Recent Trends on Blockchain for Internet of Things based Applications: Open Issues and Future Trends

Atharva Deshmukh[1], Arumugam S S [0000-0002-0233-3832], Disha Patil[3], Amit Kumar Tyagi[4,5][0000-0003-2657-8700]

1,3Department of Computer Engineering, Terna Engineering College, Navi Mumbai, 400706, Maharashtra, India

2Institute of Computer Science and Engineering, Saveetha school of Engineering, Saveetha Institute of Medical and Technical sciences, Thandalam, Chennai-602105

4School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India.

5Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India

atharva1525@gmail.com, arumugamss.sse@saveetha.com, dishampatil@gmail.com, amitkrtyagi025@gmail.com

Abstract. Today Blockchain, a decentralized, and distributed ledger technology have started taking over almost all the applications from banking, agriculture, finance, transportation, etc. Such enhancements are possible when this technology is enabled with some other technology like the Internet of Things, cloud computing, machine learning, etc. This paper does a thorough evaluation of the literature concerning blockchain enabling IoT-based applications in diverse sectors. The goal is to look at the current state of blockchain based IoT systems and applications and to demonstrate how special qualities of this technology can transform the working methods in the industry. We analysed high-quality papers published in high-ranking scientific journals over the last years to write this paper. This work presents a comprehensive classification of IoT and Blockchain enabled applications across many sectors such as Agriculture, Business, Supply Chain, Data Management, Finance, Healthcare, IoT, and Privacy, and in the end, we have added recent trends, emerging areas, and open challenges, for future research across various sectors and industries, based on a structured, systematic review and thematic content analysis of the discovered literature. We feel that our work will be of tremendous use to both academics and practitioners because we have discovered such critical components for this technology.

Keyword. Blockchain Technology, Internet of Things, Research statements, Recent Trends, Research Analysis

1 Introduction to Blockchain and Smart Contract

Blockchain systems are defined by a number of characteristics. We'll go through crucial qualities in deployments, implementation, and attributes in the sections that follow.

- *Public Blockchain, Private Blockchain, and Permissioned Blockchain:* Strategy of ledger sharing and who is authorised to participate in a system distinguishes different sorts of Blockchains [1]. A predetermined collection of nodes validates and shares ledgers inside a private Blockchain. In order to participate be an integral part of the system, nodes must first be initiated or authenticated. The network's synchronisation is the responsibility of authorised nodes. Private Blockchain is ideally suited to closed networks with perfect integrity among all nodes. Access to approved nodes is controlled by the owner, who has the ultimate power. On the other hand, public Blockchains like Bitcoin and Ethereum enable anybody to view and update the distributed ledger, with rights to confirm the ledger's integrity through a consensus mechanism. Anyone may easily join, participate in, and exit a public Blockchain network since it is entirely open and dispersed. As a result, unknown and untrustworthy nodes are used in this system. Permissioned Blockchains combine the benefits of private and public blockchains by including a large number of participants, with the primary nodes being carefully chosen at the outset. Permissioned Blockchain is best suited for semi-closed systems including a few businesses that are frequently formed as a consortium. The degree of data openness varies, but it commonly involves consortium-defined access rules to limit access to both members and information within Blockchains. Even if the system isn't completely open, the benefits of decentralization can be realized in part.
- *Centralization and Decentralization:* In most centralised database systems, transactions are intrinsically authorised or trusted by trusted centralized intermediates who guarantee their authenticity. When central servers are used, additional expenditures are incurred, and performance becomes a key concern. Blockchain technology is a key for solving distributed transaction management challenges [2], which are carried out between peers in a peer-to-peer network. Public Blockchains operations are totally decentralized, allowing for the creation of trust in transactions between untrustworthy or previously unknown nodes. Private blockchains operate in a trusted and previously unknown environment and employ access restriction mechanisms to achieve the same goal. The owner's control over node selection determines the degree of decentralisation. This configuration resembles that of a standard distributed database system. Permissioned Blockchains, like private Blockchains, function in a trusted environment but are more decentralized. The membership status of nodes is determined by consortium policies. No single party has complete control

of the system; therefore, all nodes keep Blockchain information. Decentralization enhances all forms of Blockchains to varying degrees, reducing the single point of failure and ensuring data integrity.

- *Persistency:* Since transactions inside a Blockchain ledger span the network, every node keeps and controls its very own records, thus being referred to as permanent. As long as the majority of nodes are harmless, persistence is maintained. These characteristic yields two traits: immutability (temper resistance) and transparency. Due to their transparency and immutability, blockchains could be audited [3].
- *Validity:* Unlike some other distributed applications, blockchains do not require execution out of each node. Blocks, or transactions, are broadcasted and authenticated by other nodes in a Blockchain system. As a result, any forgery would be easily apparent. This system has three main roles: proposers who offer a value, acceptors who evaluate and select the value to use, and learners who acknowledge the selected value [4].
- *Anonymity and Identity:* Anonymity is a major characteristic of public Blockchains. The identification of a user in this system is unrelated to their real-world identity. A user may create many identities to avoid identity theft [5]. Personal information does not require the supervision of a central body. As a consequence, real-world identification cannot be identified depending on transaction data, preserving anonymity to some extent. Identification is typically required for systems that are governed and controlled by known entities in scenarios such as private and permissioned Blockchains.
- *Auditability.* Records with a timestamp and durable information may be readily verified and traced by nodes in a Blockchain network. The degree of audibility varies depending on the type of Blockchain system and how it is implemented. Private Blockchains are now the least auditable because nodes are managed by a single entity, permission Blockchains are the next most auditable because some agreements, such as encrypted data, avoid information from being fully auditable, and public Blockchains are the most auditable because nodes are truly decentralized.
- *Openness and Closedness:* Open Blockchains depend on public nodes to keep records of transactions. As a result, anyone can post a transaction and engage in the system by adhering, and the information stored in the Blockchain is open to the world. Permissioned Blockchains are semi-open since nodes must be pre-specified or authenticated before joining. They're somewhere in the middle between public and private Blockchains. The data included in a Blockchain is governed by the consortium's regulations that might determine whether the data is closed or open. Private Blockchains, like permissioned Blockchains, use regulations to regulate by means of what nodes are chosen and the extent of data transparency. They are, however, reliant on a single business or owner.

