain service would facilitate complete self-governance for intelligent devices, enabling them to exchange data and engage in financial transactions independently, circumventing the necessity for a centralized intermediary. Such autonomy is achievable due to the capability of peers within the blockchain-based network to validate transaction legitimacy without dependence on a singular authoritative entity (Wright & De Filippi, 2015). One of the most crucial features of blockchain is its capacity to keep a database of all network transactions that is suitably unauthorised and reliable. Without relying on a centralised solution to manage numerous IoT application compliance and regulatory requirements, these facilities are important.

Immutability

The characteristic of a blockchain ledger to remain unchanged is commonly referred to as immutability. The immutability of recorded transactions is ensured inside the distributed ledger architecture by encrypting the antecedent item for each subsequent block, hence perpetuating an unchanging blockchain structure. Participants are also need to consider the notion of immutability within certain aspects of blockchain, including security requirements and possible weaknesses. The utilisation of a cryptographic principle, exemplified by a hash value, is employed to encapsulate individual data blocks, which consist of groupings of information or transactional narratives. The alphanumeric hash value that corresponds to each individual block is created autonomously. Furthermore, each block comprises the hash and/or digital signature of the preceding block, so providing an unbiased and retrospective link among blocks. The inherent capacity of the blockchain prevents unauthorised access or alteration of its records. Furthermore, the distributed and decentralised aspect of the blockchain arises from the consensus that is reached across a variety of nodes that house replicas of data.

Transparency

The blockchain technology functions as a tool of openness, providing unlimited access to the network and offering extensive visibility into its intricate details. The majority of blockchains are established as open-source initiatives, indicating that the source code is readily available and can be utilised by any individual. In the context of the Internet of Things (IoT), every component has the ability to get the entire historical record of blockchain transactions, as well as participate in the process of establishing consensus on the blockchain. The utilisation of this transparency results in the creation of a record that can be audited, a workflow that is not intrusive, and, in specific situations, promotes operational efficiency. The provision of transparency greatly facilitates auditors in their efforts to verify the security of cryptocurrencies, such as Bitcoin. This construct suggests the lack of a governing body with the authority to oversee or modify the Bitcoin code. As a result, individuals have the freedom to suggest improvements or modifications to the code. The development of Bitcoin occurs when a significant number of participants in the network agree that the suggested version of the code, which incorporates enhancements, is reliable and beneficial. The protection of blockchain is supported by necessary encryption methods and rigorous enforcement protocols. All modifications are documented since details are stored. The technology can make transfers more transparent and promote system accountability since it can prove secrecy by delivering unchanging data to other parties via cryptography. Any contract's terms are unchangeable and open to everyone or qualified auditors, who can conduct inspections in ways that have never been possible before. Blockchain transparency in the context of cryptocurrencies enables users to examine the complete transaction history. Blockchain technology's transparency and accountability will be used in the future to limit unlawful internet monitoring, surveillance, and human rights abuses. For instance, if a blockchain is entirely open to the public, then all information is made public and is therefore considered to be both accessible to all users and available to prevent data misuse. The utilisation of blockchain technology will enable consumers to effectively track the movement of goods across the supply chain, determine the precise makeup of their food, evaluate its nutritional and ethical characteristics, and verify the legitimacy of their purchases, all while considering labourer rights considerations. The use of blockchain processes has the potential to enhance transparency, hence fostering an equal, accessible, and conscientious digital economy through the introduction of comprehensive transparency.

Security

The utilisation of encryption to protect on-chain "addresses" ensures the integrity and security of the consensus process, as well as the preservation of participants' identities and the accuracy of any modifications or data transfers. By incorporating information and contracts into blockchain transactions, a heightened level of security can be attained. In the given situation, blockchain technology enables the seamless integration of devices by facilitating verified transfers conducted via smart contracts. The integration of blockchain technology aims to optimise the existing conventional protocols inside the Internet of Things (IoT) domain. The security protections included in blockchain technology are significantly stronger than those used in centralised data processing, making it less vulnerable to incursion by malevolent individuals. The prevailing vulnerability within conventional networks is the susceptibility of over 50% of nodes to hacking and system breakdowns. Nevertheless, the complexities involved in manipulating data within the framework of a blockchain are significantly challenging due to the simultaneous monitoring of the data-carrying machines, including mobile devices. To change data inside a blockchain, an individual with malicious intent would need to modify each individual piece of information that is stored across the various devices involved in the blockchain network. As a result, the security of blockchain technology is strengthened through the distribution of data throughout a network of interconnected machines. To maintain the integrity of the ledger, a hashing process is utilised to produce a consecutive chain of data blocks that encompass the complete transaction history.

