IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 December 2023, accepted 29 December 2023, date of publication 8 January 2024,
date of current version 18 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3351370

SURVEY

Blockchain in the Electronics Industry for Supply Chain Management: A Survey

SHRUTI JADON, ANAGHA RAO, NETRA JAGADISH, SHRISTI NADAKATTI,
THANUSHREE R., AND PRASAD B. HONNAVALLI
Department of Computer Science and Engineering, PES University, Bengaluru 560085, India

Corresponding author: Shruti Jadon (shrutijadon@pes.edu)

ABSTRACT Supply chain as an industry has gone through four-fold changes in the last century. Born as a bare-bones structure in 1.0 it grew to incorporate some form of record preservation in 2.0 and then integrated communication between two entities in 3.0. Supply chain 4.0, the current one, has total global integration of multiple entities with the records digitised. But increasing entities and pipelines, means increasing complexities, overhead and soft spots. In this paper, a systematic literature review is done with the objective of analysing existing Supply Chain 4.0. The focus of the paper is the usage of blockchain technology in the electronic industry to provide a decentralised architecture. Several papers were compared on the basis of different schemas like the type of blockchain network used, platform deployed on, security of frameworks, representation of unique identity, testing authenticity, working implementation, cost of implementation, etc. The pros and cons of various privacy and security methodologies are also explored and discussed. The paper also discusses the open issues and challenges in the same area of interest. Finally, the paper outlines the future scope to be delved into as a part of the future research.

INDEX TERMS Supply chain, blockchain, security, smart contracts, electronic chips.

I. INTRODUCTION

A supply chain is a complex network of organisations and activities that transforms raw materials into a final product. It includes every step of the journey, like suppliers, manufacturers, distributors, retailers, and customers.

Consider a simple example of the manufacturing of a smartphone. The supply chain begins with the extraction of raw materials and ends with a purchase by the consumer. Raw materials like metals and minerals are extracted for components like batteries, screens, and casings. Different components of the phone are manufactured in specialised factories. The components are brought together in an assembly plant to create complete smartphones. The smartphones are then transported to various regions through warehouses and logistics. They are sold in retail stores or online platforms. Consumers purchase and use these smartphones for communication and other functions.

It can be seen that goods are traversed through multiple stages, people, and organisations on their way to the final consumer. As supply chains get more global and complex, it increases the potential for improvement in current supply chain management practices. Traditional supply chains are dependent on a centralised authority. Due to this, they are vulnerable to several pitfalls, including but not limited to, inaccurate demand forecasts, a lack of traceability and counterfeit products in the chain. Disruptions and delays on one side of the world can cause chaos and panic among customers on the other side of the world. For example, the panic buying and stockpiling of toilet paper that occurred during the early stages of the COVID-19 outbreak caused sudden shortages. Supply chains had to quickly adjust to the increased demand, along with disruptions due to lockdowns in different parts of the world. Execution errors, such as mistakes in inventory data, missing shipments, and duplicate payments are often impossible to detect in real-time. Due to the complex and fragmented nature of the supply chain, coordinating across the different stakeholders is difficult. The

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Yu.

detection and prevention of counterfeit products in the supply chain is also a major challenge.

These disruptions in the supply chain can create major losses for companies [1], [2], at the same time destroying the customer's trust [3]. This major problem-solution mismatch coupled with the need to stay competitive globally, mounts a clear need and the perfect time for adoption of such a technological shift as backed in the research by Agi and Jha [4]. The pandemic exposed the fragility of the global supply chain [5]. Semiconductor chip shortages that started in February 2021 continue to have an impact on decisions made by industries ranging from automotive to consumer electronics. The COVID-19 pandemic caused massive disruptions to the supply chain. The sudden switch to a digital world caused an increase in demand for semiconductor chips. This coupled with the shutdown of manufacturing facilities due to lockdowns, created a global crisis. The pandemic simply worsened the already existing issues in the supply chain - a lack of visibility into supply chain processes, and not being able to predict supply and demand scenarios in a volatile market. This chip shortage provided the perfect opportunity for counterfeiters to thrive. As companies turned to third-party marketplaces, numerous counterfeit chips came into the supply chain, fooling buyers.

Evidently, the world seeks a better way to manage global supply chains. Enterprises need to invest in modernising and digitising their supply chain ecosystems, leveraging all technologies that can help in this regard. Blockchain frameworks promise to be this savior. Blockchain technology is known for features like decentralisation, security, immutability, traceability, and reliability. This technology can potentially be leveraged in the supply chain to overcome the supply chain risks discussed earlier.

In recent years, the use of blockchain technologies in supply chain management has been explored. The scope of such research ranges from conceptual frameworks [6], algorithms [7], to implemented solutions along with results [8], [9]. However, specific attention has not been paid so far to surveying the electronics industry. Hench, there is a need to fill this gap in the literature. This survey intends to provide a summary of the current state of supply chain implementations using blockchain in the electronics industry. The purpose of this paper is to serve as a guide for upcoming scholars to begin their study on this subject and comprehend its current status.

A. SCOPE OF THE PAPER

Many surveys [10], [11], [12], [13], [14], [15], [16] have been conducted that highlight the use of blockchain in supply chain systems in a variety of industries including drugs and pharmaceuticals, health, food, agriculture, luxury goods, retail and automotive industries. Most of these surveys give insight into blockchain-based solutions in their industry, elaborating on the features and problems of each solution. A comparison of specific blockchain frameworks such as Bitcoin, Hyperledger, Ethereum etc. is provided [17]. Several works provide a comparison based on the type of blockchain used, consensus algorithm, confidentiality, type of smart contract, and performance [12], [13], [14], [18], [19]. Some existing papers analyse the opportunities and challenges for blockchain in the supply chain world [20], [21]. However, all of the surveys conclude that supply chain management would benefit from the use of blockchain technology.

The contributions of existing survey papers in this domain have been summarised in Table 1. The surveys have been marked based on whether or not they contribute in terms of architecture, schemes, challenges and issues, research questions, security, implementation discussion, and future scope. From the table, it can be observed that there is no such survey work that contributes to all these points for comparison and provides insights. Through this study, the proposed survey contributes on all of these fronts. The architecture of supply chain systems with and without the application of blockchain technology has been illustrated. Deeper schemes have been suggested to segregate and study the body of work available. Open challenges in the domain have been included. Research questions have also been included in order to understand the purpose of this paper. The work has been analysed based on the security of proposed solutions. Implemented solutions with results have been analysed as well. The future scope of this area has been discussed in order to provide a direction for researchers.

This survey intends to focus on the use of blockchain technology in the supply chain of the electronics industry. Since the focus is on the use of blockchain technology to solve supply chain problems, papers leveraging Artificial Intelligence (AI), Internet of things (IoT) and other novel technologies for supply chain improvement are not included. Similarly, papers that focus on non-blockchain technologies to improve the supply chain, such as distributed data storage and wireless networks, without making use of blockchain technology, have not been surveyed.

B. MOTIVATION

The motivation of this paper is as follows:

- The growing importance of semiconductor chips and electronics systems in today's world is one of the key criteria for exploring this area. Consumer electronics like smartphones and laptops; communication systems like routers, modems, and satellite systems; aerospace and defence systems, all require semiconductor chips. As more products become "smart", every industry is reliant on the use of semiconductor chips.
- Disruptions in the supply chain will have widespread and global effects. A blockchain-based solution can solve many of the problems with the existing system.
- The existing literature mainly discusses blockchain use in the supply chain of other industries. There is a gap when it comes to discussing solutions in the electronics industry.
- The proposed survey promotes research in the blockchain domain. It aims to provide a one-stop

TABLE 1. Overview of existing survey papers.

Paper	Year	Architecture	Schemas	Challenges and Issues	Research Questions	Security	Implementation Discussion	Future Scope
[22] Abeyratne et al.	2016	✓	✗	✓	✗	✗	✗	✓
[23] Siba et al.	2016	✗	✗	✓	✗	✗	✗	✗
[24] Saberi et al.	2018	✓	✗	✓	✗	✗	✗	✗
[25] Aich et al.	2019	✗	✗	✗	✗	✗	✗	✗
[26] Blossey et al.	2019	✗	✓	✗	✗	✗	✗	✓
[27] Reda et al.	2020	✓	✗	✗	✗	✗	✗	✗
[28] Wamba et al.	2020	✗	✗	✗	✗	✗	✗	✗
[29] Chang et al.	2020	✗	✓	✓	✓	✗	✓	✓
[20] Shakhbulatov et al.	2020	✓	✗	✓	✗	✓	✓	✓
[30] Herrgoß et al.	2020	✓	✗	✗	✓	✗	✗	✗
[21] Etemadi et al.	2021	✗	✓	✓	✓	✓	✗	✓
[11] Johny et al.	2021	✗	✓	✗	✗	✗	✗	✗
[18] Dasaklis et al.	2022	✗	✓	✓	✓	✗	✓	✗
[15] Muzafar et al.	2023	✓	✗	✗	✓	✗	✗	✓
[14] Mohammed et al.	2023	✗	✓	✓	✓	✓	✗	✓
[12] Xu et al.	2023	✓	✓	✓	✗	✗	✓	✓
[16] Yasmin et al.	2023	✗	✗	✓	✗	✗	✗	✓
Proposed paper	**2023**	✓	✓	✓	✓	✓	✓	✓

destination for anyone who requires information in this area of interest.

C. ORGANISATION OF THE PAPER

Fig. 1 depicts the survey's organisational structure. All the abbreviations used in this paper are listed in Table 2. The remainder of the paper has been structured as follows. A brief summary of the purpose and subject matter of this paper has been provided in Section I. To offer a solid foundation for understanding the rest of the paper, Section II includes fundamental information on supply chains and blockchain technology. The review approach used to create this document has been discussed in Section III. To better understand the flow, Section IV illustrates how current designs might have been created with and without the application of blockchain technology. The paper suggests deeper schemas in Section V as a way to segregate and distinguish the work completed. Section VI serves to elaborate on the open issues and challenges observed in the implementations studied. Section VII discusses the future scope of this area of research. Finally, this survey has been concluded with Section VIII, which successfully summarises the work done throughout the conducted research.

II. BACKGROUND

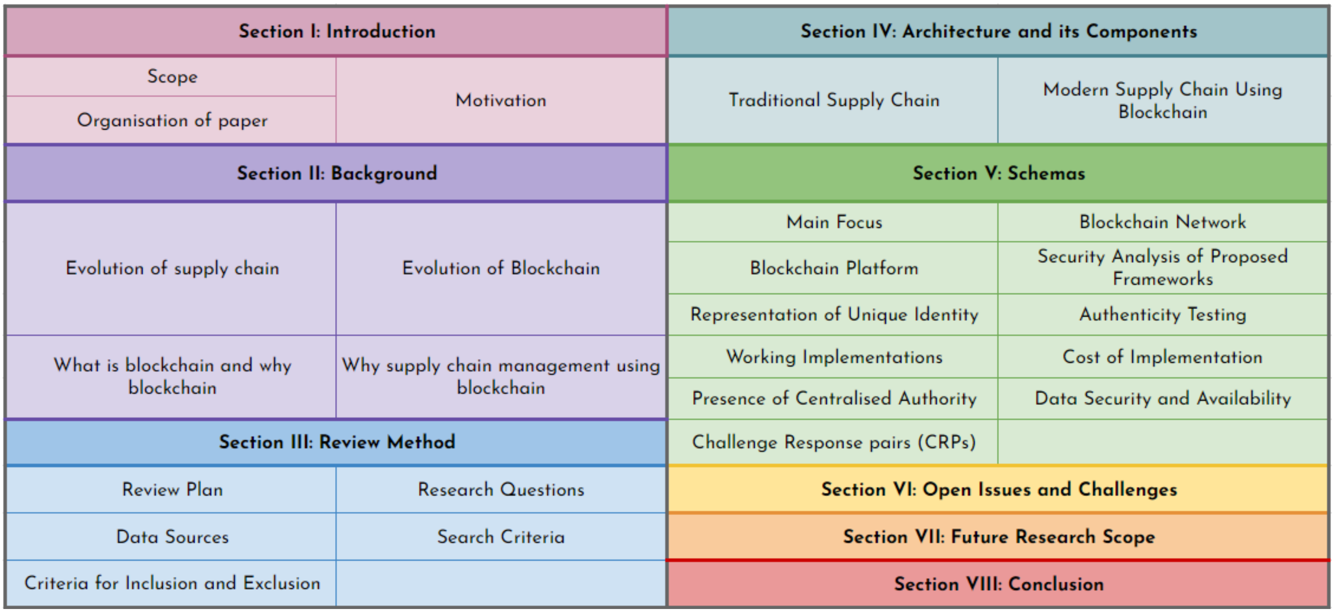
In order to achieve a better understanding of this paper, it is crucial for the reader to derive a basic understanding of supply chain systems as well as blockchain technology. The following sections cover some context so that the reader can understand the related terminology. Section II-A covers the evolution of the supply chain, and how it has transformed over the decades in response to market needs. Section II-B discusses the development of blockchain technology, which emerged as a result of the convergence of diverse ideologies. These ideologies were combined and then applied in the context of Bitcoin. To further understand how the underlying framework works, Section II-C explains the inner workings of blockchain technology. To conclude, the paper justifies why supply chain management needs blockchain technology and how it will benefit from this transition in today's world in Section II-D.

A. EVOLUTION OF SUPPLY CHAIN

The concept of supply chain management has its roots in the early eras of trade and industry when producers and merchants relied on modes of transportation including horses, carts, and ships to transfer commodities from one place to another. To further comprehend supply chain management and its tools, each of the following stages of evolution will be discussed extensively.

1) SUPPLY CHAIN 1.0 TECHNOLOGIES

Industry 1.0, also known as the First Industrial Revolution, occurred in the late 18th and early 19th centuries. It was characterised by the use of steam-powered machines and mechanisation of production [31]. During this period, supply chain management was still in the early stages and primarily involved manual processes. Push delivery process was used for the inbound as well as the outbound logistics. Products were pushed through the market, from the production side



Section I: Introduction		Section IV: Architecture and its Components	
Scope Organisation of paper	Motivation	Traditional Supply Chain	Modern Supply Chain Using Blockchain
Section II: Background		**Section V: Schemas**	
Evolution of supply chain	Evolution of Blockchain	Main Focus	Blockchain Network
		Blockchain Platform	Security Analysis of Proposed Frameworks
		Representation of Unique Identity	Authenticity Testing
What is blockchain and why blockchain	Why supply chain management using blockchain	Working Implementations	Cost of Implementation
		Presence of Centralised Authority	Data Security and Availability
Section III: Review Method		Challenge Response pairs (CRPs)	
Review Plan	Research Questions	**Section VI: Open Issues and Challenges**	
Data Sources	Search Criteria	**Section VII: Future Research Scope**	
Criteria for Inclusion and Exclusion		**Section VIII: Conclusion**	

FIGURE 1. Organisation of the paper.

TABLE 2. List of abbreviations.