Organisation of the work: Section 2 discusses about work related to blockchain and its evolution. Then, Blockchain and IoT enabled Environments like agriculture, transportation, etc., will be discussed in section 3. Section 4 discusses about blockchain for Artificial Intelligence-based Security. Then, Section 5 discusses several open issues and future trends in detail. In the last, section 6 concludes this work in brief.

2 Related work

This section gives a detailed overview of recent suggested Blockchain trends and their numerous uses. At the moment, blockchain is one of the best choices for creating a distributed, secure, and decentralized environment for the Internet of Things systems. Some researchers [6], [7] say that a smart home model based on blockchain and smart contracts analyzed different interaction processes in the model, and demonstrated through simulated tests that the proposed model may greatly lower the daily administration expenses of IoT devices. Zhang et al. [8] to provide trustworthy and distributed access control for IoT devices, researchers developed a smart contract-based framework consisting of numerous access control contracts, one judge contract, and one register contract. Iotex18 is a decentralized IoT network powered by blockchain that prioritizes privacy. It supports numerous IoT ecosystems, including shared economy, supply chain, identity management, and smart home. [9] provides a thorough examination of current blockchain technologies for advanced metering infrastructure, intelligent grid scenarios, electric cars, electric automobiles charging unit management, distributed energy resources, energy CPS, and new industrial projects. In this paper, the comparative and taxonomy study of the newest blockchain technologies, designs, and needs for smart cities are reviewed.

Blockchain is quickly gaining traction as a critical tool for safeguarding data science methods. That is, the use of blockchain to secure data collecting, processing, administration, analytics, and sharing activities is being investigated. Data analysis is feasible straight from the edge of individual devices, according to [10]. Furthermore, blockchain-generated data is vetted, organised, and immutable. Because the data produced by blockchain is guaranteed to be accurate, it improves big data." Every year, the insurance business spends tens of millions of dollars processing claims and loses millions of dollars due to fraud. Smart contracts may be used to automate claim verification, processing, and even payments, reducing claim processing time while also reducing fraud and avoiding possible problems [11]. Researchers in [12,13] describe the blockchain in 5G and beyond 5G/6G supporting technologies such as cloud computing, edge computing, software-defined networking, network function virtualization, network slicing, device-to-device communications, spectrum management. Blockchain technology is recently also been used in vehicle data management applications to solve both security and privacy problems as well as create trust among edge nodes. The work published in [14], for example, uses consortium blockchain to offer a blockchain-based safe and distributed data management system within vehicle edge computing networks.

3 Blockchain – Internet of Things enabled Environments

Within the last two years, about 90% of the data associated in the world presently was generated. Because of a) (IoT) the Internet of Things, b) population expansion the rate of growth will intensify. Whereas the growth potential of blockchain and IoT technologies is already enormous, such a symbiotic relationship between these two disciplines throws up a plethora of other possibilities. For an instance, wireless distributed and decentralized sensor node networks, are one of the cornerstones of social development and technological advancement, despite their flaws, demonstrate how blockchain design might improve IoT by increasing its potential and mitigating its flaws. Blockchain technology and its intrinsic characteristics are primarily driving the increased interest and investments in building decentralized IoT systems.

The major goal is to enable auditable and secure data transfer in context-aware heterogeneous environments with a large number of networked smart devices [15]. Furthermore, the network's efficient management and high scalability are enabled by operating in a decentralised and autonomous manner. Blockchain interoperability enables secure as well as independent actual time payment services, that could be used to advance private and public transit, traditional commerce, and e-commerce. Including of some other programs that combine these traits, EtherAPIs, which allow the monetization of API calls, and Filecoin, which is a memory storage supplier. In long term, IoT-enabled applications can be directly linked to their cryptocurrency-associated savings accounts, enabling microtransactions in commerce for services, and Similar technology might be utilized to facilitate energy sales in the smart grid. Automated product processing is enabled via distributed networks of RFID sensors in various instances, like inventory management, transportation services, and food supply chains. The data acquired by the devices might be recorded as transactions on the blockchain in these scenarios. The introduction of IoT solutions which are blockchain based might help with a variety of issues, including centralised methods' significant expenditures of upkeep. Moreover, a secure P2P and decentralised approach could enhance the safety of wireless sensor networks and IoT, allowing more control over the Internet of Things devices and system upkeep.

Without a question, there are certain restrictions, like the storage capacity of IoT devices and a lack of computing power, due to which Blockchain adoption may be limited. The authors of [16] suggest a different method for implementing a public ledger that overcomes these problems while also improving IoT applications. More effective architectures can be found in [17], which proposes a reliable lightweight architecture that is blockchain based for IoT in many application settings. Other IoT applications exist, like IBM's ADEPT (Autonomous Decentralised P2P Telemetry) system, that employs a blockchain to create decentralised network of sensors. Filament assures that autonomous device to trade payments in a secure manner. Furthermore, the authors use blockchain-based IoT software to give each item unique identification. In a similar manner, the author of [18] suggests that the Ethereum platform be used to provide secure key administration in IoT situations.