Trust

Following the confirmation of a transaction, the blockchain service initiates the implementation of smart contracts and safeguards a duplicate of the ledger entry, all of which occur without the participation of a single centralised entity. The effectiveness of this orchestration relies on the trustless characteristic of the system, wherein members within the corporate blockchain network derive confidence in the accuracy of transactional records through unhindered access to relevant information and operating guidelines.

Currently, the range of entries and transactions documented in the blockchain ledger is extensive, surpassing the limitations of centralised authority. As a result, entities and collaborators involved in transactions can create a reliable and effective business environment. In the realm of the IoT, devices can engage in collaborative transactions that are supported by the blockchain technology. The creation of a permanent and unalterable database of transactions and information on the blockchain, based on devices securely verifying their own identities, provides the necessary confidence for smooth interactions between enterprises and individuals. Devices equipped with identities regulated by blockchain technology have the potential to foster a perception of authenticity and establish a historical context. The blockchain technology serves as a medium through which related entities can establish and demonstrate mutual confidence in the information that is exchanged and distributed. The inherent transparent event record present in the blockchain ensures the accuracy of lineage, enforces protocols for data access, and facilitates the execution of autonomous activities through the use of smart contracts. The utilisation of blockchain technology enables the self-verification of data integrity and immutability, hence eliminating the necessity for a trustworthy intermediary. The integration of blockchain technology into IoT systems enables the registration, organisation, storage, and sharing of data streams. This empowers businesses to collect, analyse, and track the origin of data, thereby establishing a dependable framework for end-to-end transactions in the growing IoT environment. The preservation of data integrity in the context of the IoT is equally relevant when utilising blockchain technology. The fundamental principle is endowing devices with an identity that can be verified and examined throughout their entire existence, a procedure aided by the utilisation of blockchain technology. The potential of IoT networks that prioritise protocols for user identification and reputation systems, reinforced by blockchain services, is significant. To guarantee individual control over their identities, devices have the capability to broadcast encrypted challenges and responses to other devices by utilising their corresponding public blockchain keys. Moreover, the adoption of an identity-centric paradigm results in the establishment of a chronological sequence that is diligently monitored by the unalterable ledger of the blockchain.

IoT-Blockchain Privacy and Security

Privacy

In situations when an individual is linked to a device, as shown in e-health contexts, numerous applications inside the IoT manage sensitive data. Although blockchain is often presented as the ideal solution for managing IoT identification, there are specific scenarios where anonymity may be required, similar to the anonymity sought in the context of Bitcoin. This statement remains valid in the context of intelligent vehicles that prioritise the protection of user route privacy, as well as wearables that are specifically engineered to conceal a user's identity while transmitting sensitive information. The topic of data privacy in open and transparent blockchains has been extensively examined, and various solutions have been proposed. However, addressing data privacy in the context of IoT devices poses a more complex problem that encompasses multiple stages, starting from data collection and extending to communication and application layers. The problem of guaranteeing the security of data storage and limiting access exclusively to authorised entities is a significant challenge that necessitates the incorporation of strong cryptographic algorithms. The improvements must be aligned with the resource constraints of IoT devices and the economic viability requirements they conform to. Several encryption systems are utilised to ensure the security of communications, including Datagram Transport Layer Security (DTLS), Secure Socket Layer/Transport Layer Security (SSL/TLS), and Internet Protocol Security (IPsec). In light of the inherent limitations of IoT devices, it frequently becomes imperative to implement security protocols using devices that are less restricted, such as gateways. The integration of cryptographic hardware has the potential to facilitate the prompt execution of operations and alleviate the complexities associated with secure software methods.