Abbreviation	Full form	Abbreviation	Full form
AI	Artificial Intelligence	ECDSA	Elliptical Curve Digital Signing Algorithm
IoT	Internet of things	CDIR	Combating Die and IC Recycling
BCT	Blockchain Technology	EPC	Electronic Product Code
PoW	Proof of Work	TPRNG	Truly PseudoRandom Number Generation
PoS	Proof of Stake	TRNG	Truly Random Number Generator
PoB	Proof of Burn	PRNG	Pseudo Random Number Generator
PoET	Proof of Elapsed Time	LSFR	Linear Feedback Shift Register
PBFT	Practical Byzantine Fault Tolerance	RO	Ring-Oscillator
WSN	Wireless Sensor Networks	EPCs	Electronic Product Codes
RFID	Radio Frequency Identification	DApp	decentralised Application
RQ	Research Questions	FPGA	Field-Programmable Gate Array
CRP	Challenge Response Pairs	IDE	Integrated Development Environment
EVM	Ethereum Virtual Machine	geth	go-ethereum
BaaS	Blockchain-as-a-service	BBc-1	Beyond Blockchain One toolkit
QR code	Quick-Response code	ETH	Ether
ECID	Electronic Chip Identification Number	RL	Reinforcement Learning
IC	Integrated Circuit	USD	US Dollars
PUF	Physical Unclonable Function	OCM	Original Component Manufacturer
DLTs	Distributed Ledger Technologies	IPFS	InterPlanetary File System
zk-SNARK	Zero-Knowledge Succinct Non Interactive Argument of Knowledge	TOC	Table of Contents
IBE	Identity-based Encryption	BLIC	BLockchain protocol for IC manufacturing

up to the retailer. The level of production was decided by the manufacturer based on previous retail order trends. Push-based supply chains took longer to react to changes in demand, which led to overstocking, bottlenecks, delays, poor service standards, and outdated products [32]. Due to limited communication between the supply chain partners, the supply chain mainly focused on the movement of physical goods from one partner to another. Development of the steam-powered locomotives played a crucial role in improving communication and transportation during this period. The intralogistics or the movement of goods inside the factory was manual work with trolleys steered by humans [32].

2) SUPPLY CHAIN 2.0 TECHNOLOGIES

Industry 2.0, also known as the Second Industrial Revolution, occurred during the late 19th and early 20th centuries. It was characterised by the discovery of electricity and assembly line production. Regarding the advances in logistics, the ''automation of cargo handling'' can be found in the 1960s. Transportation modes such as railways and aircraft ships were being widely used. The mechanisation of port cargo became a significant innovation with the rise of container ships [32]. With the advent of electric power, mass production had already become a reality, as had the use of logistics tools like automatic sorting and automated warehouses. Supply chain 2.0 describes supply chains as being ''mainly paper-based'' and having little digitisation. Most processes were done manually. The digital capabilities of the organisation were very limited and available data was not leveraged to improve business decisions [33]. Supply chain management started to become global, where more than one supplier was taken into account and lasting supply relations were established [32]. Pull delivery process was used for the inbound logistics, where the goods were not produced until an order was received, i.e., materials were replenished only when they were consumed [32].

3) SUPPLY CHAIN 3.0 TECHNOLOGIES

Industry 3.0, also known as the Third Industrial Revolution, occurred during the late 20th century. It was characterised by partial automation using memory-programmable controls and computers. Since the introduction of these technologies, automation of the entire manufacturing process has become possible [31]. During Industry 3.0, the machines were controlled using software that took care of the warehouse management system and the inbound logistics. Everything was planned and automated using this system, leading to significant revenue improvements. Additionally, Supply Chain 3.0 was characterised by dynamic and flexible integration among the supply chain partners. The integration in this phase was carried out between two supply chain partners [34]. Centralised logistics and capacity planning were established to achieve market leadership, although they did experience challenges like visibility and tracking gaps present in the chain.

Another significant improvement during this time was the implementation of global transportation solutions and complete global resource planning, which led to the global expansion of several companies. IT systems were implemented and leveraged, but digital capabilities were still in the development stage. Only basic algorithms were used for planning and forecasting, and only a few data scientists were part of the organisation to improve its digital maturity [33].

With the introduction of Supply Chain 4.0, specialised, digital supply chains came into being. This has improved growth and provided opportunities for mass customisation.

4) SUPPLY CHAIN 4.0 TECHNOLOGIES

Organisations are currently leveraging tools and technologies associated with Industry 4.0, which is characterised by the application of information and communication technologies to the industry. Supply chain 4.0 has the highest maturity level, leveraging all data available for improved, faster, and more granular support of decision-making. Advanced algorithms are leveraged and a broad team of data scientists work within the organisation, following a clear development path towards digital mastery [31]. Supply Chain 4.0 is not only faster, but also more flexible to fluctuating demands and supply situations, due to which the supply chain entities are able to react dynamically to new constraints that may arise.

Supply chain management 4.0 is the integration and synchronisation of the product's entire value chain across different companies using smart technologies to build an interconnected and transparent system with real-time communication [34]. Production systems that already have computer technology are expanded by a network connection and have a digital twin on the Internet which in turn allows communication with other facilities and the output of information about themselves [34].

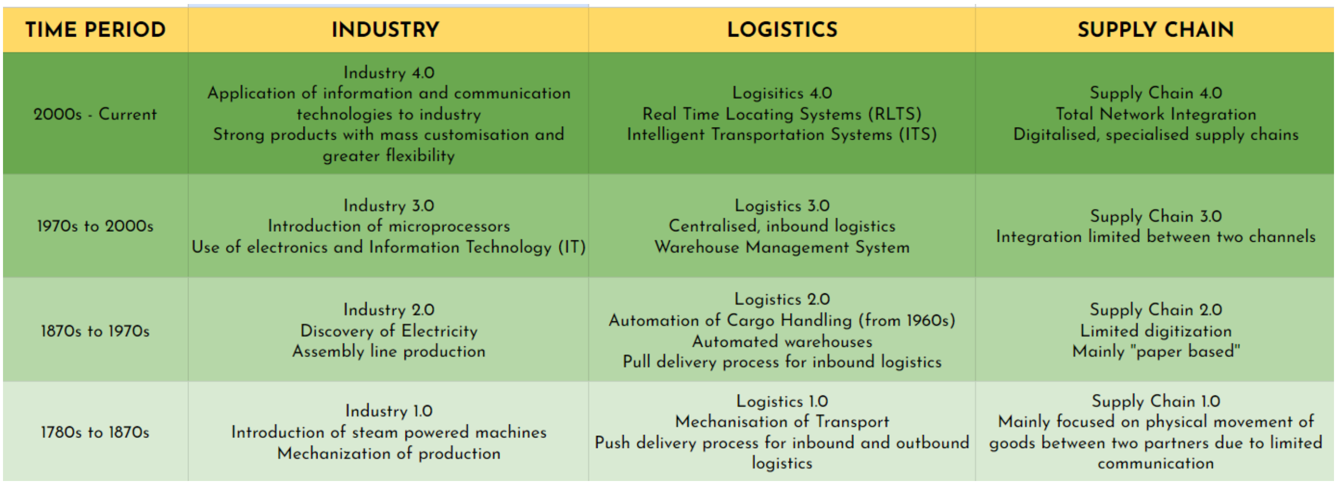
Big Data, the Internet of Things, and the Physical Internet are some of the key technologies in Supply Chain 4.0. Some of the other tools and technologies include Cloud Computing, AI, Robotics, Cyber Security, Edge Computing, and Predictive Analytics. Supply Chain 4.0 has a wide variety of use cases ranging from inventory management, demand forecasting, logistics optimisation, predictive maintenance, and automated order fulfillment. Some of the key benefits include:

- Increased visibility - Supply Chain 4.0 enables the supply chain partners to have real-time visibility of the supply chain operations, hence enabling dynamic decision-making.
- Improved decision making - Combining predictive analytics and AI enhances decision-making, making organisations more agile and responsive to market changes.
- Increased efficiency - Leveraging the current technology and level of automation, companies can reduce costs and increase the efficiency of their supply chain operations [35].

Fig. 2 clearly depicts the correlation between the evolution of the supply chain and the evolution of the industry practices and logistics. Application of information and communication technologies to the industry has enabled complete supply chain integration. The supply chains themselves have become flexible, efficient and secure.

B. EVOLUTION OF BLOCKCHAIN

Introduced by one or more individuals under the pseudonym Satoshi Nakamoto [36], the cryptocurrency Bitcoin and the underlying blockchain technology (BCT) have created a tremendous hype around electronic payment systems using the peer-to-peer paradigm of the internet. But its creation



TIME PERIOD	INDUSTRY	LOGISTICS	SUPPLY CHAIN
2000s - Current	Industry 4.0 Application of information and communication technologies to industry Strong products with mass customisation and greater flexibility	Logisitics 4.0 Real Time Locating Systems (RLTS) Intelligent Transportation Systems (ITS)	Supply Chain 4.0 Total Network Integration Digitalised, specialised supply chains
1970s to 2000s	Industry 3.0 Introduction of microprocessors Use of electronics and Information Technology (IT)	Logistics 3.0 Centralised, inbound logistics Warehouse Management System	Supply Chain 3.0 Integration limited between two channels
1870s to 1970s	Industry 2.0 Discovery of Electricity Assembly line production	Logistics 2.0 Automation of Cargo Handling (from 1960s) Automated warehouses Pull delivery process for inbound logistics	Supply Chain 2.0 Limited digitization Mainly "paper based"
1780s to 1870s	Industry 1.0 Introduction of steam powered machines Mechanization of production	Logistics 1.0 Mechanisation of Transport Push delivery process for inbound and outbound logistics	Supply Chain 1.0 Mainly focused on physical movement of goods between two partners due to limited communication

FIGURE 2. Evolution of supply chain along with the industry.

was in the making for decades. Each new advancement in cryptography and ledger technology played a part in shaping blockchain technology until it was finally developed.

The evolution can be split into pre-blockchain era and post-blockchain era, as seen in Fig. 3, with all the major milestones. It can be seen how the technologies that came into being before blockchain were introduced and conceptualised, and how blockchain grew after that. The following subsections expand on the above-mentioned eras.

1) PRE-BLOCKCHAIN ERA (1982-2008)

The core concepts behind BCT were anticipated in the late 1980s and the early 1990s. In the early 1990s, there was research going on how to maintain data ledgers. Subsequently, with their solutions and more add-ons over the years, an electronic ledger system was created. It started with the use of timestamps to create a chain of data blocks which were cryptographically secure [37]. This ledger comprised of documents with a digital signature, which made it easy to prove that these signed documents had not been altered. They also included the use of faster computable hashes instead of signing document links [38], grouping documents into blocks instead of processing them separately and inside the respective block, connecting them with a binary Merkle tree structure as a substitute for linear document linking transaction hash indicators. In 2008, the concept of the BCT was revised and proposed by Nakamoto [36] and implemented as an open-source project in 2009. Bitcoin was the first real-world application of BCT. Bitcoin is a decentralised peer-to-peer network for cryptocurrency and a well-known use case of BCT. The next section discusses the post-blockchain era and how it progressed.

2) POST-BLOCKCHAIN ERA (2008-PRESENT)

This era can be further split into four evolutions with each new evolution bringing in a significant transition into BCT's growth.

Blockchain 1.0 (2008-13): BCT emerged supporting digital ledgers where data blocks as a merkle tree were linked on a chain. Digital currencies supported its working.

Blockchain 2.0 (2013-15): Vitalik Buterin released a wildly innovative white paper [39], and created a new blockchain called "Ethereum". It enabled automated computation using smart contracts. This enabled a new era of conducting transactions on chain, that could be expanded to create decentralised applications. Hyperledger released its own blockchain platform for developers to create on. It only enabled the creation of permissionless blockchain networks.

Blockchain 3.0 (2016-2018): This era was more application-focused. Applications using blockchain were created for consumers. This era focused on IOT inclusion, reduce transaction costs, unique verification processes, address security and privacy concerns in blockchain.

Blockchain 4.0 (2018-present): As consumer-oriented applications gained popularity and received increased platform support, the feasibility and support for industry-specific applications grew. This led to the realisation of blockchain technology's potential in enterprise solutions, with industry infrastructure actively embracing and endorsing its adoption.

The next section goes into depth of technical terms and the workings of BCT.

C. WHAT IS BLOCKCHAIN & WHY BLOCKCHAIN

This section explores blockchain technology and its inner workings. A good understanding of the core fundamentals is presented. This is then used to justify and frame the properties of blockchain and why one would like to associate and implement it.

1) WHAT IS BLOCKCHAIN

The concept of blockchain is a distributed P2P network with public ledger. The records of all transactions that have been performed in the blockchain network are shared among all the participant nodes and maintained in their respective ledgers. Each transaction in the public ledger is verified by

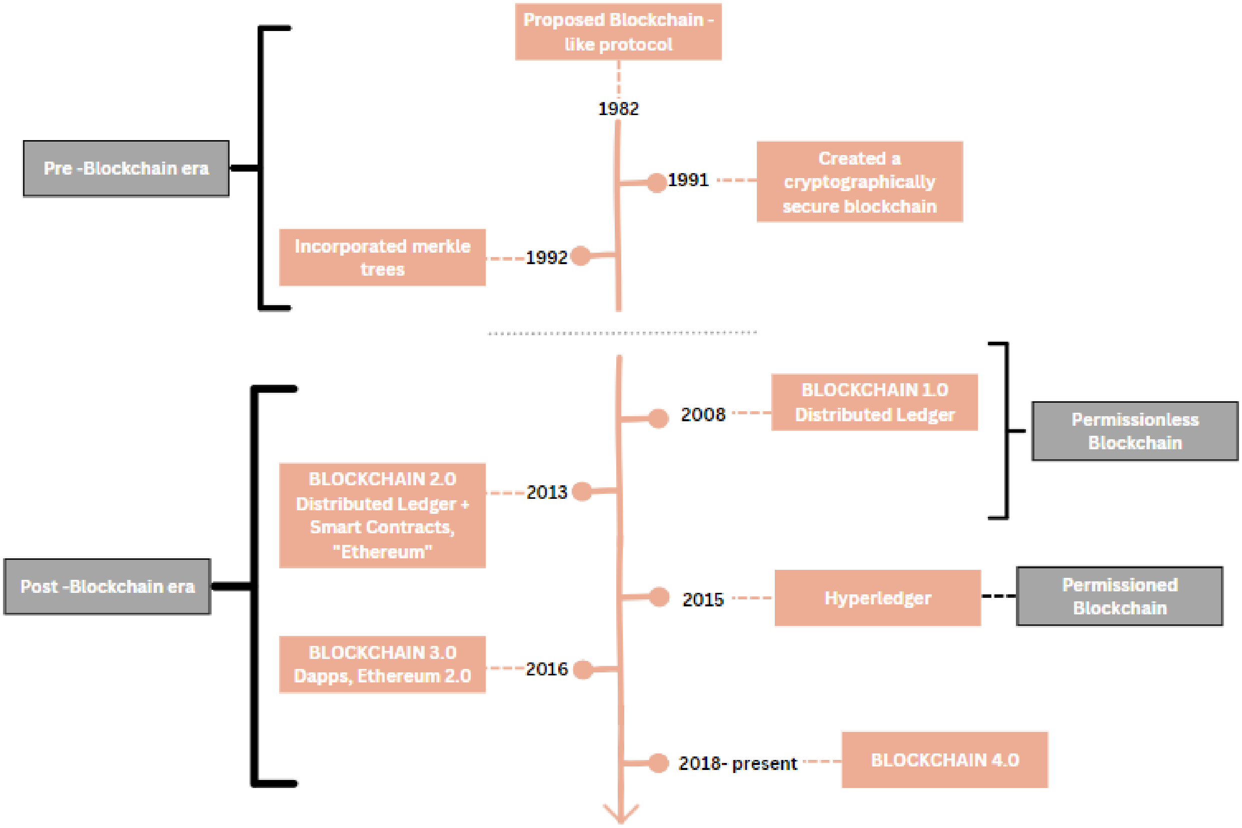

Proposed Blockchain - like protocol
1982
Pre -Blockchain era
1991
Created a cryptographically secure blockchain
Incorporated merkle trees
1992
2008
BLOCKCHAIN 1.0 Distributed Ledger
Permissionless Blockchain
BLOCKCHAIN 2.0 Distributed Ledger + Smart Contracts, "Ethereum"
2013
Post -Blockchain era
2015
Hyperledger
Permissioned Blockchain
BLOCKCHAIN 3.0 Dapps, Ethereum 2.0
2016
2018- present
BLOCKCHAIN 4.0

FIGURE 3. Timeline of blockchain development.

consensus, i.e., majority of the participants have agreed about the transactions, hence its distributed P2P nature [23].