3.1 Blockchain for Smart Agriculture

Despite the fact that blockchain technology has acquired popularity as it plays a key role in the financial departments, it also offers a wide spectrum of applications that go beyond just cryptocurrencies. Many industries, including law, healthcare, banking, real estate, and others, are poised to be transformed by technology. Agriculture, on the other hand, is a little-explored field that blockchain has the ability to profoundly revolutionize [19]. Quite significantly, it has an expanding list of problems that must be addressed immediately. Blockchain technology can help agriculture in several different ways. The following are the various steps:

3.2 Blockchain in Agriculture

Step 1: Data collection by IoT devices

By 2050, the global population is predicted to reach a count of 9.6 billion people. As a result, the farming sector is implementing IoT devices and sensors to feed the ever increasing population.

Through the IoT enabled smart agriculture:

- A sensor-based system is being developed to constantly check on the crop field (light, temperature, soil moisture, pH, humidity).
- IoT devices and sensors create data which can assist farmers in making well-calculated and informed crop-growth decisions.
- Before being saved on a data storage device, the data collected from IoT devices must be organized and structured.

Step 2: Enrichment and Cleaning of the gathered data

It is necessary to organize and comprehend the collected data before storing it on the blockchain. Data enrichment takes place to increase the quality of the acquired data by adding additional value to it. Before the data is stored on the decentralized storage platform, the following two procedures guarantee that it is cleaned:

- Addition of Meta Data

Information about the aforementioned must be incorporated to efficiently organize data: demography, type, timestamp.

- Preparing data for compliance
  - Compliance enforcement is more seamless when information is stored on the blockchain.
  - Compliance guarantees, personally identifiable data connected with data acquired and gathered from IoT devices are secured and adhere to security protocols.

After the data has been enriched, it is progressively converted into a machine-learnable format.

Step 3: Using machine learning techniques to make data more insightful

To deliver meaningful insights, ML is conducted on the data collected by the sensors. Several high-value use-cases may be driven by predictive modeling, including

- Recommendations for Crop Quality
- Crop Identification
- GrowScore (Automated crop growth factor)
- Prediction of Crop Yield
- Prediction of Crop Demand

With the information acquired using ML algorithms, farmers would be in a position to update the irrigation system regularly. Producers, merchants, Growers, service providers, and inventors in the agriculture sector should be able to access the significant insightful data transparently by storing it on the blockchain [20].

Step 4: Data gets saved on the blockchain

IPFS (Interplanetary File System), a distributed shared storage platform with addresses encrypted and recorded on blockchain technology, is being used to store high-value data obtained through machine learning. The possibility of a single point of failure exists with the current practice of storing vital information inside a centralized server. The data in a blockchain, on the other hand, is disseminated among all nodes in a network. As a result, it prohibits the system from being controlled by a central authority. Smart contracts will be triggered by the information collected in the blockchain to execute out the rules stated inside them. Smart contracts make it easier to share data stored on the blockchain with the system's many stakeholders. Because all participants in the agriculture market would have access to the same information, increasing crop or food efficiency will be smooth.

3.2.1Blockchain for weather prediction and agricultural insurance

If a farmer successfully applies for crop insurance while also utilizing blockchain technology to monitor meteorological conditions, an insurance firm may leverage smart contracts to request the relevant information from the blockchain. Farmers will instantly get reimbursement on their wallets if their claim is granted. Etherisc, a German corporation, for example, operates in this manner. The company offers blockchain-based decentralized crop insurance. Farmers may first choose crop kinds and field locations, after which they will get automated payments depending on meteorological data. [21] Farmers are paid in Etherisc's own cryptocurrency, DIP (Decentralized Insurance Protocol) tokens. It makes use of local meteorological conditions, and in the event of extreme weather, insurance policies are immediately triggered using incoming data, leading to fair, prompt, and transparent payouts that insurers cannot alter.

3.2.2Blockchain for Smart Grid

The smart grid has been projected as a solution to address future power supply concerns with the incorporation of the Internet of Things and Wireless Sensor Networks. However, problems of security and privacy in the use and trade of power data represent substantial obstacles to smart grid implementation. To solve these issues, blockchain technology is now being explored for use in smart grids. The vast expansion of renewable power integrating distributed generation, humongous Internet of Things (IoT) device adoption, rising cyber-physical concerns related to security, and the primary aim of system stability and dependability [22]. These difficulties put a lot of emphasis on developing innovative technology and long-term solutions to ensure the electrical system's security and reliability.

Blockchain's recent development in technologies has attracted a lot of interest in a variety of applications, including smart grids, due to its decentralized nature and uniqueness. The following are the different components of the smart grid where blockchain applications may be explored [23]:

- Power generation: Blockchain technology offers to dispatch agencies real-time information on the overall functioning state of a power grid. This allows them to devise profit-maximizing dispatching strategies.
- Power Transmission and Distribution: Blockchain services empower automation and encourage control centers to implement decentralised systems, which eliminate the primary problems of traditional centralised systems.
- Power Consumptions: Comparable to the transmission and generation sides, blockchain might help manage energy trade between prosumers and various energy storage technologies, along with electric automobiles.