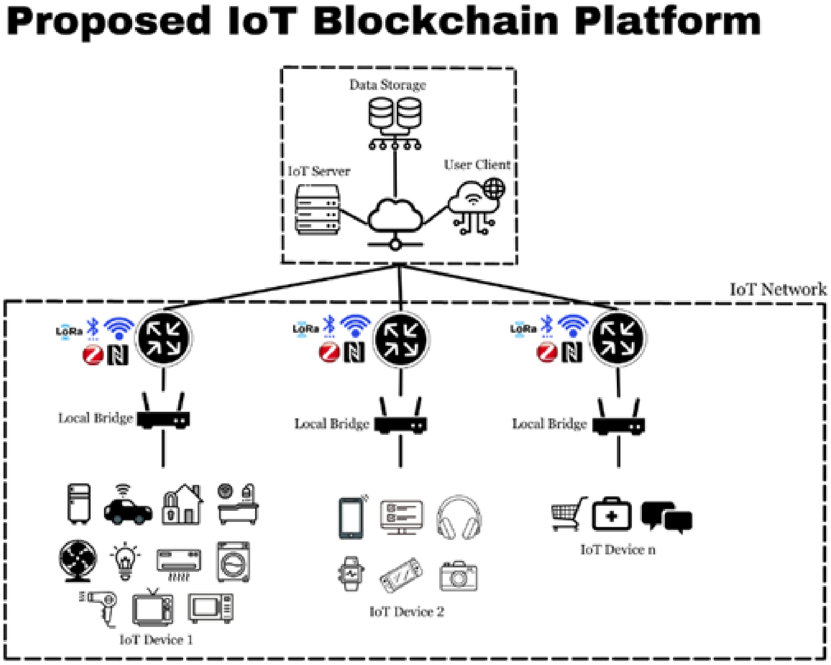
Latency

Decentralised blockchain configurations often leverage the significant latency inherent in blockchain networks to maintain consistency. Nevertheless, the significantly increased latency feature of blockchain makes it unsuitable for a wide range of IoT applications. An example worth mentioning is the case of delay sensitive IoT systems, such as automotive networks. In this context, the 10-minute block confirmation period of Bitcoin serves as an interesting illustration. The effectiveness of blockchain is significantly hindered by its inherent latency in practise. It is worth noting that the capacity of blockchain technology is insufficient to meet the requirements specified by IoT applications. For example, Bitcoin, a prominent blockchain-based cryptocurrency, only provides a capacity of 1 megabyte per every 10 minutes. The amount of IoT capacity needed is dependent on the specific application. An illustrative example can be observed in the context of a smart city IoT deployment (Khan et al., 2021). In this scenario, a fleet including 700 vehicles collectively produces a cumulative volume of vehicular trace data amounting to 4.03 gigabytes over a 24-hour period. This equates to an average of approximately 0.24 megabytes per vehicle per hour. In a comparable manner, the data collected from 55 different locations inside the parking lot is expected to accumulate to a total size of 294 KB over a period of five months. This equates to an average of only 36 B of data per point daily. The increasing number of IoT devices suggests that there will inevitably be a growing need for greater capacity in IoT applications.

Blockchain-Based IoT Applications

Figure 3 is a conceptual representation of an IoT blockchain platform. The incorporation of blockchain technology into various Internet of Things (IoT) applications has resulted in a profound and disruptive change, with far-reaching ramifications in a wide range of fields. The partnership among these organisations has resulted in significant improvements across various domains of performance, with a specific focus on vital industries including intelligent healthcare, smart grids and utilities, urban innovation, financial technology, and advanced transportation systems. The convergence of these activities represents a notable advancement in the application of blockchain technology for novel objectives. One notable area where these applications are prevalent is in the field of Smart Healthcare, which improves the quality of patient care by effectively managing data in a secure and transparent manner. Furthermore, the integration of blockchain technology by Smart Grid and Utilities aims to enhance energy management and improve the efficiency of energy distribution. Similarly, Smart City efforts utilise blockchain to optimise urban infrastructure and its associated systems. The domain of Smart Finance enables the execution of secure and efficient financial transactions, whereas Smart Transportation promotes the development of improved transportation solutions. The convergence of blockchain technology and the Internet of Things (IoT) gives rise to a novel era of potential, driving these fields towards increased effectiveness, robustness, and operational excellence.

FIGURE 3
IOT BLOCKCHAIN PLATFORM CONCEPTUAL SCENARIO



PLATFORMS IN IOT BLOCKCHAIN

This section looks at different blockchain systems that have recently emerged to fit different IoT applications.

Bitcoin Platform

Bitcoin, since its establishment in 2008, has gained acknowledgment as a form of digital currency. In the context of the Bitcoin system, transactions are recorded in a publicly available transaction ledger known as the "blockchain." This decentralised infrastructure runs through a distributed, peer-to-peer network design (Hsieh et al., 2018). The bitcoin platform relates to money and transaction processing to be done independently. The integrity of the blockchain is reliant on a computationally costly bitcoin mining process, which forbids duplicate spending and tampering with validated transactions. This "proof-of-work" method uses a great deal of energy. Numerous characteristics that are unique to Bitcoin allow for exciting uses that no other payment system could support. The majority of IoT systems utilise smart contracts, which are more popular and trustworthy and safer options in doing transactions. Bitcoin, however, uses a constrained “Script language" in order to complete the business.

Ethereum Platform

It is an “open-source” platform which is the application that allows everyone to use it. Ethereum functions as a kind of transaction-based state machine. The Ethereum blockchain's current state is altered when a legitimate transaction is carried out. A transaction is made and digitally signed by the sender. The sender confirms the transaction to an Ethereum client through a “JSON-RPC” call. The client verifies the transaction that has been sent from the sender before publishing it to the Ethereum P2P network. The confirmed transaction is then put into the pool that any miner client that receives it. This platform is also adaptable and flexible, with smart contracts that make it possible to integrate new technologies and IoT applications. It is a well-known platform that makes use of a sizable community to promote the creation of apps in a variety of programming languages, including Go, C++, and Python.