The role of the middleman is one of the most important economic and regulatory actors in our society with a lot of trust placed on them. However, blockchain has the potential to replace or minimise this role by providing a decentralised, trustless and transparent network. It acts as a middleman in many ways- as an escrow, to deal with compute and storage, and as an unbiased piece of executable logic in the form of smart contracts, which can also enable automation [23].

The following subsections provide an overview of this technology and how the key entities are involved in enabling it.

Peers and Blocks

The blockchain network is a chained storage structure where each node (acting as a peer) has a full copy of the ledger for maintenance. Instead of a centralised institution maintaining a main ledger, each node maintains its own ledger, so that the state of the ledger can be guaranteed against forgery as long as no more than half of the nodes are malicious. An external user can communicate in the blockchain via a client node through transactions. The node also validates these transactions. Full nodes are elected by consensus algorithms which then go on to propose blocks to be added onto the longest chain.

The block structure is shown in Fig. 4. As seen in the figure, a single block consists of a block header and a block body. The verified transaction data is stored in the block body, and a unique Merkle root is generated through the hash process of this data. The block header contains a lot of data, the most significant of which are the hash value of the previous block, timestamp, difficulty and random number nonce. Due to the characteristics of the hash function, if the block content is slightly modified, its hash value will change drastically, thus making it impossible to tamper with due to the chain structure of the blockchain.

Consensus Algorithms

A consensus algorithm is a procedure to reach a common agreement in a distributed and decentralised environment. For consensus to come about, all the nodes need to agree on the correctness of the transactions. The miner node (full node) is selected through consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Proof of Burn (PoB), Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance (PBFT), etc. The elected miner node packages the verified transactions in the blockchain network into blocks and broadcasts them to all nodes, while other nodes add the newly generated block to their copy. The blockchain is decentralised by such a consensus mechanism.

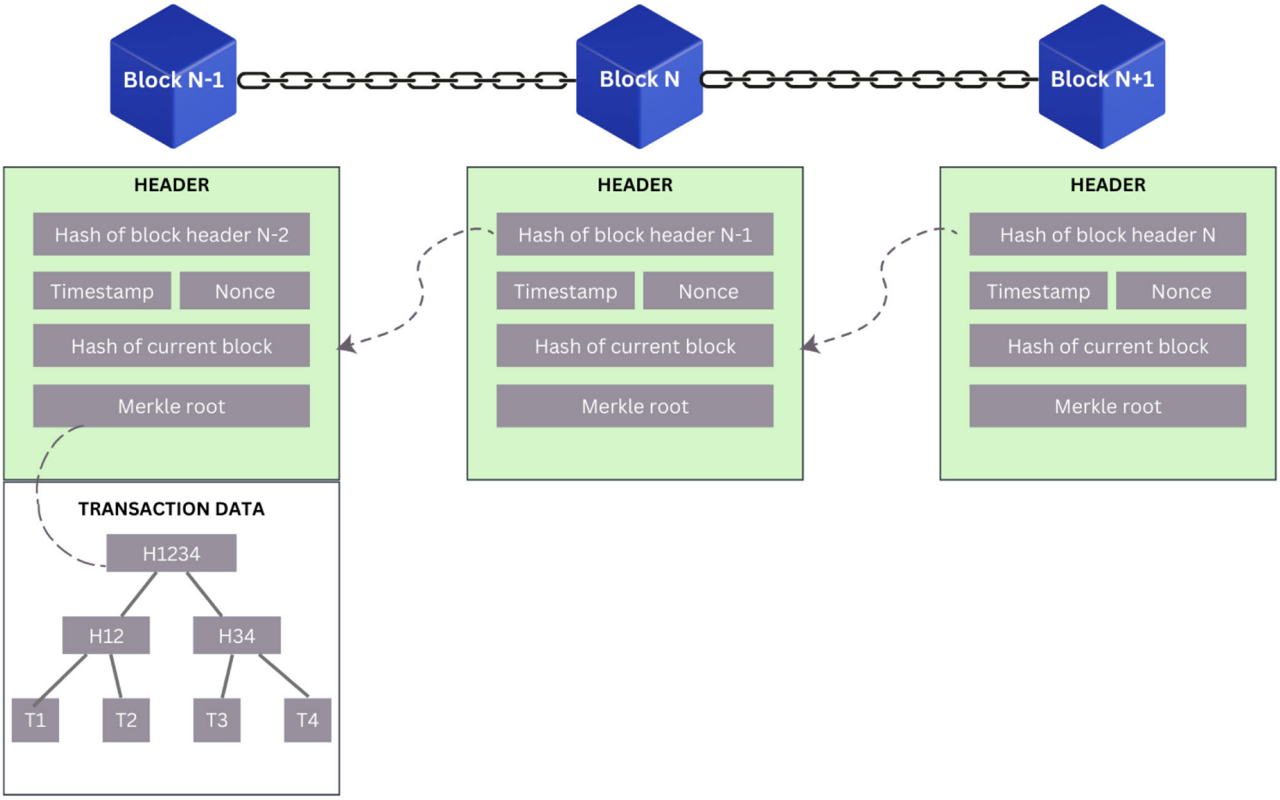


FIGURE 4. Block as chain.

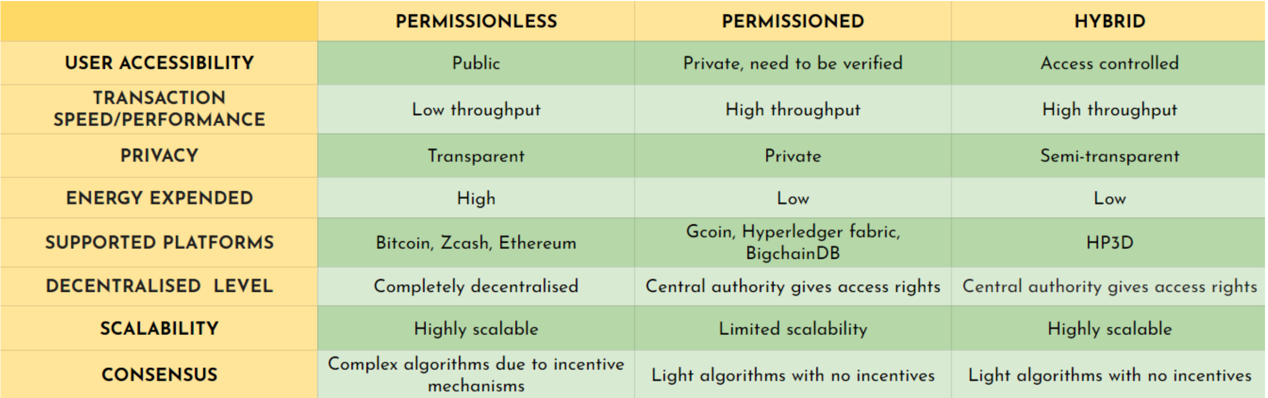
In **PoW**, nodes with higher computational power get a higher advantage as they are able to quickly solve the puzzle and win the rights to add the next block. In **PoS**, the nodes have to stake some amount to be involved in the mining process. Its energy consumption is lower than PoW, but due to bias on how much stake is put in, there is a certain level of centralisation. An alternative consensus process called **PoB** aims to solve the problem of a PoW system's excessive energy consumption. The person who burns the most coins receives greater preference instead of employing mining rigs to solve computational challenges and earning the privilege to mine a block. To burn coins, the coins are sent to a verifiably unspendable address by the miners. **PoET** can only be used under private blockchain. Developed by Intel, it requires every node to have a secure execution environment. It is a random selection mechanism wherein each participating node generates a random wait time (using the secure environment), and the node with the shortest wait time gets to create the next block. **PBFT** is also used in private networks and has reliance on a set of replica nodes called validators. All transactions are broadcasted to validators, and on receiving a supermajority (at least 2/3rd) agreement, they will be committed to the blockchain. It is powerful since it can handle 1/3rd of the nodes being malicious, but due to the validators it isn't fully decentralised.

Network types

Blockchain as such is a distributed ledger, but the means by which the nodes operate, its access controls and data flow is highly dependent on the type of network created. Due to different requirements, there are different types of networks created to cater to an application or to an organisation's need. On a broad level, there are three types of blockchain networks - public, private and hybrid networks.

In a **permissionless or public blockchain** anyone who wants to join can access the network and participate in the consensus mechanism. Participants don't have to divulge their identities while using public keys that permit pseudo-anonymous identities; they can change them at any moment. Permissionless blockchains make use of a consensus algorithm that establishes tight guidelines for accepting proposed blocks as well as a built-in incentive system that recognises and rewards honest involvement. There is a high level of transparency due to its public nature, in terms of viewing and taking part. Decentralisation is nonetheless accomplished, at the price of limited transaction throughput consuming more energy and introducing scalability problems.

Access to the network and participation in the consensus method are restricted in **permissioned or private blockchains**; users of these networks must first register



	PERMISSIONLESS	PERMISSIONED	HYBRID
USER ACCESSIBILITY	Public	Private, need to be verified	Access controlled
TRANSACTION SPEED/PERFORMANCE	Low throughput	High throughput	High throughput
PRIVACY	Transparent	Private	Semi-transparent
ENERGY EXPENDED	High	Low	Low
SUPPORTED PLATFORMS	Bitcoin, Zcash, Ethereum	Gcoin, Hyperledger fabric, BigchainDB	HP3D
DECENTRALISED LEVEL	Completely decentralised	Central authority gives access rights	Central authority gives access rights
SCALABILITY	Highly scalable	Limited scalability	Highly scalable
CONSENSUS	Complex algorithms due to incentive mechanisms	Light algorithms with no incentives	Light algorithms with no incentives

FIGURE 5. Different types of blockchain networks.

in order to access the blockchain. This gives organisations greater control, privacy and security. Byzantine fault tolerant (BFT) consensus algorithms can identify fraudulent conduct since the registered members of a permissioned blockchain are aware of the identity of the participants. Since validators are given a certain amount of confidence, permissioned blockchains do not require incentive structures to encourage honest participation. The users of these blockchains have access to data in the distributed ledger. With the sacrifice of reduced decentralisation, such qualities enable a permissioned blockchain to employ a lightweight consensus algorithm that can achieve high transaction throughput with high scalability. The cost includes a higher degree of centralisation compared to public blockchain. The central authority needs to be trusted and there are high maintenance costs involved. A consortium blockchain is a type of private network built to serve a group of organisations. There are some users of each organisation with higher access control over the data, so not every node is treated equal. It is more private and rigid with respect to data flow, transactions, and entry of new individuals. It is more efficient since there is a higher degree of control between lesser users.

The advantages of both permissioned and permissionless blockchains are combined in a **hybrid blockchain**. By definition, it combines the high throughput and data privacy of permissioned blockchains with the high degree of decentralisation of permissionless blockchains. A blockchain of this type has both a private and public ledger. It stores non-sensitive data in a public ledger that is accessible to all participants and sensitive data in a private ledger that is only accessible to a select group of specified stakeholders. Organisations can have a collective decision-making process. But this also means higher complexity in setting up and managing the same. Fig. 5 describes the stark differences between the different types of networks. As seen in the figure, hybrid networks enable the benefits of the other two networks to come through [20].

2) WHY BLOCKCHAIN

On a blockchain, all the data and its entire history are accessible to all nodes. Information and data are controlled by several nodes without the use of a central node. Without a middleman, each party may independently check the records of its transaction partners. Thanks to a distributed ledger's record-keeping, resilience can be achieved as data becomes replicated across multiple points. This data becomes immutable, making it impervious to tampering. In the event of any modifications, the changes and the responsible party can be identified through the preserved provenance, all while retaining access to the data in its original state prior to any changes. Transactions on the chain can be linked to computer logic and, in a sense, programmed because the ledger is digital. Users can then configure algorithms and rules that initiate transactions between nodes automatically [40]. Traceability or provenance can enhance the traceability of the supply chain. A wallet address is a 30-plus-character alphanumeric address that uniquely identifies each node, or user, on a blockchain but does not publicly. In a blockchain, transactions happen between addresses. Everyone with access to the system can see every transaction that is approved in the blockchain thus making the system transparent. A level of anonymity is preserved due to the nature of wallet addresses, unless the owners' information is unintentionally or intentionally disclosed to the public.

D. WHY SUPPLY CHAIN MANAGEMENT USING BLOCKCHAIN

Blockchain technology offers several advantages for supply chain management, which is why it is being increasingly explored and implemented in this field. Here are some reasons why blockchain is considered beneficial for supply chain management:

- Transparency: Blockchain provides a decentralised and immutable ledger that records all transactions and activities within the supply chain. This transparency enables participants to view and verify the authenticity and integrity of data, ensuring trust among stakeholders.
- Traceability: With blockchain, every step of the supply chain can be recorded in a tamper-proof manner. IoT devices like QR codes, wireless sensor networks (WSN), and radio frequency identification (RFID) can be used to track and organise information. Each transaction,

including the movement of goods, changes in ownership, and quality checks, can be tracked and traced back to its origin.
- Enhanced security: The decentralised nature of blockchain, along with cryptographic techniques, makes it highly secure. Data stored on the blockchain is encrypted, and any changes or additions require consensus from multiple participants, making it difficult for malicious actors to tamper with the information. This increased security helps protect against data breaches, unauthorised access, and data manipulation.
- Supply chain visibility: Blockchain enables real-time visibility into the supply chain by providing a single source of truth for all stakeholders. Participants can access relevant information, such as the origin of products, their journey through the supply chain, and associated certifications or compliance data. This visibility improves collaboration, coordination, and decision-making across the supply chain network.
- Efficiency and cost savings: By providing a transparent and secure platform, blockchain fosters trust and collaboration among supply chain participants. It facilitates direct peer-to-peer interactions, eliminating the need for intermediaries. Smart contracts also enable automated, trust-based interactions between parties, improving efficiency and reducing disputes.

III. REVIEW METHOD

The following review method has been done based on the recommendation of Kitchenham et al. [41], [42] as described in the following subsections.

A. REVIEW PLAN

The proposed survey begins with the identification of relevant research questions (RQ), followed by the identification of verified and trusted data sources. Through a systematic survey, collection of pertinent works, studies, and publications has been done. Search criteria, criteria for inclusion and exclusion technique of the databases, and quality evaluation are also identified at the outset of this planned survey. Only pertinent data is then extracted for the suggested survey after the quality of the identified material has been verified. An organised survey with clear objectives helps to reduce bias among researchers.

B. RESEARCH QUESTIONS

In proposing any literature survey, the first step after generating a review plan is to understand the research questions which correctly maps with the objective of the survey. The research questions for the proposed paper mainly focus on:

- Evolution of Supply Chain 4.0 in the electronics industry
- Integration of technologies like cryptography and blockchain
- Understanding the future use of this survey in various applications

The proposed survey identifies the current literature on supply chains using blockchain technology in the domain of electronics. The research questions along with their objectives have been listed in Table 3.