3.2.3Blockchain for Cyber Layer in Smart Grid

It demonstrates that every smart grid application, such as cyber-physical security and energy trading, might have its own specified blockchain. The different energy dealers in the grid, like consumers, prosumers, and power plants, will be integrated into the energy trading blockchain. The charging procedures between multiple stations and prosumers are made easier by the blockchain for electric automobiles. Microgrid blockchain is in charge of the microgrid's control and operations, along with the different distributed generations. Ultimately, cyber-physical security's integration into blockchain technology will be in charge of managing data protection and smart grid security challenges. The smart grid's functioning will be strengthened and smoothed thanks to the integration of these different blockchains [24].

3.2.4Microgrid architecture based on agents or aggregators

Within the electrical power system, the entire available computing capacity is boosted when all peers that engage inside the network devote a share of their computational capability. Different microgrid components, such as wind energy aggregators energy storage aggregators, and smart metering aggregators, potentially have their own blockchains. These various chains will enable a more dependable, flexible, and controlled framework and secure operating for microgrids. Furthermore, it strengthens the bond of trust between utilities and microgrid owners. Furthermore, the Blockchain improves the electrical power system's scalability; hence, adding another client inside the microgrid would result in a minor increase when it comes to complexity.

3.2.5Smart Grid Protection and Security

The electrical power system will benefit from greater security provided by a blockchain. The immutability of the data on the Blockchain is ensured by the cryptographic securitization used in conjunction with the consensus process. If the addition of an energy transaction/data is been done inside the blockchain, it will be difficult to delete or change the transaction for malicious intentions, leading to a very resilient and secure system. The Blockchain also improves the electrical power system's resiliency. In comparison to centralized data systems, there is no single point of failure because every peer inside the network has a copy of the ledger, reducing the vulnerability to malicious activities and making the overall electrical power system more durable [25].

3.3 Blockchain for Smart Home and other Appliances

Several smart home companies have recognized that Blockchain could be the future aspect of smart homes because of data tampering issues. Blockchain technology is considered to have the ability to provide a solution to IoT security concerns. Because Blockchain gives a much more flexible and dynamic variety of automated profiles, nobody needs to be concerned about data hacking or data breach The data from smart appliances may now be saved on the blockchain thanks to this approach. Each gadget will be assigned a unique identification, also the user will be provided a private key that can be accessed via their cellphones. Users may save preset configurations and access them securely through a blockchain ledger using that private key.

As a result, incorporating blockchain into an IoT system would enable considerably more secured and sophisticated used cases with respect to the automation industry. Blockchain technology is being used to track and cut energy usage. Despite higher costs owing to the usage of low-resource IoT devices, blockchain delivers better privacy and security in the smart home, and the advantages are regarded as beneficial. Digital signatures may be applied to detect fraudulent activities while also establishing a unique identity for each smart home device. Renewable energy trading platforms are being created and implemented in the microgrid as the need for renewable energy grows. Microgrid has offered several applications and creative solutions for effective system management, owing to the proliferation of technologies like Smart homes enabled by the Internet of Things, linked networks, and Blockchain [26].

The sensor layer, storage layer, management hub layer, application layer, and firmware layer, make up an innovative IoT architecture for smart factories based on blockchain. The sensing layer comprises numerous types of sensors, whilst the application layer provides customers with various services such as failure prediction and real-time monitoring. A layer named the management hub layer incorporates a specific node known as the management hub, which is responsible for encrypting, packaging data, and parsing, uploaded to Create blocks before storing it in the blockchain database. The storage layer includes a data center that distributes encrypted, blockchain records and tamper-resistant data, and syncs at a predefined frequency. Each layer is linked together by the firmware layer, which implements technologies including distributed algorithms, data storage, and data acquisition. Based on the provided defense mechanisms associated with the designed architecture under this research, the author claims that the suggested architecture may significantly improve the Integrity, Availability, Confidentiality, and CIA requirements. The suggested architecture can also be seen as a good foundation for enhancing smart home security.

They will also add a cloud-based mechanism to the network. There will be three levels in the suggested configuration: gateway, cloud layer, and device. The device layer would be the very first layer in a smart home network, and it will comprise sensors and devices for monitoring and collecting data. The getaway layer would then act as a second year, with access to the data created from the first layer, delivering it to consumers as needed. The cloud layer will also be the third tier, establishing ID registrations for each piece of data that the getaway layer processes on the blockchain [27].

3.4 Blockchain for Smart Transportation

Blockchain for commercial and trucking transportation promises to increase the agility, innovation capability, and efficiency of supply chains by creating transaction and document transparency throughout the freight environment. Blockchain provides security characteristics that distinguish it from typical logistics IT solutions. As a result, blockchain offers a lot of potentials to address a lot of problems in the transportation and freight industries. Supply chains benefit from blockchain because it allows for more cost-effective delivery and quicker. It also facilitates vendor communication, product traceability and, most significantly, facilitates access to financial resources. Blockchain eliminates the requirement for intermediaries in payment processes because of its decentralized nature. In contrast with the traditional financial institutions, blockchain enables speedier transactions by allowing P2P cross-border digital money transfers. After a successful smart contract settlement and exchange of products, the data is uploaded to a private or public blockchain, along with algorithmic signatures that are impossible or extremely difficult to modify [28, 29]. Data on supply chain transactions, as well as timestamps and information about authors, is saved. This information can be tracked by anybody with access to the blockchain, and it can even be exchanged with the consumers to promote end-user integrity and transparency.