The Hyperledger Platform

The project is an “open-source”, permissioned distributed ledger that was created by the Linux Foundation. Enterprise-grade open-source technology called Hyperledger Fabric is managed by “IBM” and the “Linux Foundation”. Hyperledger Fabric does not have a cryptocurrency, and network access is only granted for the one that uses the network. Anyone may join the network. The method used by Hyperledger Fabric to create blocks and validate transactions is known as PBFT. Chaincode (smart contract), is a code which allows its user in creating and constructing applications that connect with the network, and controls the transactions in Hyperledger Fabric. Through the use of an isolation method referred to as channel, network transactions may be made private. The platform also makes sure that only the user members could access its transaction and data in a channel.

Multichain Platform

A P2P network with access limits, anonymity, and support for application development and deployment are all features of the private blockchain platform known as Multichain. The Multichain platform adds new financial transaction-related features to the current “Application Program Interface” (API) of Bitcoin's core software. Through command-line and API interfaces, the platform supports multichain configuration. Additionally, it is an authorised blockchain that delivers alternatives for its application development. Depending on the needs of the organisation, it may be an open or closed blockchain. Additionally, it is a blockchain platform that accepts Java, C++, Python, and C code. If there are worries about data removal, Multichain is a permissioned blockchain that offers an option for the IoT, but it is not safe against data theft. Additionally, it is expensive and inefficient for intelligent objects and other resources to communicate with one another within a permissioned Multichain.

Quorum Platform

Based on the Ethereum core and adapted to function as a permissioned consortium platform, Quorum is a permissioned blockchain platform. It is a significant participant in the permissioned ledger market. Quorum supports crash and Byzantine fault tolerance consensus techniques, as well as smart contract and transaction confidentiality and privacy. It allows for Turing-complete smart contracts, making it possible to create general-purpose blockchain applications for use in a variety of fields. Since it is open and permissionless, its Proof-of-Work (PoW) consensus mechanism and internal currency provide security. It supports the RAFT and IBFT Consensus algorithms (Renduchintala et al., 2022).

IOTA Platform

IOTA is a platform for the distributed ledger technology (DLT) that was created for IoT applications to overcome the latency, scalability, and transaction cost issues of Blockchain. Its key ideas behind IOTA are a ledger based on directed acyclic graphs (DAGs) called Tangle that replaces the chain of blocks and a novel validation process that depends on cooperating nodes rather than miners as in Blockchain to verify new transactions. Based on their IoT capabilities, IOTA categorise these platforms as full or lite nodes.

Machine-to-Machine (M2M) communication is the term used by IOTA to describe how it communicates between one IOT device to another IOT device. IOTA uses Tangle to get beyond the issues with double spending, scalability, and transaction costs that other cryptocurrencies, like Bitcoin, encounter. It requires the sender of a transaction to do a proof-of-work-like agreement of two transactions, the users of IOTA become miners; as a result, activities of initiating a transaction and confirming transactions are linked in IOTA. There will never be specialised miners; rather, individuals who conduct transactions have an influence on the system.

HDAC Technology

The integration of a built-in payment mechanism into the public permissioned blockchain network marks the introduction of the first-ever contract for the IoT. This technological advancement enables individuals to participate in a transactional service that facilitates the management of Machine-to-Machine (M2M) communication for IoT devices. This includes many areas such as smart vehicles, intelligent dwellings, and connected water systems. The Internet of Things (IoT) contract offers a wide range of functionalities, including device connectivity and security processing. The facilitation of this process is achieved by employing the Web Assembly language, which is a virtual machine built on an open standard. This language supports several programming languages and is compatible with the framework developed by HDAC Technology. The primary objective of HDAC Technology is to integrate blockchain technology with existing conventional platforms that are in line with the digital transformation period. This integration aims to foster a wide array of commercial initiatives. The potential for corporate growth relies on the technical expertise and ability to scale of the organisation. The aforementioned phenomenon fosters a state of peaceful cohabitation and cooperation among various entities involved in the blockchain ecosystem. Additionally, it is crucial to acknowledge that the HDAC platform is presently in the process of being developed and is scheduled to be deployed as an Internet of Things (IoT) contract specifically designed for smart home applications.