C. DATA SOURCES

In order to conduct a thorough survey, an extensive and comprehensive overview is necessary. To collect the required information and data, digital libraries such as Springer, ACM, IEEE Xplore, Wiley, and Science Direct have been searched.

Additional sources include: technical books, papers, websites of forecasting agencies and other related information, and online material regarding past surveys have been included as a part of this survey.

D. SEARCH CRITERIA

Different search criteria and keywords were used for the identification of the work papers and survey papers. Keywords like ''supply chain'' and ''blockchain'' were used to define the bounds and narrow down the search to only relevant work as illustrated in Fig. 6 and Fig. 7. The keywords used are included but not limited to the words mentioned in Fig. 6 and Fig. 7. The search phrases in Fig. 6 and Fig. 7 have not shown up in some research papers since the search string is occasionally absent from the abstract and title. The papers with the specified keywords have been manually searched in digital sources to find these papers. A manual searching process with the specified keywords has been employed in various digital sources in order to conduct an extensive survey.

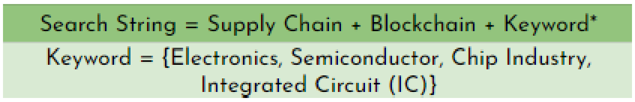
E. CRITERIA FOR INCLUSION AND EXCLUSION

Blockchain is being used in a wide variety of application areas today. Similarly, there is a large amount of work being done in the area of supply chain management. Due to this, the search strings ''supply chain'' and ''blockchain'' generate a large number of irrelevant results. The inclusion of the keyword did reduce the number of irrelevant results but did not eliminate it. As shown in Fig. 8, a thorough filtration technique was developed in order to create a relevant database of materials. For greater coverage, additional survey articles, instructional papers, technical patents, books, reports, and other resources have also been included. Fig. 8 shows the stages of inclusion and exclusion of papers. In the first stage, materials were included and excluded based on the title. The second stage involves filtration based on the abstract and conclusion of the material. In the third stage, only materials that belong to the domain of interest, i.e. electronics are retained. Research papers exploring other domains including agriculture, luxury goods, pharmaceuticals, etc., have not been reviewed as a part of this survey as they are out of scope. The fourth stage involves the reading of the papers and exclusion based on the quality and content of the material.

The next section will discuss the architecture and components involved in the traditional and modern supply chains that are built using blockchain technology.

TABLE 3. Research questions.

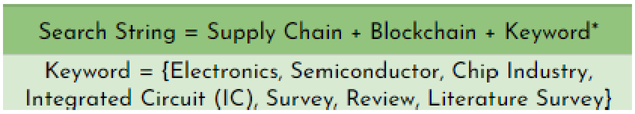
Q. No.	Research Question	Objective
RQ 1	What is the need for blockchain in supply chain?	To develop a deeper understanding regarding the advantages of the use of blockchain in the supply chain.
RQ 2	What are the eliminations in the current electronics supply chain?	To understand the shortcomings that exist in the electronics supply chain as of date.
RQ 3	How does blockchain improve the working of electronics industry?	To classify existing literature survey; various taxonomies and comparative analysis based on existing survey on the use of blockchain in the electronics supply chain, which is used to understand the relative advantages and disadvantages of existing architectures and implementations.
RQ 4	What are the open issues and challenges in such applications?	To provide information on open research issues and challenges in areas involving electronics supply chain using blockchain technology.



Search String = Supply Chain + Blockchain + Keyword*

Keyword = {Electronics, Semiconductor, Chip Industry, Integrated Circuit (IC)}

FIGURE 6. Search string employed for the collection of work papers.



Search String = Supply Chain + Blockchain + Keyword*

Keyword = {Electronics, Semiconductor, Chip Industry, Integrated Circuit (IC), Survey, Review, Literature Survey}

FIGURE 7. Search string employed for the collection of related survey papers.

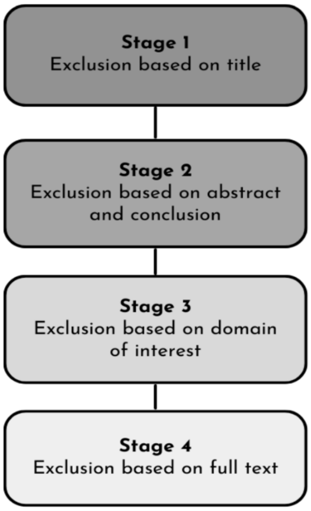

Stage 1
Exclusion based on title
Stage 2
Exclusion based on abstract and conclusion
Stage 3
Exclusion based on domain of interest
Stage 4
Exclusion based on full text

FIGURE 8. Criteria for inclusion and exclusion.

IV. ARCHITECTURE AND ITS COMPONENTS

This section provides a comprehensive overview of the underlying structure and constituent elements that form the foundation of our system. By delving into the architecture, readers will gain a deeper understanding of how different components interact to fulfill the system's objectives seamlessly.

A. TRADITIONAL SUPPLY CHAIN

A traditional supply chain typically follows a sequential flow of activities and information, starting with the sourcing of raw materials from suppliers, followed by manufacturing and distribution to end customers through intermediaries like wholesalers and retailers. Throughout this traditional supply chain process, valuable information such as customer feedback and demand data may be collected at various points. This data is crucial for decision-making processes, helping companies optimise production, adjust inventory levels, and plan for future product development and marketing strategies. Fig. 9 depicts the flow of a traditional supply chain with various stakeholders.

However, traditional supply chains do come with their own set of challenges. One significant issue is the limited visibility across the entire supply chain. Each entity involved in the chain often maintains its own set of data and information, leading to difficulties in obtaining real-time insights into critical aspects like inventory levels, production status, and fluctuations in demand. This lack of visibility can result in inefficiencies, delays, and coordination problems. Additionally, data tends to be stored in isolated silos, making it challenging to share information seamlessly between different stakeholders. Many processes within the supply chain, such as verification and documentation, still rely on manual and paper-based methods, which can be time-consuming and prone to errors. Furthermore, the lack of transparency in traditional supply chains creates opportunities for counterfeit products to infiltrate the system, as it may be challenging to verify the authenticity of products. Compliance with safety, quality, and environmental regulations across multiple jurisdictions can also be a complex undertaking.

To address all of these challenges and establish trust among consumers, a level of transparency is required that is often unattainable within a traditional supply chain framework. This is where blockchain technology comes into play. By integrating blockchain into the system, it becomes possible to track every movement within the supply chain, enhancing visibility and ensuring trust and authenticity. The subsequent section will provide further insights into how blockchain can achieve this.

B. MODERN SUPPLY CHAIN USING BLOCKCHAIN

When blockchain technology is applied to the supply chain, it introduces a decentralised and transparent architecture that

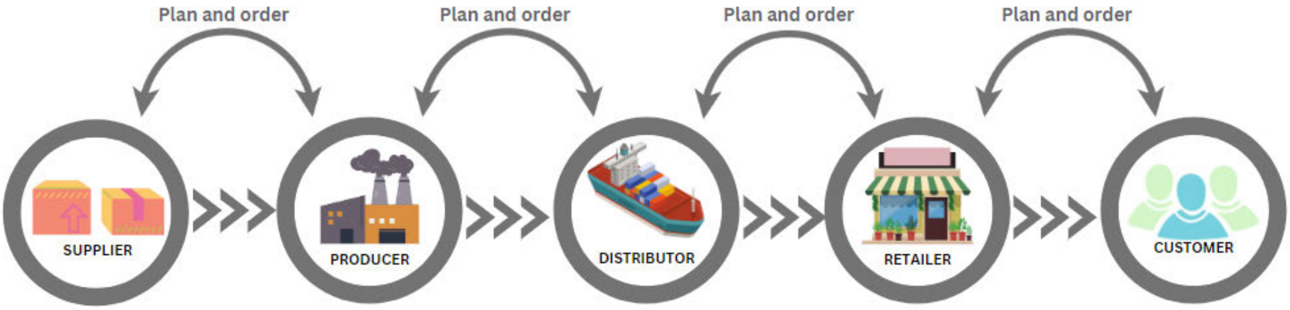


FIGURE 9. Traditional supply chain without blockchain technology.

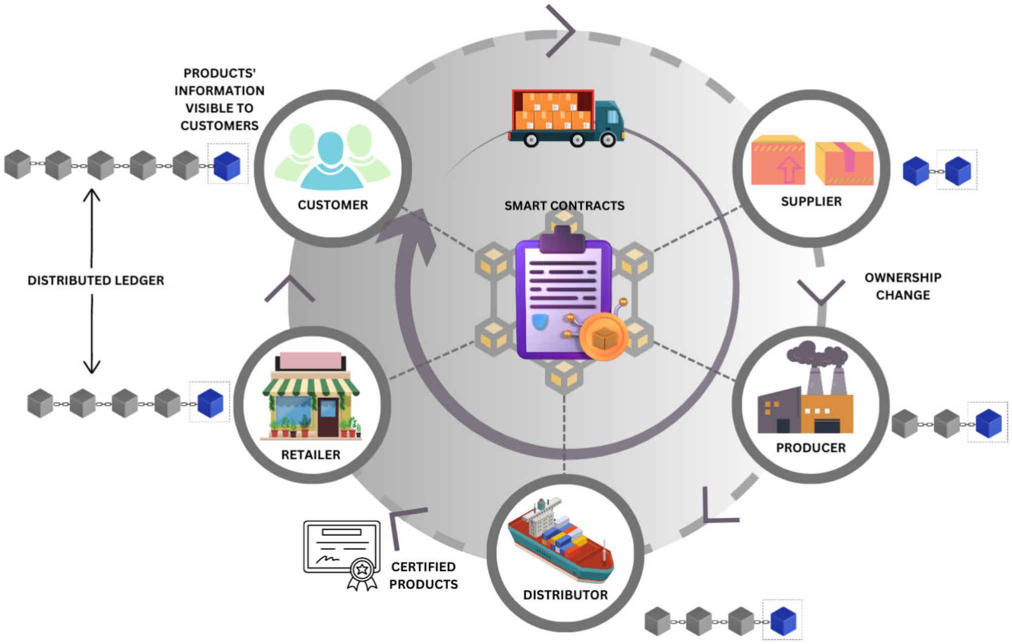


FIGURE 10. Supply chain implemented with blockchain technology.

enhances traceability, security, and trust. Fig. 10 presents a visual depiction of the supply chain incorporating the use of blockchain technology. This illustration encompasses a multitude of stakeholders, the execution of smart contracts among these participants, and their involvement in a unified blockchain network. The components of the supply chain system are:

- Blockchain Network: Consists of a distributed ledger that securely records and stores transactions or data across multiple nodes or computers. Every time the product is processed by any of the entities in the supply chain, the ledger is updated with the necessary details making it completely traceable and transparent. Each node maintains a copy of the ledger, ensuring redundancy and eliminating the need for a central authority or intermediary. The consensus mechanism ensures agreement on the validity of transactions recorded on the blockchain. It allows the network participants to collectively validate and reach a consensus on the accuracy and integrity of the data. The use of cryptographic hashes and digital signatures ensures data integrity and authenticity, enhancing the security and trustworthiness of the network.
- Smart Contracts: Smart contracts are self-executing contracts with predefined rules encoded on the blockchain. Blockchain frameworks limit the amount of running code by establishing service fees for every executed line of code. Therefore, allowing only deterministic code. They automate and enforce the terms and conditions of agreements between parties involved in the supply chain. All participants in the supply chain can access and verify the terms and execution of smart contracts, reducing the risk of disputes or discrepancies. The transparent nature of smart contracts fosters trust among stakeholders,

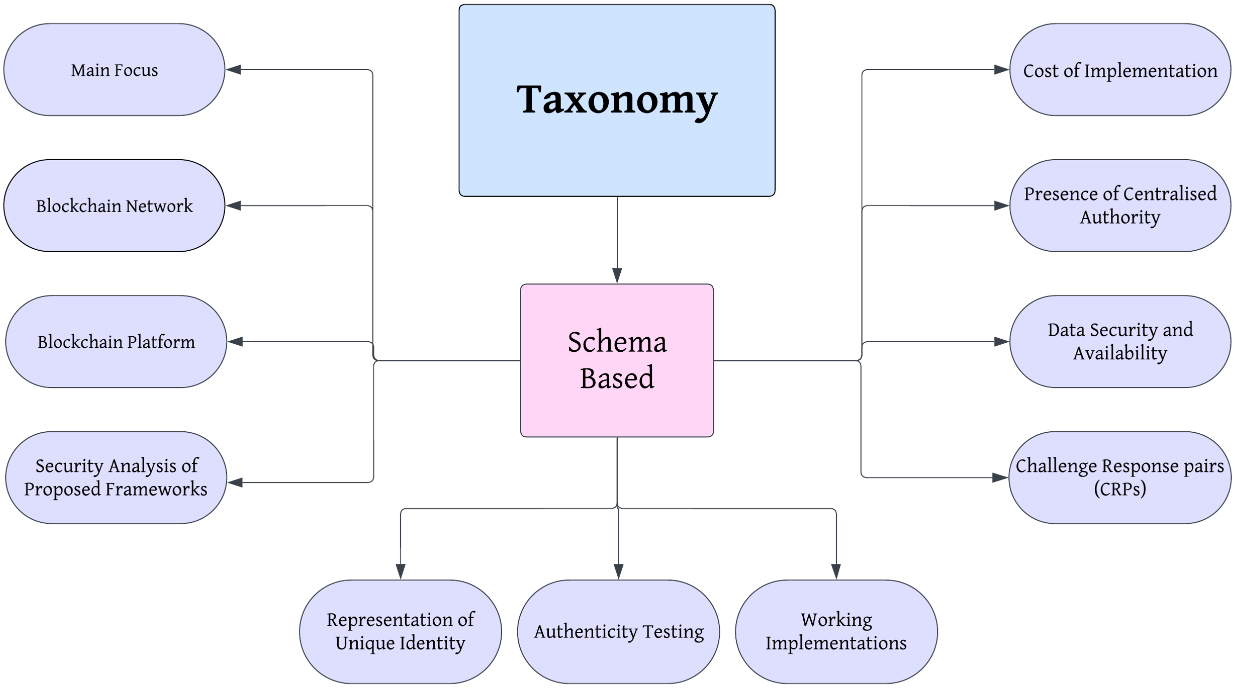

Taxonomy
Schema Based
Main Focus
Blockchain Network
Blockchain Platform
Security Analysis of Proposed Frameworks
Cost of Implementation
Presence of Centralised Authority
Data Security and Availability
Challenge Response pairs (CRPs)
Representation of Unique Identity
Authenticity Testing
Working Implementations

FIGURE 11. Taxonomy of the paper (representation of subsections).

minimises the potential for fraud, and promotes fair and accountable business practices. Smart contracts facilitate the automation of payment and settlement processes in the supply chain. For example, when goods are delivered, a smart contract can automatically trigger the release of payment to the supplier or initiate the necessary financial transactions between involved parties. This automation eliminates manual payment processes, reduces administrative overhead, and accelerates cash flow within the supply chain.

- Product Identity and Traceability: Each product in the supply chain is assigned a unique digital identity that is recorded on the blockchain. This identity can include information such as product details, manufacturing location, certifications, and relevant timestamps. By scanning a product's unique identifier, stakeholders can access its complete transaction history, providing end-to-end traceability and verifying its authenticity. The decentralised nature of the network, combined with cryptographic security and smart contract automation, enables trust and collaboration among supply chain participants while reducing reliance on intermediaries.