Blockchain may be used in conjunction with IoT monitoring technologies to collect reliable data associated with each step of the transportation process. When a consumer gets damaged products, for example, it can be identified where and when the damage occurred. The IoT technology may gather information from the vehicle's sensors, and blockchain monitoring can reveal who is handling the merchandise at any particular time. Pharmaceutical goods and Food may also be tracked for quality and safety utilizing environmental sensors and blockchain. For delivery or pickup, blockchain can incorporate regulations that require the verification of original government-authorized photo identity documents. The supply chain's integrity is protected by blockchains since the records could only be authenticated with the agreement of all parties. By capturing data regarding deliveries and pickups, blockchain can assist in tracking the performance history of particular carriers. This information aids logistics businesses in making better selections when onboarding carriers, resulting in a more efficient supply chain. Smart algorithms are used to improve freight routes while minimizing delivery costs when IoT data is integrated with external data sources such as traffic or weather. [30] The usage of RFID tags isn't a new trend in the supply chain; they've been around for a while. Companies may use blockchain to combine sensors with RFID tags to assure product quality by keeping a complete record of provenance.

3.5 Blockchain for finance and banking

Blockchain technology is ready to deliver significant changes to the financial and banking industries. The financial and banking industry is now confronting a number of issues [31]. Blockchain has the ability to address these challenges by increasing security and lowering overall costs. The following are some of the challenges that blockchain as a technology can overcome:

- Transaction speed is slow.
- The Threat of Hacking and Fraud
- Expensive Know-Your-Customer (KYC) Process
- Reliance on Third-Party Intermediaries.

Decentralized technology, with its immutable ledger technology, great transparency, and high-speed payments, can help the present system in a variety of ways. Banks might benefit from significant cost reductions and operational efficiency as a result of such deployment. Aside from the delays, conventional KYC processes have duplication of efforts and significant costs. The attributes of blockchain technology can easily address the problems. By storing KYC documentation on a blockchain, you may cut down on time and money spent in this entire process. Other banks could utilise the KYC statements recorded on the blockchain to avoid having to ask consumers to go through the KYC procedure again [32].

The following are the stages the blockchain takes to execute and store a transaction:

- Whenever a new transaction is entered into the blockchain, peers from multiple systems in different geographic areas begin verifying the authenticity of the transaction.
- The data is transferred to a block when it has been successfully verified. A block is a unit of limited storage that groups together several transactions.
- When a block's space is occupied, the data is saved in the successive block. Then, several blocks are joined together to form a 'blockchain.' The joining of blocks will result in a long, permanent ledger.
- Your transaction will be completed after the transaction has been successfully coupled onto the blockchain. You can go back in time with your transactional data whenever you choose.

Banks, on the other hand, eliminate single points of failure using blockchain's distributed network. Each transaction inside a blockchain ledger is subjected to a complex series of encryptions that are interconnected with respect to the next. As a result, an unchangeable sequence of encrypted data "blocks" is created, each of which is reliant on the others in the ledger's sequence. In today's IT ecosystem, it offers one of the finest security protections against fraud and hacking. Loan operations are safer, traceable, and faster with blockchain, lowering administrative expenses, data duplication, third-party approvals, and the risk of human mistakes.

3.6 Blockchain for Smart Logistics

In the domain of Supply Chain Management, a [33] article provides a smart logistics system encompassing smart contracts, logistics planners, and asset condition monitoring. A prototype of the system is developed, demonstrating responsibility, traceability, and liability for asset management by various stakeholders participating in a logistical scenario across the supply chain. [34] A Hyperledger Sawtooth based architecture for Smart Logistics and Supply Chain is described by researchers. Two Smart Logistics system configurations are used in the performance evaluation tests. When concurrent transactions are submitted to several nodes, the system's performance suffers. The goal of blockchain technology is to increase supply chain accountability and transparency while also allowing for even more flexible value chains. The solutions based on blockchain have a lot of potential to revolutionise supply chains in 3 sectors: demand, visibility, and optimization. Blockchain can be used in recognising counterfeit goods, logistics, reducing the amount of paper processed, allowing all the sellers and buyers to trade without a middleman, and facilitating origin tracing. [35, 36] Moreover, using applications that are based on blockchain in supply chain networks has been shown to protect security, which also resulted in far more robust contract management mechanisms between the fourth-party logistics (4PL) and third-party logistics (3PL) for improving tracking mechanisms, combating information asymmetry while providing traceability assurance, and better data management across supply chain which would directly improve food safety, provide improved service to the customer and enhance IP protection.

4 Blockchain for Artificial Intelligence-based Security

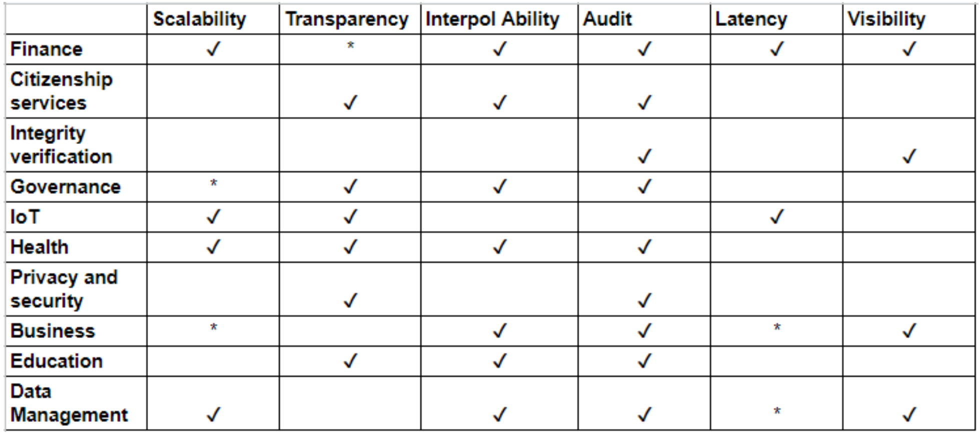
Artificial intelligence (AI) and blockchain are two important technologies that are making major changes in the corporate world. Despite the fact that each technology is extremely advanced and it has its own set of goals to achieve, combining the two has a lot of potential for decision-making solutions and creating new security. The blockchain is a decentralized database that is shared by every user inside a network and it allows transaction information to be conveniently recorded and audited without being tampered with. [37] AI, on the other hand, is concerned with developing intelligent machines which can function and respond in a variety of ways. For various Artificial Intelligence components, like algorithms, processing power, and data, blockchain can enable coordination platforms and decentralized marketplaces.