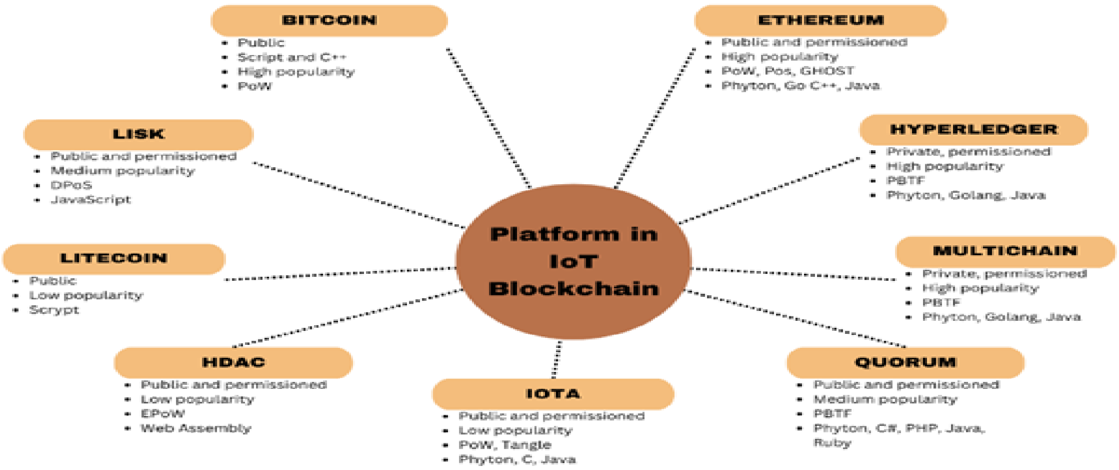
Litecoin Platform

A “peer-to-peer” Internet currency called Litecoin enables fastest, and charges almost zero penny for anyone that wants to use it. It is a totally decentralised, “open-source”, and global payment network that has no centralised control. Mathematics safeguards the network and gives users control over their own money. Compared to the top maths-based currency, Litecoin boasts faster acceptance times for transactions and more storage capability. The main objective of the creation of Litecoin, which is currently recognised as a well-known Bitcoin substitute, was to carry out lower value transactions fast. The network can support more transactions without the need for further software adjustments since blocks are created more often. As a result, while selling more expensive items, merchants may choose to wait for several conformations while still experiencing quicker confirmation times.

Lisk Platform

With the help of the well-known open-source blockchain framework Lisk, programmers may create and modify decentralised system services using JavaScript. Anyone is allowed to create and own a bespoke sidechain that may be used by the platform to create an entire application. “Lisk Commander”, “Lisk Element”, and “Lisk Core” are the three main tools that make up this platform, which it is the early progress of many more. Each Lisk node employs compressed JavaScript Object Notation (JSON) objects that contain blocks and transactions for communication. While its backend leverages NodeJS, a server-side JavaScript technology, the Lisk logic on each node uses remote procedure calls (RPC) and events to transmit transaction objects and block objects to other nodes.

FIGURE 4
PLATFORM IN IOT BLOCKCHAIN



ANALYSES OF IOT BLOCKCHAIN

This section looks at different blockchain innovations that have recently seemed to work well with various IoT applications as summarized in Table 1 (Atlam et al., 2020; Kumar & Mallick, 2018; Kwok & Koh, 2020).

TABLE 1
SEVERAL BLOCKCHAIN ADVANCEMENTS HAVE DEMONSTRATED SUCCESSFUL INTEGRATION WITH A RANGE OF IOT APPLICATIONS IN RECENT TIMES

Mode of Blockchain	Addressed Blockchain Technology	Solution Type	Proposed Solution	Supported IoT Application	Reference
Private	Distributed ledger	Architecture	To protect a private, decentralized, lightweight blockchain	IoT	[31]
	-	Scheme	To protect data transfer and sharing	IoT	
	Programmable Contracts	Algorithm	To safely outsource bilinear pairings of Internet of Things devices	IoT devices	

	-	Framework	To protect product records in diverse zones	IIoT	
	Programmable Contracts	System	Bilinear pairings-based outsourcing security	IoT devices	
	Programmable Contracts	Model	Keeping IoT data		
	Agreement mechanism	Architecture	Scalable and secure IoT resources	General IoT	
	-	Architecture	Reduce the rate of device drops.	IoT devices	
	Agreement mechanism	Mechanism	Secure information sharing of IoT based blockchain	General IoT	
	-	Scheme	Enhance client privacy, protect assets, and clients	IoT devices	
	Agreement mechanism	Model	Validate test environments and their impact on open blockchain	IoT devices	
	-	Connection protocol	Assistance with dispersed services	IoT network	[32]
	Programmable Contracts	Framework	To control immutability, authentication, and data protection.	Healthcare applications	
	Agreement mechanism	System	Bolster identity verification	IoT network	
	Agreement mechanism	Architecture	Control and keep track of patient data	Smart health	
	Programmable Contracts	Method	To control trust and monitor computation	IoT	