This integration between the various components ensures comprehensive end-to-end visibility and transparency throughout the supply chain process. In the next section, the discussion revolves around the different schemas used to categorise the content of various papers.

V. SCHEMAS

This section discusses and differentiates the existing body of work on supply chain management using blockchain technology. The section begins with a comparison of the main focus of each paper along with the various subjects addressed within each paper. This is followed by the differentiation of papers on the basis of the type of blockchain network used, platform deployed on, security of frameworks, representation of unique identity, testing authenticity, working implementation, cost of implementation, presence of centralised authority, data security and availability, encryption mechanisms and CRP (Challenge Response Pairs). A taxonomy diagram describing the interrelationships and features of each schema is described in Fig. 11.

A. MAIN FOCUS

Several papers [6], [7], [8], [9], [30], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62], [63], [64], [65], and [66] in the supply chain field have been reviewed as a part of this survey, including works studying the electronics industry. These papers covered a wide range of topics, including data storage, anti-counterfeiting measures, security and trust enhancement, tracking and tracing technologies, scalability improvements, specialised studies on integrated circuits, and the dynamics of refurbished devices. This section is devoted to summarising the central themes covered in each paper, with a focus on their essential components. Table 4 gives an overview of the same. These summaries include whether or not the papers incorporate aspects such as optimisation, architectural frameworks, implementation details, cost analysis, privacy considerations, scalability, the use of IPFS, risk modelling, and third-party verification authorities. If any form of optimisation was performed on the proposed implementation,

TABLE 4. Main focus 1-Optimised; 2-Architecture/ Framework; 3-Implementation given; 4-Cost analysis; 5-Privacy concerns; 6-Scalability; 7-IPFS used; 8-Risk modelling; 9-Third-party verification authority.

Paper	Domain	Year	1	2	3	4	5	6	7	8	9
Islam et al. [45]	Traceability protocol for counterfeit device detection	2018	✗	✓	✓	✗	✓	✗	✗	✗	✗
Bose et al. [67]	Authentication mechanism to secure both active and passive IC transactions and a composite consensus protocol for IC industry	2018	✗	✓	✗	✗	✓	✓	✗	✓	✗
Jangirala et al. [7]	Data storage (for IoT devices)	2019	✗	✓	✗	✓	✓	✗	✗	✓	✗
Kulkarni et al. [56]	Security and Trust	2019	✗	✓	✓	✗	✗	✗	✗	✗	✓
Cui et al. [43]	Anti-counterfeiting	2019	✓	✓	✓	✓	✗	✓	✗	✓	✗
Zhang et al. [49]	Recycled ICs	2019	✓	✓	✓	✗	✗	✗	✗	✓	✗
Benčić et al. [64]	Wine industry	2019	✓	✓	✓	✓	✓	✓	✗	✗	✗
Xu et al. [53]	Counterfeiting in electronics supply chain. Device authenticity	2019	✗	✓	✗	✗	✗	✓	✗	✓	✓
Islam et al. [51]	Traceability protocol to track and detect counterfeit devices	2019	✓	✓	✓	✓	✗	✓	✗	✓	✗
Demir et al. [54]	Framework for last-mile delivery using blockchain and IoT	2019	✗	✓	✗	✗	✓	✗	✗	✗	✗
Wei et al. [6]	Data storage	2020	✗	✓	✗	✓	✓	✓	✗	✗	✗
Omar et al. [58]	Automate processes and information exchange	2020	✗	✓	✓	✓	✓	✗	✓	✓	✗
Dasaklis et al. [62]	Refurbished/remanufactured mobile phones.	2020	✓	✓	✓	✗	✗	✗	✓	✗	✗
Anita et al. [59]	Anti-counterfeiting	2020	✗	✓	✓	✓	✓	✓	✓	✓	✗
Sigwart et al. [52]	IoT data provenance	2020	✗	✓	✓	✓	✓	✓	✗	✗	✗
Vosatka et al. [63]	Recycled ICs	2020	✗	✓	✗	✗	✗	✗	✗	✓	✗
Herrgoß et al. [30]	Planning in semiconductor manufacturing	2020	✗	✓	✗	✗	✓	✓	✗	✗	✗
Vosatka et al. [47]	cloned IC’s	2020	✗	✓	✓	✗	✗	✓	✗	✓	✗
Pandey et al. [65]	Medicine	2020	✗	✓	✓	✓	✓	✗	✗	✓	✗
Huang et al. [68]	Counterfeit IC detection and verification	2020	✗	✗	✓	✓	✗	✗	✗	✗	✗
Chaudhary et al. [9]	Scalable and automated authentication	2021	✓	✓	✓	✓	✗	✓	✓	✗	✗
Watanabe et al. [57]	Information infrastructure to authenticate data	2021	✓	✓	✓	✗	✗	✗	✗	✗	✗
Rekha et al. [61]	Traceability	2021	✗	✓	✓	✗	✓	✗	✗	✗	✗
Anthony et al. [55]	Anti-counterfeiting	2022	✗	✓	✓	✓	✗	✗	✗	✗	✗
Khan et al. [8]	Traceability of post-production business processes using IoT	2022	✗	✓	✓	✓	✓	✓	✓	✓	✗
Oi et al. [66]	General	2022	✗	✓	✓	✓	✗	✗	✗	✓	✗
Hossain et al. [46]	Authenticity Verification of electronics	2022	✗	✓	✗	✗	✓	✗	✗	✓	✓
Vashistha et al. [48]	Electronic Chiplets	2022	✗	✓	✓	✗	✗	✗	✗	✓	✗
Vashistha et al. [50]	Counterfeiting in electronics supply chain. Device authenticity	2022	✗	✓	✓	✗	✓	✓	✗	✗	✗
Zhang et al. [44]	FGPA device tracking and traceing	2023	✗	✓	✓	✗	✓	✗	✗	✓	✗

the paper has been marked as optimised. Papers have been marked on whether an architecture has been explicitly proposed. They have been marked on whether a working implementation of the framework has been provided. If the results of the implementation have been analysed on the basis of gas costs, they are marked under cost analysis. Papers are marked on whether they address privacy concerns such as confidentiality of data. Scalability of the solution with an increase in participants is important to check if it is feasible for the real world. Some papers use IPFS to store data. Papers have been marked under risk analysis if security threats and scenarios have been protected against. They have been marked by the presence of a third-party verification authority.

B. BLOCKCHAIN NETWORK

Blockchain technology enhances transparency and trust in the supply chain by providing real-time visibility and tracking of goods. It is crucial to choose a blockchain network which satisfies the applications and requirements of a project. Public blockchain is a permissionless, non-restrictive, distributed ledger system but it consumes a lot of energy and introduces scalability issues. Private blockchain is a permissioned and restrictive blockchain that operates in a closed network which however, is more centralised compared to a public blockchain due to a single authority maintaining the network. It is also more scalable compared to a public blockchain. On the alternative, consortium blockchains are better suited for applications where there is a need for both types of blockchains, i.e., public and private. Multiple organisations provide access to pre-selected nodes for reading, writing, and auditing blockchains, maintaining the decentralised nature without a single authority. However, consortium style blockchains are less transparent and anonymous compared to other blockchains. A more detailed properties analysis about the respective network types is present in Section II-C.

Cui et al. [43], built the prototype system using a permissioned blockchain along with a non-resource intensive consensus algorithm. By utilising a non-resource intensive consensus mechanism, the consortium blockchain avoids the cost of a transaction fee and increases efficiency. As a result, the consortium blockchain would minimise the cost of the daily operations in the supply chain, which is ideal for building a supply chain tracking system. Zhang et al. [44] proposes the use of a consortium style blockchain for the FPGA supply chain as it involves numerous entities and consortium style blockchain is a good fit since it is a permissioned platform governed by multiple organisations, hence combining the merits of both private (efficiency) and public (decentralisation) blockchains.

Hossain et al. [46] makes use of a consortium style blockchain as it has more than one central point of contact. Higher transaction rates can be achieved since a smaller number of peers participate in the consensus, as compared to a public blockchain. Furthermore, it enables transparency in supply chain activities by allowing asset verification, and transactions to be approved through voting. Vosatka et al. [47] makes use of a consortium style blockchain as well since it is a flexible, semi-private network with governing bodies managing permissions, combining decentralisation, transparency, and speed with private blockchain security. Chaudhary et al. [9] include certain TA node addresses in the contract, and these TA nodes hold extra privileges. The permissionless blockchain here allows any peer node to access/call the smart contract anywhere.

Vashistha et al. [50] makes use of a consortium-style blockchain as it provides the benefits of both public and private blockchains. Consortium blockchains limit the number of peers on the network, enabling them to offer a higher transaction rate. The transactions also do not require any fees, unlike a public blockchain. Similarly, Islam et al. [51] also uses a consortium permissioned blockchain. Demir et al. [54] uses a public blockchain as they want the end users to be read-only members of the blockchain. They believe in transparency of information along with anonymous participation of members.

The authors' chosen network type and platform combination are displayed in Table 5. As seen, most opted for consortium style blockchain due to it requiring verified entities yet supporting decentralisation unlike its private counterpart. Private networks were considered by beginner supply chains, and switched to consortium as more peers joined. Public was chosen when end users were also considered as an entity. This allowed them to access ledger data without the cumbersome process of joining the chain as a verified node.

C. BLOCKCHAIN PLATFORM

The previous section went into depth as to how to determine which network type one should choose which fits their requirements. To complement that network and their needs, the reader should also explore and be aware of the various platforms available, and why they should choose one over the other. The technology stack is ever-evolving and changing everyday. This paper focuses on four main types, which are the ones primarily chosen and used in the majority of the papers discussed; Ethereum, Hyperledger, cloud based and local private blockchain.

Ethereum is an open-source public blockchain and has gained widespread recognition due to its ability to develop and deploy smart contracts and decentralised applications. It enabled a new era of development using the Ethereum Runtime Environment (EVM) for the smart contracts to run on. Ethereum has transitioned to running on PoS algorithm, driving down its transactional costs. In the work proposed by Anthony et al. [55] a private Etheruem network was used and it was chosen because an anti-counterfeit system needs to be fast, and Ethereum is notably faster than its predecessor, the Bitcoin blockchain. Zhang et al. [9], employed an Ethereum blockchain with specific nodes that possess additional privileges within their permissioned blockchain. Benčič et al. [64] used a public network, and Islam and Kundu [51] used consortium based.

TABLE 5. Blockchain network.

Paper Name	Network	Platform
Wei et al. [6]	-	Hyperledger fabric
Zhang et al. [55]	Private	Ethereum
Kulkarni et al. [56]	-	Hyperledger fabric
Khan et al. [8]	Public	Ethereum
Chaudhary et al. [9]	Public	Ethereum
Watanabe et al. [57]	-	Ethereum
Dasaklis et al. [62]	Private	Local
Vosatka et al. [63]	Consortium	Cloud
Oi et al. [66]	-	Ethereum
Cui et al. [43]	Consortium	Hyperledger Fabric
Zhang et al. [44]	Consortium	Hyperledger Fabric
Islam et al. [45]	Consortium	-
Hossain et al. [46]	Consortium	Hyperledger Fabric
Vosatka et al. [47]	Consortium	-
Herrgoß et al. [30]	Private or consortium	Hyperledger Fabric
Benčić et al. [64]	Public	Ethereum
Jangirala et al. [7]	Private	-
Pandey et al. [65]	Private	Hyperledger Fabric
Vashistha et al. [50]	Consortium	Hyperledger Fabric
Islam et al. [51]	Consortium	Ethereum
Demir et al. [54]	Public	Hyperledger Fabric

TABLE 6. Pros and cons of the platform used.

Platform	Pros	Cons
Ethereum	Enables permissionless setup. Interoperability with other blockchains, promoting collaboration and data sharing.	PoW consensus, which uses a lot of resources.
Hyperledger	Enables permissioned setup. Plug and play framework to suit any consensus algorithm. More security as fine-grained control over data visibility, enhancing privacy and security.	Due to setting up entire blockchain from scratch, building and updates are more complex. Limited decentralisation as private blockchain.
Cloud Based	Easier to deploy and set up with preconfigured frameworks. Manages scalability	Dependency on providers leads to centralisation. Security concerns on providers
Local Private Blockchain	Easier set up, correction and testing. Zero cost to handle before actual deployment. Security vulnerabilities can be tested without risk.	Only a simulation of deployed blockchain. Cannot rely on local blockchain to handle real deployment.

Hyperledger platform is the most preferred in the enterprise sector due to it enabling complete customisation of the application from blockchain level. There is total modularity even in choosing consensus algorithm, hardware, scalability, network type, etc. It is the most preferred type for permissioned, privacy-focussed softwares. Kulkarni et al. [56] put the design and the requirements of the chip on smart contract Hyperledger.

Blockchain-as-a-service (BaaS), was conceptualised by cloud suppliers. Major hardware infrastructure could now be set and maintained. This enabled better scalability and also gave a wider range of architecture modularity in the blockchain. But due to central cloud suppliers, some amount of centralisation is introduced.

Local private blockchains are made to run on nodes running on a local system. Although not a platform as such, it is mentioned here since it is a good experiential playground over direct deployment, due to costs and security constraints. This is a good medium to gauge the approximate real-time working.

Table 6 provides a relative comparison of the papers based on the proposed platform. A large number of papers have opted for Hyperledger Fabric to build their application due to its modular architecture which enables developers to create custom blockchain networks with high flexibility. It is designed for use cases in which privacy, security, and scalability are critical requirements.

D. SECURITY ANALYSIS OF PROPOSED FRAMEWORKS

Any firm engaged in the creation, delivery, or distribution of goods and services must prioritise the security of their supply chains. Implementing safeguards to guard the supply chain against any threats, dangers, or interruptions that could jeopardise its integrity, safety, or effectiveness is known as supply chain security. Additionally, adopting typical Web 2.0 centralised technology comes with several threats. There is a great amount of trust involved, whose burden is carried by the smaller players. Such reasons encourage continuing the search for developing more efficient, optimal and secure supply chains, especially as globalisation becomes larger with more and more links involved.

Blockchain helps in the establishment of a decentralised network where each node has the ability to participate in the consensus mechanism, thereby enabling individual nodes to express their trust preferences. This provides a way for the community as a whole to come to a consensus on decisions. It includes vetting potential new nodes into the system, given they guarantee some form of authentication as proof. By this process they are granted some level of authorisation to data and network. It is especially crucial in a supply chain environment, to allow only vetted entities into the process who are known and established amongst their business partners, thus curbing the entry of malicious entities.

The nodes also carry the responsibility of vetting the correctness of every transaction that passes through the network, and each maintain their own immutable ledger of approved transactions. This guarantees non-corruptible verification of transactions, involvement and awareness of flow by all entities and a reliable and replicated ledger which can be accessible at all times without fail. Data will never be inaccessible as some copy will always be available in one of the nodes. The ledger is public, at least to the nodes of the network, so some form of transparency is guaranteed. The tradeoff is the problem of confidential transactional data being public. In this case, its encrypted form can be put on chain, and only relevant stakeholders are given the key to decrypt it at will. Only when the majority of the community turns out malicious and acts against the interest of the network, will the trustless system fail. It is assumed that the probability of such an occurrence is minimal, given that it would necessitate an entity to prioritise its own self-interest, and typically, no single participant possesses a substantial stake allowing independent action.

This section seeks to articulate the security advantages purported by the papers upon the utilisation of their proposed methodology. By supply chain requirements, the most appropriate outcomes that should be necessitated are traceability of the product, availability of data, confidentiality of data, transparency of flow, immutability of ledger, counterfeit product detection and prevention and guarantees against other cyber-attacks.