These will accelerate AI innovation and adoption at an unparalleled and unprecedented scale. AI judgments will also become more explainable, trustworthy, and visible, thanks to blockchain. Because all data on the blockchain is public, AI is essential for ensuring users' confidentiality and privacy. Thousands of parameters and tradeoffs between performance, decentralisation, security, and other factors go into the operation and creation of a blockchain. [38] Artificial intelligence (AI) can assist these decisions, as well as optimise and automate blockchain for better governance and performance. AI solves this problem with a new content selection technique to provide both tailored content and privacy. A decentralised and distributed content provider, such as a blockchain-based social network, can utilize AI to tailor content for consumers.

5 Open Issues and Future Trends

Blockchain is, without a doubt, a strong and rapidly developing technology. Decentralization, High security, and auditability are all advantages of blockchain-based systems. Despite these advantages, blockchain adoption in IoT systems faces a number of obstacles. We'll talk about these issues, as well as possible future research prospects, when it comes to integrating IIoT networks with blockchain, in this part [39].

Table 1. This table shows the parameters that make each type of blockchain application possible. The check (✓) indicates that this requirement is necessary, but the (*) indicates that it is conditional on the situation.



	Scalability	Transparency	Interpol Ability	Audit	Latency	Visibility
Finance	✓	*	✓	✓	✓	✓
Citizenship services		✓	✓	✓		
Integrity verification				✓		✓
Governance	*	✓	✓	✓		
IoT	✓	✓			✓	
Health	✓	✓	✓	✓		
Privacy and security		✓		✓		
Business	*		✓	✓	*	✓
Education		✓	✓	✓		
Data Management	✓		✓	✓	*	✓

5.1 Scalability

In both private and public blockchain networks, all consensus techniques need fully participating nodes to keep a replica of all the transaction data in a network. At the expense of scalability, it provides fault tolerance, decentralization, and security. In conventional databases, extra storage is only necessary if the number of records grows. Systems based on the blockchain, however, need more processing power to execute transactions more quickly. The scalability of blockchain has been a hot topic in academia. Now In this section, we describe some of the most notable contributions to resolving the scalability issue. We require a solution to connect IoT gateways with public blockchains, as well as inter-blockchain communication and horizontal scalability through a side chain. These models cannot be considered as a definitive answer because they can give good scalability at a restricted level. As a result, blockchain scalability is still a work in progress. Because of their networking and high performance overheads, blockchain scalability is a major barrier in the deployment of digital banking and IIoT applications. Vertical scaling of blockchain might be one possible study avenue to tackle the scalability issue. Horizontal scaling, on the other hand, maybe a more viable solution to this problem. As a result, semantically autonomous inter-blockchain communication might be a new study area.

5.2 Resource-constrained IoT devices

By connecting smart devices with the conventional internet, IoT improves network automation. The majority of IoT devices have limited resources, which makes it difficult to employ blockchain based decentralized designs. Because of their low battery life and processing power, IoT devices are unable to participate in the PoW consensus procedure. IoT devices typically lack sufficient capacity to retain a whole copy of the blockchain. As a result, combining resource-limited IoT devices with a blockchain based network may restrict the degree of decentralization. To overcome this issue, a memory optimized blockchain approach for IoT has been developed. IoT devices suffer from a lack of authentication and authorization, as well as restricted interoperability, in addition to networking and computing limits. Some Blockchains may be used to store both unstructured and structured data on the internet. As a result, blockchains has the potential to allow IoT device interoperability. In blockchain networks, researchers [40] developed roles for nodes. It also contains a restricted role for IoT devices, which eliminates the requirement for IoT devices to keep a full record of blockchain transactions. For private blockchain deployments, this technique is more viable. Although, with public blockchains, has one viable approach is to put transactions onto the blockchain via an IoT gateway. [41] In this context, computationally powerful IoT gateways that could really actively participate in the public blockchain will be required. The expansion of blockchain to the IoT edge might be another future study topic. Blockchain's networking overhead and high speed prevent it from being used on a resource constrained IoT device. IoT gateways can be utilized to transmit transactions into a blockchain network utilizing lightweight clients to address this difficulty.

5.3 The trade-off between public-private blockchains

Understanding the distinctions between private and public blockchains is essential for determining what compromises you'll have to make when building a blockchain solution. Distributed ledger technology is at the heart of both private and public blockchains. Scalability, performance, security consensus, and permissions are five main areas where they differ. Consensus is used to verify transactions on both public and private blockchains, although there are many alternative approaches to obtain consensus.