	-.	Model	Improved IoT data search monitoring and control	IoT network	
	Programmable Contracts	Model	Supports IoT for businesses	Smart financial	
	Programmable Contracts	System	Control and observe smart cities	Smart cities	
	-	Framework	Extrapolate IoT data	Industrial IoT	[33]
	Programmable Contracts, Distributed ledger	Framework	To oversee and manage health data	Healthcare applications	
	-	Scheme	IoT blockchain security-based management	Healthcare IoT devices	
	Local ledger	Framework	Increases the local ledger's scalability	General IoT	

FUTURE RESEARCH IN IOT BLOCKCHAIN

To prevent unauthorised access to IoT systems, it is necessary to implement access control mechanisms that are lightweight, flexible, and controlled. These mechanisms should be able to adapt to the specific characteristics (such as dynamic nature and large scale) of an IoT system. It is also important to review the feasibility of traditional access control proposals in incorporating lightweight security measures and flexibility. The IoT and blockchain technology are two rapidly evolving fields that have the potential to transform various industries. There are several areas where research and development in the intersection of these two technologies could lead to significant advancements (Khezr et al., 2019). Here are a few potential directions for future research in IoT and blockchain as depicted in Figure 6.

Scalability

One of the main challenges with current blockchain technology is that it can struggle to scale to meet the demands of large IoT networks. This is because traditional blockchain protocols are designed to handle a relatively small number of transactions per second and are not well-suited for the high volume of transactions and data generated by IoT devices. Researchers are therefore working on developing new blockchain protocols that can handle the large number of transactions and data generated by IoT devices. These new protocols may include technologies such as sharding, which allows transactions to be processed in parallel across multiple nodes, or layer 2 solutions, which move some of the transaction processing off the main blockchain.

Interoperability

Another challenge in the field of IoT and blockchain is the lack of interoperability between different IoT systems and devices. This means that devices from different manufacturers or using different protocols may not be able to communicate with each other or exchange data. Researchers are working on ways to create a decentralised and open standard for IoT devices that can be used across different systems, allowing devices from different manufacturers to work together seamlessly.

Privacy and Security

Ensuring the privacy and security of IoT devices and the data they generate is of critical importance. This is because IoT devices often collect sensitive data about their users and the environments in which they are deployed, and the data they generate may be valuable to hackers or other malicious actors. Researchers are therefore developing new technologies and protocols to secure IoT networks and protect against cyber threats. These may include technologies such as zero-knowledge proofs, which allow data to be verified without revealing the underlying data itself, or secure multi-party computation, which allows data to be processed in a way that preserves its privacy.

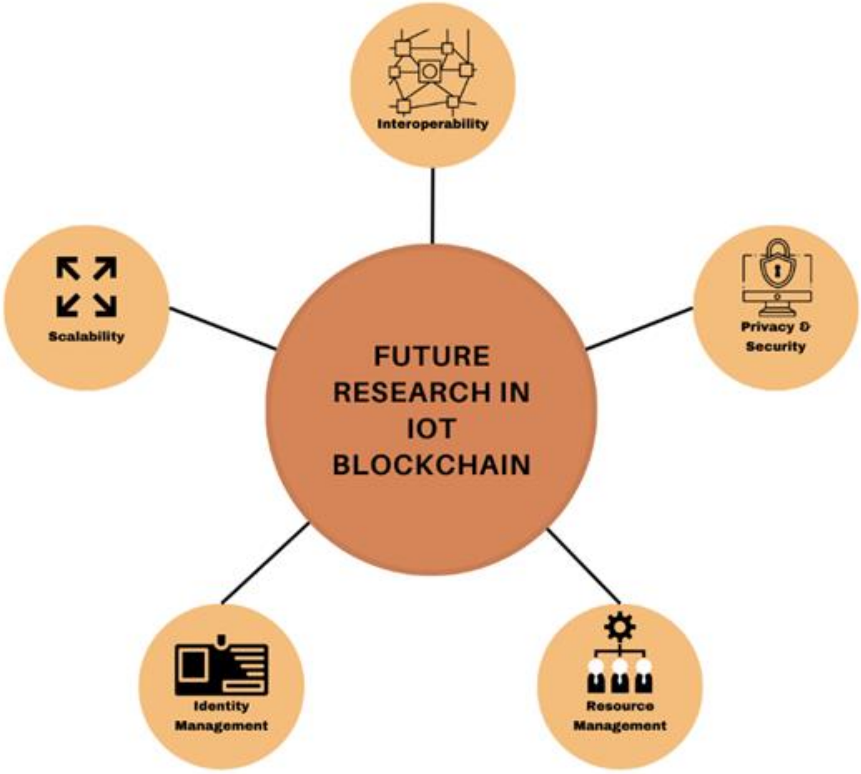
Resource Management

With the increasing number of IoT devices being deployed, there is a need to manage the resources required to operate them, including energy and bandwidth. Researchers are exploring ways to optimise resource utilisation in IoT networks using blockchain technology. This may involve using smart contracts to automatically allocate resources based on demand or using blockchain-based marketplaces to facilitate the exchange of resources between different devices.