Table 7 shows work papers differentiated on what security metric they guarantee. It can be seen that there are a few papers [44], [55], [61], [62] that have included blockchain technology, but still cannot guarantee all its properties. Some papers [49], [58], [66], [67] add-on to existing technology and provide anti-counterfeit measures by discussing several cases of fraud and how their work prevents it.

Analysis of the framework's response to various attacks like illegitimate device registration, illegitimate transfer and illegitimate off-chain distribution has been carried out in work proposed by Cui et al. [43]. Zhang et al. [44] discussed the effectiveness of the developed framework in terms of recycled devices, overproduced devices, remarked devices, cloned devices and tampered bitstreams. Similarly, Hossain et al. [46] analysed performance of proposed architecture in cases of counterfeit IC detection. Zhang et al. [49] measures resistivity of the proposed architecture against several attack scenarios such as tampering with the RFID content, impersonation of a distributor, improper registration, key breach, etc. To enable a consumer centric approach, Zhang and Guin [55] allowed users to check the authenticity of the products by comparing the seller's address with the current product owner's address recorded in the blockchain. This also accounts for anti-counterfeiting and traceability. Khan and Ahmad [8] discusses how the proposed system offers high security, transparency, privacy, resilience, and robustness. Even integrity, availability, non-repudiation, confidentiality and smart contract vulnerabilities are accounted for Omar et al. [58] conducted a vulnerability analysis in which the smart contract codes are analysed using security tools: Smart Check, Oyente. Their solution also ensures security features and combats issues related to data integrity, availability, authenticity, accountability, and cyber-attacks like DDoS. The solution proposed by Anita et al. [59] consists of Uport, which uses blockchain technology as an identity verification authority where a smart contract reflects a user's digital identity while allowing the user to revoke and restore his keys, hence also helping in the key recovery process.

Rekha et al. [61] were able to trace authentic products with lineage i.e tracking of order history and transfers from manufacturing till the product reaches the consumer with multiple manufacturer entry points. Similarly, Pandey and Litoriya [65] combine lineage of product transfer along the supply chain entities with anti-counterfeit strategies from the product's birth. This allows them to decrease the probability of a single point of failure and transparently show any diverted goods while also confirming the authenticity of the product. As for frauds in manipulating authentic products, Oi et al. [66] manages to cover a possible attack wherein the logistics company replaces the genuine product with the fake and hands the fake to the end user. Thus they guarantee product authenticity, prevent product replacement and are able to distinguish each transaction.

TABLE 7. Security analysis of the proposed frameworks.

Paper name	Traceability	Availability	Confidentiality	Transparency	Immutability	Anti- Counterfeit Product	Cyber-Attack
Khan et al. [8]	✓	✓	✓	✓	✓	✗	✗
Rekha et al. [61]	✗	✗	✗	✗	✓	✗	✗
Omar et al. [58]	✗	✓	✗	✓	✓	✗	✓
Anita et al. [59]	✓	✓	✓	✓	✓	✓	✗
Oi et al. [66]	✗	✗	✓	✗	✓	✓	✗
Cui et al. [43]	✓	✓	✗	✓	✓	✓	✓
Zhang et al. [44]	✓	✗	✗	✗	✓	✗	✓
Hossain et al. [46]	✓	✓	✗	✓	✓	✓	✗
Zhang et al. [49]	✓	✗	✗	✗	✓	✓	✓
Benčić et al. [64]	✓	✓	✗	✓	✓	✓	✗
Jangirala et al. [7]	✓	✗	✓	✗	✓	✗	✓
Pandey et al. [65]	✓	✓	✗	✓	✓	✓	✗
Zhang et al. [55]	✓	✗	✗	✗	✓	✓	✗
Vashistha et al. [50]	✓	✗	✓	✗	✓	✓	✗
Islam et al. [51]	✓	✗	✗	✓	✓	✓	✗
Bose et al. [67]	✓	✓	✓	✓	✓	✓	✓

Cui et al. [43] and Bose et al. [67] provide all of the security metrics that were analysed, namely, traceability, availability, confidentiality, transparency, immutability, anti-counterfeit measures, and guarantees against cyber attacks. In the work proposed by Bose et al. [67] combination of authentication and key exchange protocol called {PUF + IBE}(Identity Based Encryption) to help with avoiding the requirement of explicitly storing the secret challenge-response pairs. Their proposed consensus protocol along with the security mechanisms aid them in avoiding a lot of IC related vulnerabilities. Thus, the proposed frameworks provide a variety of security metrics.

E. REPRESENTATION OF UNIQUE IDENTITY

Creating a new unique ID for a product is an essential practice in supply chain management and inventory tracking. Unique product identifiers help distinguish individual items, prevent duplication, and enable efficient management throughout the product's lifecycle. Thus, there is a need for proper selection or creation of such methodologies or algorithms, to try and decrease the probability of reproducibility.

Furthermore, the choice of representation of this identity is an important criteria. It factors into important tradeoff decisions relating to security, reproducibility, costs, permanence, product type, importance etc. These are the two important decisions to be made, as the entire supply chain technologies you choose revolve around being compatible with it, whilst also still guaranteeing certain thresholds are met on the parameters most important to that industry and the entities involved. The bottomline should be how pragmatic the choices work on a global scale.

There are different ways of representing these unique identities. A ***QR code***, short for "quick-response code," is a form of 2D matrix barcode. It is an optical image that can be read by machines and contains specific information related to the labeled item. In practical usage, QR codes store data for location and identification purposes. They find applications in product tracking, item identification, time monitoring, document management, and broader marketing efforts. ***RFID*** is a wireless system that utilises radio waves at various frequencies to transmit data. This system comprises two primary components: tags and readers. The reader, equipped with one or more antennas, emits radio waves and receives signals from RFID tags. These tags use radio waves to convey their identity and other relevant information to nearby readers. Applications of RFID technology span across inventory control and equipment tracking. An ***Electronic Chip Identification Number***, often referred to as an ECID is a unique identifier associated with an electronic microchip or integrated circuit (IC). A ***Physical Unclonable Function*** (PUF) is a physical entity that, under specific input conditions or challenges, produces a distinct "digital fingerprint" output, serving as a unique identifier. PUFs are often based on unique physical variations occurring naturally during semiconductor manufacturing. Table 8 represents the choice of representation with it's respective merits and demerits. The reader can guage which identity is now better suited for their product. In this section, the discussion focuses on the integration of various techniques for representing a unique identity found in different works compiled in the survey.

Zhang et al. [44] introduces the concept of PUFs that generate challenge-response pairs, forming partial markings alongside the ECID. While PUF CRPs remain confidential for device authentication, ECID is publicly accessible for device identification. RFID readers serve as key components in the representation strategies of solutions proposed in [6],

TABLE 8. Choice of representation.

Type	Pros	Cons
RFID	High Durability and Longevity, Enables real-time tracking, High data capture accuracy	High cost of tags and related infrastructure, compared to traditional barcode systems, RFID emitted signals can be intercepted by unauthorised parties, raising privacy and security concerns, Range of RFID tags is generally limited to a few meters, depending on the frequency used
QR	Cost effective and easy to use, High data capacity compared to traditional barcodes	High counterfeiting risks
PUF	Tamper resistant, Low infrastructure cost	PUFs can be influenced by environmental conditions and hardware aging, which can impact accuracy
ECID	Improves inventory and recall management, Enhanced real-time visibility	Initial infrastructure costs can be high
DLT	Maintained on distributed ledger, so guarantees immutability and traceability of tags.	Maintains only digital authenticity of device and not physical.

[7], [57], and [59]. Certain studies utilise identities generated directly by manufacturers, as these identities are assigned and engraved during the product's inception. For instance, Wei et al. [6] adopt the item numbers as a unique identifier for goods. This information is then stored within an RFID tag embedded in the chip itself. Another approach, employed by Vosatka et al. [63], involves the use of ECID that's permanently etched into the chip's read-only memory during manufacturing. Vashistha et al. [50] takes a similar route, binding speed and grade data to ECID to facilitate the detection of re-marked chips. QR codes were leveraged by Pandey et al. [65] identification by opting for multiple QR codes per product in each batch, sub-batch, and packet due to their straightforward generation and utilisation. Taking it up a notch, Benčić et al. [64] embraces Distributed Ledger Technologies (DLTs) owing to their permanence on the blockchain and limited reproducibility. However, this approach still shares the challenge of physical removal and offers only a digital guarantee. PUFs present an intriguing dynamic, necessitating generation each time for product identification due to their non-physical nature. Nevertheless, this characteristic ensures a high level of authenticity, as other physical representations remain relatively reproducible. The works propsed by Islam et al. [51] and Oi et al. [66] employs PUF outputs for device identification and authentication, with the relevant information securely stored within the ledger. Bose et al. [67] make use of {PUF +IBE} to stregthen the identification and authentication process. This combination helps with avoiding the requirement of explicitly storing the secret challenge-response pairs produced by the PUFs.

Generating unique identities

This part specifically talks about how the unique identities in the above section mentioned are generated. Some studies employed PUFs for device identification, as evidenced in [44], [45], and [51]. The process of generating addresses for participants involves the utilisation of the Elliptical Curve Digital Signing Algorithm (ECDSA). Islam et al. [49] introduce a digital signature computed from registration data including Ring Oscillator(RO) frequency and measurement conditions, combines with ECID stored on RFID tags to generate unique identities. Jangirala et al. [7] presents an approach where the blockchain generates a 20-byte public key address, known as an account identifier (in Ethereum), when provided with the tag or reader ID as input. Vashistha et al. [50], on the other alternative, demonstrates that a unique identifier can be derived from IC, parameters such as package markings, ECID, or the Combating Die and IC Recycling (CDIR) mechanism. Islam et al. [51] introduces two distinct PUF-based authentication approaches: one employs strong PUFs, while the other relies on weaker variants. Utilising the Keccak 256 algorithm, Khan et al. [8] generates unique identifiers. Watanabe et al. [57], the reader's identifier is encoded in the digest of the public key. To retrieve tag information and evidence, a search key is formulated through the amalgamation of a random number and the tag ID. This random number serves to obscure the tag ID from the blockchain service operator, typically shared among relevant parties by the RFID service. In the realm of PUFs, these mechanisms derive unique identities from specific physical attributes that inherently yield distinct outputs. Anita et al. [59] employs the Electronic Product Code (EPC), particularly EPC-C1G2, a standard in RFID-enabled supply chains, for product identification. Tag authentication here employs the Truly PseudoRandom Number Generation (TPRNG), a combination of Random Number Generator (TRNG) and Pseudo Random Number Generator (PRNG). A 1 bit random number supplements the PRNG cycle ring, aligning the output sequence of the Linear Feedback Shift Register (LSFR) with the unpredictability and irreproducibility of TRNG. The TRNG stands out as a simple yet effective algorithm that operates independently of external dependencies. In a bid to enhance its capabilities, it was combined with PKI in the research documented by the authors in [61]. Vosatka et al. [47] adopts a hybrid strategy, incorporating RO PUFs derived from FPGA hardware implementations and ECID. Shunpei et al. However, Oi et al. [66] opted to leverage IoT sensor data and product information as

TABLE 9. Representation of unique identities.

Paper Name	Generate unique identity						Represent Unique Identity				
	RFID	PUFs	ECID	RNG	Algos	Others	RFID	QR	DLT	PUF	ECID
Wei et al. [6]						✓	✓				
Khan et al. [8]					✓						
Rekha et al. [61]				✓	✓						
Watanabe et al. [57]	✓						✓				
Anita et al. [59]						✓	✓				
Vosatka et al. [63]											✓
Oi et al. [66]		✓								✓	
Cui et al. [43]		✓								✓	✓
Zhang et al. [44]		✓	✓							✓	✓
Islam et al. [45]		✓			✓					✓	
Vosatka et al. [47]		✓	✓								
Zhang et al. [49]	✓		✓				✓				
Benčić et al. [64]									✓		
Jangirala et al. [7]						✓	✓				
Vashistha et al. [50]			✓			✓					
Pandey et al. [65]								✓			
Islam et al. [51]		✓			✓					✓	
Demir et al. [54]						✓					
Chaudhary et al. [9]		✓								✓	
Bose et al. [67]		✓				✓				✓	

input for PUFs, although its susceptibility to noise introduces the potential for erroneous outcomes.

Table 9 represents the distribution of choice of representation of the generated unique IDs. As seen, most papers prefer RFIDs due to its cost, ease of use and compatibility with most technologies. Using only PUFs suffered from greater instability due to environment changes. Due to that, some papers included joining different representation techniques like PUFs with ECID to guarantee a greater probability of authenticity whilst still keeping costs relatively low.

F. AUTHENTICITY TESTING

While conducting this survey, it has been observed that one of the biggest problems in the supply chain is the verification of the authenticity of the product. Given the involvement of multiple stakeholders and entities throughout the chain, it becomes incredibly hard to pin-point the source of disingenuous counterfeit products. Testing plays a major role in the authentication of a product. This could be done by verification of the products' unique ID at every stage of the supply chain. Various technologies including electronic product codes (EPCs), PUF challenge-response pair authentication, barcodes and RFID technology have been used for the same. However, these systems rely on centralised certificate authorities and databases, making them insecure and vulnerable to cyber-attacks. This issue can be solved by the introduction of immutable decentralised blockchain systems. These systems enable product tracking to its origin through every step in the supply chain. Data integrity is not compromised at any stage given the immutability of the ledger. The ability to track the product's lineage and authenticity validation at every step allows us to identify the point of issue of counterfeit devices, and take necessary steps to eliminate the same. Every entity who comes in contact with the product is required to enter all the relevant data into the ledger. Due to this increased surveillance introduced through blockchain technology, on both the stakeholders and the products, there is an increased level of transparency and traceability, which in turn increases trust among the stakeholders. In this section, the testing methods and technologies used in various papers will be reviewed to validate the authenticity of the product.

Table 10 gives an overview of the authenticity testing methodologies adopted and segregates them based on physical or digital tests. In the paper by Cui et al. [43], participants engage in the verification of device IDs using hashed data within the blockchain framework. This process entails retrieving the unique ID of the device and subsequently comparing it with the hashed records stored in the blockchain. Trustworthy participants are granted access to historical traces associated with the device. Any absence of the device ID triggers a flagging mechanism. Zhang et al. [44] implement an ECID-based verification for ensuring authenticity. The end-user initiates

TABLE 10. Authenticity testing.