Blockchain based financial applications in IIoT networks have not yet progressed to the point where they can compete with other major financial systems like PayPal and Visa, they process roughly 2000 transactions every second while popular cryptocurrencies like Bitcoin, Ethereum, etc are just processing roughly 15 transactions per second. Although private blockchains have a faster transaction rate, they do not offer completely decentralized networks. To ensure Byzantine fault tolerance, the consensus algorithms employed in private blockchain involve a round of voting. This isn't appropriate for use on public blockchain networks. In a public blockchain, the principle is that all users are equal and there is no central authority. The public blockchain has been delayed because it uses a lottery-based consensus method to produce a permissionless and secure transaction platform. As a result, blockchain consensus algorithms force a compromise between decentralization and transaction speed. Beyond cryptocurrency, applications must provide consumers with anonymity while supporting numerous application scenarios. Different blockchains are required in applications where blockchain is dispersed over multiple geographic areas and different use cases, like IIoT. By properly connecting with one another, these blockchains may deliver a variety of IoT services.

6 Conclusion

Despite the fact that blockchain applications are adapting more widely and are used frequently, apparently, there are still a lot of challenges to overcome. As a result, blockchains would become not only more efficient and scalable but also much more durable. When taken singly, the features they give are not innovative, and the majority of the systems on which they are based are well-known, for quite a few years. The integration of each of these features, on the other hand, makes them ideal for a vast range of purposes and applications, which explains the widespread interest from a number of industries. As blockchain technology matures, several industries/domains than those identified in our survey are expected to use it.

Many people strive to encourage blockchains as a solution and database replacement, however, this isn't the reality. Conventional databases, as previously said, should be used in a range of circumstances. We also identified the most relevant individual characteristics for an individual application domain. It thus streamlines the process of selecting the right blockchain and modifying it to the application's specific needs.

7 References

1. Amit Kumar Tyagi, “Analysis of Security and Privacy Aspects of Blockchain Technologies from Smart Era’ Perspective: The Challenges and a Way Forward”, in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.
2. Sawal, Neha and Yadav, Anjali and Tyagi, Amit Kumar and Sreenath, N. and G, Rekha, Necessity of Blockchain for Building Trust in Today’s Applications: An Useful Explanation from User’s Perspective (May 15, 2019). Available at SSRN: https://ssrn.com/abstract=3388558 or http://dx.doi.org/10.2139/ssrn.3388558
3. Siddharth M. Nair, Varsha Ramesh, and Amit Kumar Tyagi, Issues and Challenges (Privacy, Security, and Trust) in Blockchain-Based Applications, Book: Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles, 2021, Pages: 14, DOI: 10.4018/978-1-7998-3295-9.ch012
4. S. Mishra and A. K. Tyagi, "Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technolgy," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 123-128, doi: 10.1109/I-SMAC47947.2019.9032557.
5. A. M. Krishna and A. K. Tyagi, "Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020, pp. 1-8, doi: 10.1109/ic-ETITE47903.2020.332.
6. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops),* 2017, pp. 618–623.
7. A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for IoT,” in *Proc. ACM 2nd Int. Conf. Internet Things Design Implement.*, 2017, pp. 173–178.

8. Y. Zhang *et al.*, “Smart contract-based access control for the Internet of Things,” *arXiv preprint arXiv:1802.04410*, 2018.
9. M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Ghias, L. H. Koh, and L. Yang, “Blockchain for future smart grid: A comprehensive survey,” *IEEE Internet of Things Journal*, 2020.
10. J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, “A survey of blockchain technology applied to smart cities: Research issues and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.
11. B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, “Blockchain for smart cities: A review of architectures, integration trends and future research directions,”*Sustainable Cities and Society*, p. 102360, 2020.
12. S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, “Securing smart cities through blockchain technology: Architecture, requirements, and challenges,” *IEEE Network*, vol. 34, no. 1, pp. 8–14, 2020.
13. E. Nagel and J. Kranz, “Smart city applications on the blockchain: Development of a multi-layer taxonomy,” in *Blockchain and Distributed Ledger Technology Use Cases*. Springer, 2020, pp. 201–226.
14. W. Zhang, Z. Wu, G. Han, Y. Feng, and L. Shu, “Ldc: A lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications,” *Future Generation Computer Systems*, 2020.
15. Crosby, Michael, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. "Blockchain technology: Beyond bitcoin." Applied Innovation 2, no. 6-10 (2016): 71.
16. Sengupta, Jayasree, Sushmita Ruj, and Sipra Das Bit. "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT." Journal of Network and Computer Applications 149 (2020): 102481.
17. Gao, Zhimin, Lei Xu, Lin Chen, Xi Zhao, Yang Lu, and Weidong Shi. "CoC: A unified distributed ledger-based supply chain management system." Journal of Computer Science and Technology 33, no. 2 (2018): 237-248.
18. Hang, Lei, and Do-Hyeun Kim. "Design and implementation of an integrated iot blockchain platform for sensing data integrity." Sensors 19, no. 10 (2019): 2228.
19. Hou, Rui, Shanshan Li, Hongyan Chen, Guowen Ren, Wei Gao, and Lijun Liu. "Coupling mechanism and development prospect of innovative ecosystem of clean energy in smart agriculture based on blockchain." Journal of Cleaner Production 319 (2021): 128466.
20. Sheshasaayee, Ananthi, and J. V. N. Lakshmi. "An insight into tree-based machine learning techniques for big data analytics using Apache Spark." In 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), pp. 1740-1743. IEEE, 2017.
21. Jha, Nishant, Deepak Prashar, Osamah Ibrahim Khalaf, Youseef Alotaibi, Abdulmajeed Alsufyani, and Saleh Alghamdi. "Blockchain Based Crop Insurance: A Decentralized Insurance System for Modernization of Indian Farmers." Sustainability 13, no. 16 (2021): 8921.
22. Mollah, Muhammad Baqer, Jun Zhao, Dusit Niyato, Kwok-Yan Lam, Xin Zhang, Amer MYM Ghias, Leong Hai Koh, and Lei Yang. "Blockchain for future smart grid: A comprehensive survey." IEEE Internet of Things Journal 8, no. 1 (2020): 18-43.
23. Khan, Fakhri Alam, Muhammad Asif, Awais Ahmad, Mafawez Alharbi, and Hanan Aljuaid. "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development." Sustainable Cities and Society 55 (2020): 102018.
24. Chen, Jian, Mohamed A. Mohamed, Udaya Dampage, Mostafa Rezaei, Saleh H. Salmen, Sami Al Obaid, and Andres Annuk. "A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks." Applied Sciences 11, no. 21 (2021): 9972.
25. Chen, Guang, Mingda He, Jianbin Gao, Chang Liu, Yuan Yin, and Qing Li. "Blockchain-based cyber security and advanced distribution in smart grid." In 2021 IEEE 4th International Conference on Electronics Technology (ICET), pp. 1077-1080. IEEE, 2021.
26. Singh, Saurabh, In-Ho Ra, Weizhi Meng, Maninder Kaur, and Gi Hwan Cho. "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology." International Journal of Distributed Sensor Networks 15, no. 4 (2019): 1550147719844159.
27. Zhou, Yiyun, Meng Han, Liyuan Liu, Yan Wang, Yi Liang, and Ling Tian. "Improving iot services in smart-home using blockchain smart contract." 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), pp. 81-87. IEEE, 2018.