Identity Management

Managing the identities of IoT devices and ensuring that only authorised devices can access certain resources is another important area of research. Researchers are working on developing decentralised identity management systems that use blockchain technology to secure and verify identities. These systems may use technologies such as self-sovereign identity, which allows users to control their own identity information, or decentralised identity frameworks, which allow identities to be verified by multiple parties. Overall, there are many exciting research opportunities in the intersection of IoT and blockchain. These technologies have the potential to transform industries and create new opportunities for innovation.

FIGURE 6
FUTURE RESEARCH IN IOT BLOCKCHAIN



CONCLUSIONS

The aim of this work is to encourage the integration of blockchain technology with the IoT by analysing the security systems. Cyberattacks and other security and privacy risks are more prevalent with IoT equipment. We can conclude that the most important blockchain platforms, such Ethereum and Hyperledger-Fabric, have been used for IoT applications. Additionally, we underline how blockchain technology helps IoT applications scale. Further, we investigate the most recent breakthroughs and applications in IoT. In our perspective, blockchain technology holds significant importance in the context of IoT applications. Extensive evidence substantiates the assertion that the utilization of blockchain technology yields tangible enhancements in individuals' quality of life. Prior to using blockchain technology in the context of the IoT, it is imperative to address a number of challenges and concerns that arise within this domain. This inquiry and survey are expected to contribute significantly to the resolution of many challenges encountered in the utilization of blockchain technology.

ACKNOWLEDGEMENT

We would like to extend our heartfelt appreciation to our esteemed professors and educators for their steadfast dedication and diligent efforts in imparting invaluable knowledge to us. Their commitment has greatly contributed to our advancement in enhancing our skills and comprehension in the field of Computer Networking, IoT security, and Blockchain technology.

REFERENCES

Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2021). A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. *Cluster Computing*, *24*(1), 37–55. https://doi.org/10.1007/s10586-020-03137-8

Anthony Jnr., B. (2022). Toward a collaborative governance model for distributed ledger technology adoption in organizations. *Environment Systems and Decisions*, *42*(2), 276–294. https://doi.org/10.1007/s10669-022-09852-4

Atlam, H.F., Azad, M.A., Alzahrani, A.G., & Wills, G. (2020). A Review of Blockchain in Internet of Things and AI. *Big Data and Cognitive Computing*, *4*(4), 28. https://doi.org/10.3390/bdcc4040028

Berryhill, J., Bourgery, T., & Hanson, A. (2018). Blockchains unchained. OECD Working Papers on Public Governance. https://doi.org/10.1787/3c32c429-en

Bhushan, B., Khamparia, A., Sagayam, K.M., Sharma, S.K., Ahad, M.A., & Debnath, N.C. (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*, *61*, 102360. https://doi.org/10.1016/j.scs.2020.102360

Chard, K., Dart, E., Foster, I., Shifflett, D., Tuecke, S., & Williams, J. (2018). The Modern Research Data Portal: A design pattern for networked, data-intensive science. *PeerJ Computer Science*, *4*, e144. https://doi.org/10.7717/peerj-cs.144

Chowdhury, M.J.M., Ferdous, M. S., Biswas, K., Chowdhury, N., & Muthukkumarasamy, V. (2020). A survey on blockchain-based platforms for IoT use-cases. *The Knowledge Engineering Review*, *35*, e19. https://doi.org/10.1017/S0269888920000284

Farooq, M. S., Riaz, S., Tehseen, R., Farooq, U., & Saleem, K. (2023). Role of Internet of things in diabetes healthcare: Network infrastructure, taxonomy, challenges, and security model. *Digital Health*, *9*, 205520762311790. https://doi.org/10.1177/20552076231179056

Han, R., Gramoli, V., & Xu, X. (2018). Evaluating Blockchains for IoT. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5. https://doi.org/10.1109/NTMS.2018.8328736

Hathaway, M. (2021). Getting Beyond Norms: When Violating the Agreement Becomes Customary Practice. In P. Cornish (Ed.), *The Oxford Handbook of Cyber Security* (pp. 561–577). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.013.36

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. *Journal of Organization Design*, *7*(1), 14. https://doi.org/10.1186/s41469-018-0038-1