Paper name	Blockchain network	Testing method	Physical testing	Digital testing
Wei et al. [6]	-	Lineage tracking of order history and transfers from birth till consumer.	✗	✓
Anthony et al. [55]	Private	Authenticity of products verified by comparing the seller address with the current product owner's address recorded in the blockchain.	✗	✓
Kulkarni et al. [56]	-	Various parameters of the chip are tested at each level and results are checked with the originally uploaded values, enabling the tracking of the stage of alteration.	✓	✗
Rekha et al. [61]	-	Uses PKI to encrypt unique ID. Verified by decrypting and matching with onchain data.	✗	✓
Anita et al. [59]	-	RFID based tracking is used and every single part is accounted for providing end to end visibility.	✗	✓
Oi et al. [66]	-	Appends hash of received key onto the blockchain and verifies by comparing it with onchain value.	✓	✓
Cui et al. [43]	Consortium	Participants verify device IDs on the blockchain with retrieved unique IDs. Trusted participants can access historical traces, and if IDs don't exist, the devices are flagged.	✓	✓
Zhang et al. [44]	Consortium	End-user sends DApp authentication request, receives partial bitstream, packages in-field information, and returns to FPGA chain for verification (ECID based).	✗	✓
Islam et al. [45]	Consortium	Buyer uses public key to query blockchain transactions, verify ownership authenticity, and compare device holder hash values for authenticity confirmation.	✗	✓
Hossain et al. [46]	Consortium	By analysing traceability information.	✗	✓
Vosatka et al. [47]	Consortium	Authenticity verification uses device ECID, ensuring chips are authentic if PUF CRP response matches blockchain ledger.	✗	✓
Zhang et al. [49]	-	Digital signature comparison verifies NVM content integrity, and chip age is determined by comparing stored RO frequency with measured range.	✓	✓
Benčić et al. [64]	Public	Stakeholders store ownership transfer information and Smart Tag confirmations on blockchain for product lifecycle.	✗	✓
Vashistha et al. [50]	-	Analyses ownership record. CDIR sensors detect recycled ICs.	✓	✓
Pandey et al. [65]	Private	Every entity can verify from onchain data.	✗	✓
Islam et al. [51]	Consortium	Uses strong PUFs for physical testing using CRPs. Uses weak PUFs for digital testing using the digital signature.	✓	✓
Chaudhary et al. [9]	Private	Authenticity of the chip is decided based on a comparison of results between the CRP hash stored on IPFS and the authenticate device function value.	✓	✓
Huang et al. [68]	-	Validation involves defining a testing path (list of various tests) and, storing results in blockchain-associated transaction blocks, incorrect outputs signifying counterfeiting.	✓	✓

an authentication request through a DApp (decentralised Application) and receives a partial bitstream for FPGA (Field-Programmable Gate Array) download. Vital field data is encapsulated within this partial bitstream, which is then transmitted back to the FPGA chain as a response packet for validation.

Within the context of the paper authored by Islam et al. [45], the buyer employs a public key to query blockchain transactions, thereby verifying ownership authenticity. Additionally, device holder hash values are compared to confirm authenticity. Authenticity verification, as described by Vosatka et al. [47], occurs at each stage by utilising the device's ECID and PUF CRPs. A chip's authenticity is established when its PUF response aligns with the corresponding entry in the blockchain ledger. To identify suspected clone devices and associated participants, the authors of [47] record the ECID and CRPs of marked clone devices on a ledger.

Zhang et al. [49], propose a verification technique which involves comparing digital signatures to ensure the integrity of NVM content. Furthermore, chip age determination hinges on a comparison between stored and measured RO frequencies. Zhang et al. [55] introduces testing functionality enabling customers to authenticate products by comparing the seller's and current product owner's addresses in the blockchain. Inconsistencies flag the product as invalid. Consumers can query a product's ID within the system to access detailed information, safeguarding against product switching.

Kulkarni et al. [56] focuses on tracking alteration stages by leveraging timestamps in each update, aiding in pinpointing intrusion times and identifying responsible parties.

Comprehensive chip testing at different stages, encompassing various parameters and scan tests, is outlined, including stuck-at tests, at-speed tests, and challenge-response pairs, among others. Anita et al. [59] employed RFID tags for product tracking across the supply chain, affording manufacturers visibility over components and movement.

The authentication process detailed in [9] by Chaudhary et al. employs the "authenticateDevice" function to retrieve CRP hash from the blockchain. This hash is then used to access the original CRP through IPFS. Comparing IPFS and blockchain hashed responses determines chip authenticity. Rekha et al. [61] make use of private key pairs and decrypt encrypted text within the IC, allowing end users to validate the IC's legitimacy. If matched, the IC is genuine; otherwise, it's identified as potentially forged, with traceability via the blockchain database. Keys generated via PUF by Oi et al. in [66] are hashed and compared with on-chain data to facilitate verification. Repeated verifications are recorded on-chain to prevent duplication. Verification in the work proposed by Benčić et al. [64] involves stakeholders recording ownership transfers on the blockchain during product life cycle transitions. End users can cross-reference Smart Tag information with blockchain entries for verification. A similar lineage methodology for product tracking is adopted by Pandey et al. [65].

G. WORKING IMPLEMENTATIONS

As described in section II, blockchain networks come in various types, each tailored to meet specific application requirements. Among these, there are diverse public and permissionless networks like Ethereum, Binance Smart Chain, and Polkadot. For creating smart contracts, developers use blockchain-specific programming languages such as Solidity (for Ethereum) or Vyper (for Binance Smart Chain). Development and testing tools like Truffle and Hardhat are valuable for this purpose. Remix is an open-source integrated development environment (IDE) primarily designed for the development of Ethereum-based smart contracts and DApps.

On the other hand, permissioned or private blockchains are characterised by restricted access, where participants need approval to join and interact with the network. Prominent platforms like Hyperledger Fabric and Corda are widely adopted for building these private blockchain networks.

For those seeking simplified deployment and management of blockchain networks, there's the option of leveraging cloud-based services. These services are provided by cloud giants like AWS, Azure, and GCP, making the process of setting up and maintaining blockchain networks much more straightforward.

This section consists of the discussion about the working implementations and research findings extracted from our compilation. By examining these studies, valuable insights can be gained into the practicality and outcomes of utilising blockchain in supply chain contexts. From successful use cases to potential limitations and areas for improvement, this section sheds light on the tangible impact of blockchain technology on supply chain processes.

The smart contracts proposed by Anthony et al. [55], deployed on the Ethereum network provided by Remix. The testing was conducted using a dummy set of transactions. The system ensured robust traceability by meticulously recording and documenting each stage of the transaction, leaving no room for gaps or omissions. Its primary focus was to empower consumers with tools to verify the authenticity of products, promoting transparency and trust in the supply chain. Despite its advanced features, the system managed to maintain a cost-effective approach, making it accessible even for medium-priced products to leverage its benefits. Kulkarni et al. [56] created a network of their own along with developing smart contracts on a platform provided by IBM. The testing was done by providing incorrect inputs at the consumer level, which resulted in errors being displayed on the consumer's screen. The smart contracts were effectively programmed to enable asset tracking within the supply chain, thereby enhancing traceability. The smart contracts by Khan et al. [8] were written and tested on Remix IDE.The proposed smart contracts were rigorously tested to prevent supply chain violations in both forward and reverse operations within IoT-enabled smart cities. Scalability issues of existing blockchain solutions were addressed by storing extensive big data sets related to electronic devices, e-waste, and participants on the IPFS server. This solution proved to be practical, secure, viable and highly dependable. Chaudhary et al. [9] used go-ethereum (geth) for creating a local ethereum blockchain network. The deployment cost is coming out to be 64.09 USD, but this would be a one-time investment.The use of IPFS for storing challenge and response have profusely reduced the storage overhead which has been the main goal of the paper. The prototype proposed by Watanabe et al. [57] was developed using the BBc-1 (Beyond Blockchain One) toolkit. The prototype uses the toolkit to grow a Merkle tree off-chain, and periodically writes only the corresponding Merkle root to Ethereum, making the blockchain service inexpensive to use. The solution can prove the authenticity of logistics information using inexpensive passive RFID tags and blockchain. The smart contracts given by Omar et al. [58] were deployed on Remix IDE and tested. The key properties of the proposed blockchain VMI solution in addressing major security and privacy concerns were also discussed. Implementing the presented solution encourages cost-savings and would result in increased profits to supply chain stakeholders. Comparison with other Blockchain-Based VMI State-of-the-art Solutions is also done. The authors of [59] created a private Ethereum network with EVM built in using Qtum (blockchain platform that combines elements of both Bitcoin and Ethereum to create a hybrid blockchain) and stored user data stored on a ledger that is accessible only to clients and specific service providers. In comparing transaction throughput and latency with PoS and PoW, the PoA mechanism exhibited a consistent average transaction latency of approximately

TABLE 11. Working implementations.

Paper Name	Network	Smart contracts used	Deployed on	Results
Cui et al. [43]	Consortium	Registration, Device tranfer, Transfer confirmation, Tracking and verification	Hyperledger Fabric	*Consortium blockchain and Hyperledger features eliminate transaction fees and enhance efficiency. *The average latency slightly decreases to 0.76 seconds when the transaction rate reaches 10 transactions per second (tps).
Anthony et al. [55]	Public	-	-	*System promotes traceability by recording and registering each transaction step. *Functions for consumers to verify product authenticity. *Low cost, suitable for medium-priced products.
Kulkarni et al. [56]	-	-	-	*Invalid inputs at the consumer level resulted in an error message on the consumer screen. *Smart contracts were effectively programmed to track supply chain assets, promoting traceability.
Khan et al. [8]	Private	Registration, Order Manager, Waste Manager, Bid reputation Manager, and Data Destruction Manager	Remix IDE network	*Smart contracts to prevent supply chain violations in IoT-enabled smart cities. *Scalability issues solved by storing data sets on the IPFS server *The solution is practical, secure, viable, and highly dependable.
Chaudhary et al. [9]	Public	eletronicSupplyChain.sol: registerDevice, authenticateDevice, traceOwnership , deviceInfo , OwnershipTransfer, UpdateDevice	local ethereum blockchain network	*Deployment cost is 64.09 USD, representing a one-time investment. *The utilisation of IPFS for storing challenge and response significantly minimises storage overhead.
Watanabe et al. [57]	Public	-	-	*Demonstrates the authenticity of logistics information employing cost-effective passive RFID tags and blockchain.
Omar et al. [58]	Public	Registration ,Reporting, Replenishment, Payment,Transportation Cost Request	Remix IDE	*Discusses key properties in addressing major security and privacy concerns. *Encourages cost-savings *Increased profits to supply chain stakeholders. *Comparison with other blockchain based VMI Solutions.
Anita et al. [59]	Private	Registration, product transaction phase, product confirmation phase.	Qtum	*Compared transaction throughput and latency with other mechanisms like PoS and PoW and on multiple nodes. *Average transaction latency remained constant (approximately 32 seconds) under PoA, while it was 46 seconds under PoW and 40 seconds under PoS-based mechanisms. *Transaction throughput improved compared to existing systems.
Dasaklis et al. [62]	Local	Processes, Stakeholders and lineage reverse logistics	-	*Local blockchain tests revealed average transaction times in the magnitude of milliseconds (e.g., contract deployment and constructor). *Facilitates real-time RL (Reinforcement Learning) traceability.
Oi et al. [66]	Local	Registration, Verification and identification	Remix IDE	*Increased information on the blockchain leads to higher costs. *Future efforts are required to reduce gas consumption.
Zhang et al. [44]	Consortium	Covered in [50]	Hyperledger minifabric	*Time overhead for network transmission, response packet generation, and statistics generation: 1.13 seconds. *Dapp's computational performance equates to 1,000 device registrations in 20 minutes, handling 40 transactions per minute.
Benčić et al. [64]	Public	-	Ethereum	*Solution was implemented and tested within the context of the TagItWine use case, transforming wine bottles into digital products. *Gas costs per functionality were computed and analysed.
Pandey et al. [65]	Private	-	Local	*The system was tested on various configurations, and the system throughput, defined as the number of blocks generated within a specified time limit, was computed for each test run.
Vashistha et al. [50]	Consortium	Asset Creation, Asset Inquiry, Asset verification, Asset update, Asset removal	Hyperledger minifabric	*To validate the effectiveness of eChain, the research group divided into two teams: the Red team and the Blue team. *The Red team generated a dataset of genuine ICs, while the Blue team generated a dataset of counterfeit ICs. *After verifying 10,000 ICs, it was found that 15% of them were classified as counterfeit.
Islam et al. [51]	Consortium	Ownership contract, with functions for device registration, ownership verification, device authentication and ownership transfer	Ethereum testrpc, a blockchain emulator	*A total of 2,176 bytes of data was included in the challenge and hashResponse fields of a transaction.
Huang et al. [68]	-	-	Local Blockchain	* Simulation on two or three levels of the blockchain *Running time analysed for different numbers of ICs (3, 5, or 10) and different numbers of tests(10 or 20)

TABLE 12. Simulation/ Experimental setup.

Paper Name	Deployed on	System Configuration
Cui et al. [43]	Hyperledger Fabric	Environment with 3 machines, each of them equipped with 8 core CPU and 16GB RAM.
Anthony et al. [55]	Remix IDE network	Solidity version 0.8.15
Kulkarni et al. [56]	IBM platform	Linux Ubuntu OS
Khan et al. [8]	Remix IDE network	-
Chaudhary et al. [9]	A local ethereum blockchain network running on Intel(R) core	go-ethereum (geth) version 1.9.25-stable-e7872729 for creating a local ethereum blockchain network running on Intel(R) core i7-4790 CPU @3.60GHz with 12GB RAM
Watanabe et al. [57]	-	* Tested on Ubuntu 20.04.3 and macOS 11.6.1 * The only physical reader currently supported is the CDEX CRU-920MJ.
Omar et al. [58]	Remix IDE network	Solidity version 0.4.25
Anita et al. [59]	Qtum	-
Dasaklis et al. [62]	Created using node and ganache; deployed on Truffle	-
Oi et al. [66]	Remix	MacOS - Processor is 1.6GHz dual core intel core i5. Memory is 8GB, 1600MHz DDR3
Zhang et al. [44]	Hyperledger minifabric	Consists of seven peer nodes each having Intel Xeon processor and 32 GB RAM
Benčić et al. [64]	Ethereum	-
Pandey et al. [65]	Local	11 Windows 64 bit PC's connected to form a decentralised system
Vashistha et al. [50]	Hyperledger minifabric	Intel Xeon Processor with four cores and 32 GB of RAM
Islam et al. [51]	Ethereum testrpc, a blockchain emulator	-
Huang et al. [68]	Local Blockchain	Intel i7-6700K CPU and 32 GB memory

32 seconds, outperforming PoW (46 seconds) and PoS (40 seconds). Additionally, the proposed BA2C solution showcased improved transaction throughput over existing systems, demonstrating its efficiency in processing a higher number of transactions in both counterfeit and non-counterfeit scenarios. These findings highlight the advantages of PoA-based approaches in achieving faster and more reliable transactions, making them promising for enhancing blockchain-based systems in practical applications.

Dasaklis et al. [62] created a local Ethereum blockchain using Node and Ganache (personal blockchain development environment that allows developers to create and test Ethereum-based applications and smart contracts in a local, controlled environment.). Truffle was used to compile and deploy the smart contracts. The derived results in the form of recording average transaction time. They showed an average result of contract deployment and constructor in the magnitude of milliseconds thus justifying they can enable real time traceability. Similarly Oi et al. [66] worked on a local implementation wherein they deployed their contracts on Remix IDE and it was able to access local IoT sensor data. Results were delivered on the 3 stages they split up the chain on namely registration, verification and identification. Their results on implementation costs concluded that gas is already high, and is set to increase with framework complexity. So its pragmatism is low. Another local network was created by Pandey et al. [65] which is based on hyperledger fabric architecture. They recreated and emulated it using 11 windows 64 bit PCs connected in a way to form a decentralised system on a local network. Testing run on different configurations was done where they recorded the system throughput for each run.

Benčić et al. [64] established protocol for interactions between stakeholders. The DL-Tags solution has been implemented, deployed and tested in the framework of the wine industry where wine bottles become digital products. Gas costs per functionality were calculated. Table 11 mentions all the work papers that produce an implementation of their proposed framework. Differentiation based on factors of network type, smart contracts used for functionality, platform deployed on and the chosen method to represent their results are used for comparison.

Simulation / Experimental Setup

The papers have been surveyed based on simulation conducted or experimental setup used. The systems have been proposed along with system configuration, which describes the hardware and software requirements. This information has been depicted in Table 12, along with the deployment framework for reference.