28. Chattaraj, Durbadal, Basudeb Bera, Ashok Kumar Das, Sourav Saha, Pascal Lorenz, and YoungHo Park. "Block-CLAP: Blockchain-Assisted Certificateless Key Agreement Protocol for Internet of Vehicles in Smart Transportation." IEEE Transactions on Vehicular Technology 70, no. 8 (2021): 8092-8107.
29. Baig, Mirza Jabbar Aziz, M. Tariq Iqbal, Mohsin Jamil, and Jahangir Khan. "Design and implementation of an open-Source IoT and blockchain-based peer-to-peer energy trading platform using ESP32-S2, Node-Red and, MQTT protocol." Energy reports 7 (2021): 5733-5746.
30. Jangirala, Srinivas, Ashok Kumar Das, and Athanasios V. Vasilakos. "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment." IEEE Transactions on Industrial Informatics 16, no. 11 (2019): 7081-7093.
31. Singhal, Nikita, Mohit Kumar Sharma, Sandeep Singh Samant, Prajwal Goswami, and Yammanuru Abhilash Reddy. "Smart KYC using blockchain and IPFs." In Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies, pp. 77-84. Springer, Singapore, 2020.
32. Al Mamun, Abdullah, Sheikh Riad Hasan, Md Salahuddin Bhuiyan, M. Shamim Kaiser, and Mohammad Abu Yousuf. "Secure and transparent KYC for banking system using IPFS and blockchain technology." In 2020 IEEE region 10 symposium (TENSYMP), pp. 348-351. IEEE, 2020.
33. Arumugam, Senthamiz Selvi, Venkatesh Umashankar, Nanjangud C. Narendra, Ramamurthy Badrinath, Anusha Pradeep Mujumdar, Jan Holler, and Aitor Hernandez. "IOT enabled smart logistics using smart contracts." In 2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS), pp. 1-6. IEEE, 2018.
34. Perboli, Guido, Vittorio Capocasale, and Danilo Gotta. "Blockchain-based transaction management in Smart Logistics: A Sawtooth framework." In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1713-1718. IEEE, 2020.
35. Bhargava, Amitabh, Deepshikha Bhargava, P. Naveen Kumar, Guna Sekhar Sajja, and Samrat Ray. "Industrial IoT and AI implementation in vehicular logistics and supply chain management for vehicle mediated transportation systems." International Journal of System Assurance Engineering and Management (2022): 1-8.
36. Capocasale, Vittorio, Danilo Gotta, Stefano Musso, and Guido Perboli. "A Blockchain, 5G and IoT-based transaction management system for Smart Logistics: An Hyperledger framework." In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1285-1290. IEEE, 2021.
37. Soltanisehat, Leili, Reza Alizadeh, Haijing Hao, and Kim-Kwang Raymond Choo. "Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review." IEEE Transactions on Engineering Management (2020).
38. Awotunde, Joseph Bamidele, and Sanjay Misra. "Feature Extraction and Artificial Intelligence-Based Intrusion Detection Model for a Secure Internet of Things Networks." In Illumination of Artificial Intelligence in Cybersecurity and Forensics, pp. 21-44. Springer, Cham, 2022.
39. Shabnam Kumari, Amit Kumar Tyagi, Aswathy S U, “The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities and Challenges”, in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.
40. Castells-Rufas, David, Adrià Galin-Pons, and Jordi Carrabina. "The regulation of unlicensed sub-GHz bands: Are stronger restrictions required for LPWAN-based IoT success?." arXiv preprint arXiv:1812.00031 (2018).
41. Ozyilmaz, Kazim Rifat, and Arda Yurdakul. "Designing a Blockchain-based IoT with Ethereum, swarm, and LoRa: the software solution to create high availability with minimal security risks." IEEE Consumer Electronics Magazine 8, no. 2 (2019): 28-34.