Joshi, A.P., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, *1*(2), 121–147. https://doi.org/10.3934/mfc.2018007

Khan, D., Jung, L.T., & Hashmani, M.A. (2021). Systematic Literature Review of Challenges in Blockchain Scalability. *Applied Sciences*, *11*(20), 9372. https://doi.org/10.3390/app11209372

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Applied Sciences*, *9*(9), 1736. https://doi.org/10.3390/app9091736

Kumar, N.M., & Mallick, P.K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*, *132*, 1815–1823. https://doi.org/10.1016/j.procs.2018.05.140

Kwok, A.O.J., & Koh, S.G.M. (2020). Neural Network Insights of Blockchain Technology in Manufacturing Improvement. *2020 IEEE 7th International Conference on Industrial Engineering and Applications (ICIEA)*, pp. 932–936. https://doi.org/10.1109/ICIEA49774.2020.9101957

Lai, R., & Lee Kuo Chuen, D. (2018). Blockchain – From Public to Private. In *Handbook of Blockchain, Digital Finance, and Inclusion* (Volume 2, pp. 145–177). Elsevier. https://doi.org/10.1016/B978-0-12-812282-2.00007-3

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, *125*, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019

Namasudra, S., & Akkaya, K. (2023). Introduction to Blockchain Technology. In S. Namasudra & K. Akkaya (Eds.), *Blockchain and its Applications in Industry 4.0* (Vol. 119, pp. 1–28). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-8730-4_1

Pavithran, D., Shaalan, K., Al-Karaki, J.N., & Gawanmeh, A. (2020). Towards building a blockchain framework for IoT. *Cluster Computing*, *23*(3), 2089–2103. https://doi.org/10.1007/s10586-020-03059-5

Peres, R., Schreier, M., Schweidel, D.A., & Sorescu, A. (2023). Blockchain meets marketing: Opportunities, threats, and avenues for future research. *International Journal of Research in Marketing*, *40*(1), 1–11. https://doi.org/10.1016/j.ijresmar.2022.08.001

Pustišek, M., & Kos, A. (2018). Approaches to Front-End IoT Application Development for the Ethereum Blockchain. *Procedia Computer Science*, *129*, 410–419. https://doi.org/10.1016/j.procs.2018.03.017

Qureshi, A., & Megías Jiménez, D. (2020). Blockchain-Based Multimedia Content Protection: Review and Open Challenges. *Applied Sciences*, *11*(1), 1. https://doi.org/10.3390/app11010001

Renduchintala, T., Alfauri, H., Yang, Z., Pietro, R.D., & Jain, R. (2022). A Survey of Blockchain Applications in the FinTech Sector. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(4), 185. https://doi.org/10.3390/joitmc8040185

Shackelford, S., & Myers, S. (2016). Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2874090

Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information*, *14*(2), 117. https://doi.org/10.3390/info14020117

Tang, B., Kang, H., Fan, J., Li, Q., & Sandhu, R. (2019). IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things. *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, pp. 83–92. https://doi.org/10.1145/3322431.3326327

Turner, S.W., Karakus, M., Guler, E., & Uludag, S. (2023). A Promising Integration of SDN and Blockchain for IoT Networks: A Survey. *IEEE Access*, *11*, 29800–29822. https://doi.org/10.1109/ACCESS.2023.3260777

USENIX Association (Ed.). (2005, December 13). *Proceedings of the Second Workshop on Real, Large Distributed Systems: December 13, 2005, San Francisco, CA, USA*.

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2580664

Wu, J., Dong, M., Ota, K., Li, J., & Yang, W. (2020). Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT. *IEEE Network*, *34*(1), 69–75. https://doi.org/10.1109/MNET.001.1900179

Yadav, A.K., Singh, K., Amin, A.H., Almutairi, L., Alsenani, T.R., & Ahmadian, A. (2023). A comparative study on consensus mechanism with security threats and future scopes: Blockchain. *Computer Communications*, *201*, 102–115. https://doi.org/10.1016/j.comcom.2023.01.018

Zafar, B., & Ben Slama, S. (2022). Energy Internet Opportunities in Distributed Peer-to-Peer Energy Trading Reveal by Blockchain for Future Smart Grid 2.0. *Sensors*, *22*(21), 8397. https://doi.org/10.3390/s22218397

Zainuddin, A.A., Omar, N.F., Zakaria, N.N., & Mbourou Camara, N.A. (2023). Privacy-Preserving Techniques for IoT Data in 6G Networks with Blockchain Integration: A Review. *International Journal on Perceptive and Cognitive Computing*, *9*(2), 80–92. https://doi.org/10.31436/ijpcc.v9i2.405