Simulations have been carried out on a variety of system configurations, including Linux Ubuntu OS [56], [57] and macOS [57], [66], Windows OS [65]. Experimental analysis of the proposed solutions has been carried out in terms of throughput, transaction latency, gas prices and storage required [9], [43], [50], [51], [68].

Some of these papers have also provided information on the storage used in terms of the number of bytes, or data fields in the block. Cui et al. [43] have used a block size of 30 bytes in their solution. In another solution proposed by Chaudhary et al. [9], there is a fixed storage overhead of 92 bytes for device registration, irrespective of the number of CRPs. The solution proposed by Vashistha et al. [50] makes use of 128 bit ECIDs to encode all the required information. The implementation of a 128-bit arbiter PUF proposed by Islam et al. [51] involves a set of 128 challenges, with MD5-128 hash applied to the corresponding 128-bit responses, resulting in a total of 2,176 bytes of data in the challenge and hash response fields of a transaction. The required data fields in the solution proposed by Huang et al. [68] include Hash Value, Counterfeit Status, and Transactions, with the Hash Algorithm specified as SHA-1, featuring an output size of 160 bits.

Theoretical solutions are built on a set of assumptions and hypotheses about how things should work. Practical testing allows you to validate whether these assumptions hold in real-world conditions. It helps ensure that the solution one proposes aligns with the actual behaviors and dynamics of the environment in which it will be deployed. Hence these working implementations are important in order to decide whether the proposed solution is feasible or not.

H. COST OF IMPLEMENTATION

In Ethereum, the execution of instructions relies on a concept known as "gas," which effectively separates computational costs from the price of Ether (ETH). When one interacts with the Ethereum network by executing smart contracts or transactions, they incur costs for the computational resources and processing power required, which are paid in the form of gas. Gas is a fee measured in tiny fractions of Ether, known as "gwei" (10^{-9} ETH).

Gas serves as compensation for network validators, who maintain and secure the Ethereum blockchain. The actual cost of gas is determined by various factors, including supply, demand, and network capacity at the time of the transaction.

Two essential terms associated with gas are "gas limit" and "gas price." The gas limit represents the maximum workload you anticipate validators will perform for a specific transaction. A higher gas limit indicates an expectation of more computational work. On the other hand, the gas price represents the cost per unit of computational work. Therefore, the total cost of a transaction is the product of the gas limit and the gas price.

Additionally, many transactions include "tips" or extra fees, which are added to the base gas price. These tips can expedite transaction processing; the higher the tip, the quicker the transaction is likely to be completed. The ultimate cost of a transaction in Ethereum is determined by multiplying it by the current exchange rate with US Dollars (USD). Consequently, the transaction's total cost is denominated in USD.

In this section, the cost of implementations associated with all the approaches are discussed. The successful deployment of any supply chain solution heavily relies on its economic feasibility, and understanding the costs involved is crucial for making informed decisions. By comprehensively examining the cost factors, the aim is to provide an in depth understanding of the financial aspects of each approach, aiding businesses in identifying the most cost-effective and sustainable solution for their supply chain needs.

Average cost needed to operate the system proposed by Anthony et al. [55] is 715,046.3 gwei or 0.92 USD per product with 2 ownership transfers. Khan et al. [8] provide us with a detailed view of gas consumption of various functions in the different smart contracts they've created. Chaudhary et al. [9] claim that in a typical 5 stage electronic supply chain, it would cost approximately 21.56 USD using their approach. In the study presented by Omar et al. [58] the cost incurred by the vendor does not exceed 7 USD, while the retailer and distributor do not exceed 1 USD. Anita et al. [59] opined that, the cost of the contract deployment is 0.94 US dollars and the cost for other functions would be less than $1. Oi et al. [66] recorded cost of major device milestones like registration, verification and identification. The cost lies in the range $22-$54. In the work presented by Benčić et al. [64] gas costs for product creation, transfer of ownership, adding a new stakeholder, and voting is recorded. Vashistha et al. [50] propose eChain and eliminate any costs during the operations. Pandey et al., [65] concede that there is a tradeoff between cost and security. As more nodes are put in, costs increase, but security also increases. Islam et al. [51] use 0.11 USD to register devices (121478 gas), 0.03 USD to transfer ownership (30365 gas), and using their formula, the total cost of maintaining the identity of a chip in the supply chain with five entities is about 0.23USD. Table 13 depicts the same as mentioned above.

Since each transaction comes with a price, not knowing how much the whole solution might cost makes it hard to decide if one should adopt it. Hence to measure the viability and feasibility of the solution proposed, the cost of implementation is needed.

I. PRESENCE OF PARTIAL CENTRALISED AUTHORITY

In this section, analysis of the works based on the presence of a partial centralised authority in the framework is conducted. This partial centralised authority may be a certificate authority, or simply a privileged entity of the blockchain network. The goal of most blockchain networks is to achieve a high level of decentralisation. However, private or permissioned blockchains often have a central authority that controls the network. This central authority often has the power to add or remove participants, making it more centralised compared to public blockchains. It is easier to maintain privacy, control and scalability in networks like these. In the work of Khan et al. [9] TA nodes refers to

TABLE 13. Cost of implementation.

Paper name	Cost of Implementation
Anthony et al. [55]	715,046.3 gwei or 0.92 USD per product with 2 ownership transfers
Khan et al. [8]	Gas Consumption of various Functions in smart contracts
Chaudhary et al. [9]	For a 5 stage electronic supply chain, approximately 21.56 USD.
Omar et al. [58]	For vendor, <7 USD, while for the retailer and distributor <1 USD
Anita et al. [59]	Contract deployment, 0.94 USD and for other functions <1 USD
Oi et al. [66]	Registering device is 54.24 USD , verifying device is 22.45 USD and identifying device is 22.21 USD
Benčić et al. [64]	Product creation :1478198 gas, Transfer of ownership : 14649 gas, Add a new stakeholder :63599 gas, Voting :89603 gas
Vashistha et al. [50]	Echain is free from any cost of the transaction
Pandey et al. [65]	Proposed system is computationally intensive. However, more nodes available to reach the consensus which makes the system tamper proof.
Islam et al. [51]	0.11 USD to register device (121478 gas), 0.03 USD to transfer ownership (30365 gas).0.23 USD for maintaining the identity of a chip.

TABLE 14. Presence of partial centralised authority.

Paper Name	Partial centralised authority
Wei et al. [6]	Sender, receiver, and third-party each have their own CA node.
Vashistha et al. [50]	Certificate Authority component issues digitally signed certificates to the consortium memebers for their identification and signing transactions before posting.
Chaudhary et al. [9]	TA node is a privileged authority such as IP owner and original component manufacturers (OCM) that can do PUF characterisation of a chip.

a privileged entity, such as an IP owner or an Original Component Manufacturer (OCM), with the capability to perform PUF characterisation of a chip. On the other hand, peer nodes possess limited privileges, implying they lack the authorisation to write data onto the blockchain. Consequently, peer nodes are incapable of altering the state of the Ethereum network through any means.

Table 14 describes the existence and role of any centralised authority present in their solution. Ideally, there should be no centralisation to make the method truly decentralised. But realistically, some amount of centralisation always seeps in to make the implementation more workable.

J. DATA SECURITY AND AVAILABILITY

Data security in blockchain refers to the measures and techniques employed to safeguard the confidentiality, integrity, and availability of data stored on a blockchain network. Data availability encompasses the idea that data should be readily available to its users, while protecting it from unauthorised access, modification, or destruction.

Security of the data stored on the blockchain is a concern to all the involved entities. Due to the immutable and decentralised nature of data storage on the chain, some parties may feel that the privacy of their data is being compromised. It is critical in any blockchain implementation to safeguard the data from attackers, as well as from potentially malevolent entities in the blockchain network.

A number of security measures have been implemented in the works studied in order to promote the protection of user data. These measures range from encryption functions to storing the data at a different location. In addition to this, data availability measures have been taken, in order to ensure that data is accessible and retrievable when needed.

Table 15 consists of all the papers that have explained their data security methods and the various encryption mechanisms used to employ the same. To maintain a stricter lineage, Rekha et al. [61] make sure to record data on the chain at every stage of manufacture, and also to record the transfer of ownership in encrypted format.

The expense of using blockchain for all data storage is an overhead. To provide scalability and integrity for storing and retrieving crucial data of the entire activity, Dasaklis et al. [62] use an off-chain storage solution utilising IPFS (InterPlanetary File System). In particular, each stakeholder keeps all the pertinent data and essential traits locally using a Table of Contents (TOC) technique. The hashes of each individual record (from each TOC) are then recorded on the blockchain. With this method, they are able to effectively get data for monitoring the various activities by relying just on the related TOC from each stakeholder.

TABLE 15. Data security and availability along with encryption mechanisms.

Paper Name	Data security and availability
Wei et al. [6]	Data stored on chain, encrypted using RSA.
Khan et al. [8]	Uses smart contract modifiers, data is encrypted
Rekha et al. [61]	Data stored on chain, encrypted.
Omar et al. [58]	Data stored off-chain on IPFS. Data is encrypted and signed using SHA-256
Dasaklis et al. [62]	Data stored off-chain on IPFS. Hashing is used for efficient retrieval.
Anita et al. [59]	Zero-Knowledge Succinct Non Interactive Argument of Knowledge (zk-SNARK) to ensure privacy of participants.
Cui et al. [43]	Data stored on-chain, encrypted
Vosatka et al. [47]	Data stored in three ledgers, one of which is permissioned.
Zhang et al. [49]	Data stored on chain, encrypted using RSA or ECC.
Vashistha et al. [50]	Data stored on-chain.
Demir et al. [54]	Receiver information is kept on-chain or represented with identifiers
Jangirala et al. [7]	Data is encrypted using proposed scheme, hashing is performed.
Islam et al. [51]	Data is encrypted using a symmetric encryption algorithm like AES.
Bose et al. [67]	Data is stored on a secure database and it is optionally encryted.

In the work of Khan et al. [8], the system stores transactions, data, and metadata on the immutable distributed ledger using an event-based technique. Through cryptographic techniques, the blockchain preserves the integrity of data, and the access modifiers in smart contracts aid in the protection of user data. Omar et al. [58] also ensure data security by encryption. Each transaction in the block is hashed by a secure hash function such as SHA-256 and then signed using a secure digital signature algorithm. Hence, if a miner attempts to alter the information, then it will be automatically detected by other miners in the network. The second way that the data could be tampered with is by users. Users may attempt to manipulate and tamper with stored data. With a blockchain-based solution, such an attempt is impossible as the data is immutable using a hashing mechanism. Similarly, Zhang et al. [49] encrypt data onto the blockchain using a hash function and an encryption function (RSA or ECC). They add a digital signature of the IC, storing it in the non-volatile memory of the RFID. Anita et al. [59] propose the use of Zero-Knowledge Succinct Non Interactive Argument of Knowledge (zk-SNARK) to ensure the privacy of supply chain participants. Vosatka et al. [47] eliminate a single failure point of data loss using decentralised storage. They make use of a combination of three ledgers to store all the data. Wei et al. [6], Cui et al. [43] all store data on the chain. RSA cipher is used for data encryption. Similarly, Vashishtha et al. [50] also stores data on-chain. There is no encryption mechanism mentioned. They make use of private cloud infrastructure with entities of electronics supply chain. In the work of Demir et al. [54], whether the receiver information is kept on-chain or represented with identifiers is the choice of the developer. In case the information is kept off the chain, a resource URL should be included to access the customer information.

While Jangirala et al. [7] and Islam et al. [51], do not specify the location of data storage, both implementations make use of cryptographic techniques for the encryption of data. Jangirala et al. [7] come up with a mechanism for lightweight blockchain-enabled RFID-based authentication protocol (LBRAPS). LBRAPS is based on bitwise exclusive-or (XOR), one-way cryptographic hash, and bitwise rotation operations. With the help of the proposed authentication scheme (LBRAPS), the data is securely brought back to the supply node(s) from the tag(s) by encrypting the data using the established session key. In the work of Islam et al. [51], in the hardware authentication module using weak PUF, key generation and private key encryption take place. The private-public key pair may be keys for RSA, DSA, Schnorr, El Gamal, Elliptic Curve-based public key cryptosystems, and so on. The encryption is done using a symmetric encryption algorithm, like AES and the encrypting key is obtained from any random 128-bit string from the PUF (private key is encrypted using the encrypting key).

K. CHALLENGE RESPONSE PAIRS(CRPS)

Physical unclonable functions (PUFs) are techniques in hardware security that exploit inherent device variations to produce an unclonable, unique device response to a given input. These can be used to uniquely identify every piece of silicon. While these PUFs are unique from IC to IC, they are deterministic and repeatable, and can be used to generate a unique key for every chip.

TABLE 16. Challenge response pairs.

Paper name	Blockchain Network	CRP (CHALLENGE AND RESPONSE)
Chaudhary et al. [9]	Private	Fetch device's challenge hash from IPFS; authenticated using embedded PUF responses.
Zhang et al. [44]	Consortium	FPGA bitstream-encoded PUF downloaded on target device for CRP collection.
Islam et al. [45]	Consortium	Buyer fetches challenges from blockchain, IC's PUF responses authenticated if hashes (of challenge and response) match.
Vosatka et al. [47]	Consortium	IC authentic if its CRP and PUF response match ledger data; high confidence indicates no cloning.
Islam et al. [51]	Consortium	Buyer applies challenges to IC; IC authentic if PUF value matches blockchain's hash.

PUFs are frequently split into two groups, strong and weak, and their strength is determined by how many challenge-response pairs (CRPs) a single device can produce. When a PUF only supports a few challenge-response pairs, it is said to be weak. These challenge-response pairings may scale only linearly or as a polynomial function of the PUF size. Entity authentication and key storage frequently employ weak PUFs. A PUF that scales well enough to accommodate a high number of CRPs is known as a powerful PUF. The size of a powerful PUF may have an exponential effect on the number of CRPs. Strong PUFs enable PUF-based communication protocols and guard against attacker eavesdropping.

PUFs make use of challenge-response authentication, differing from conventional cryptographic methods. During the manufacturing process, PUFs are fed a series of challenges, and the unique responses to these challenges are recorded. This information is critical for the detection of counterfeit technology and enhances security.

In the CRP family of protocols, one party poses a query (the ''challenge''), and the other party must offer a valid response (the ''response'') in order to be authenticated. The challenge's objective is to demand an answer that only authorised users will be able to provide. Through this method, access, control, and the use of digital resources can be restricted to only authorised users and activities.

Using simple passwords or dynamic requests, challenge-response authentication safeguards digital assets and services from unauthorised users, programs, or actions, ensuring secure access to digital assets. Challenge response pairs can be used to identify counterfeit devices and chips that may be recycled, cloned, remarked,etc. A device is considered to be authentic if its CRP and PUF response matches with that stored in the blockchain ledger.

Table 16 provides an overview of the papers that have chosen to make use of challenge-response pairs for authenticity testing and verification purposes.

Zhang et al. [44], use weak PUFs to generate the CRPs and they are sent back to the Original Component Manufacturers (OCMs) along with the part marking and electronic chip ID. The data privacy policy keeps PUF CRPs secret, visible only to trusted OCMs, while ECID and part marking can be made public for identification and device authentication. In the solutions presented by Islam et al. [45] and Islam et al. [51] the buyer retrieves challenges from blockchain and applies them to the integrated chips, where the PUF generates corresponding responses. The integrated chip is authenticated if the calculated hash matches the blockchain hash. In the study presented by Vosatka et al. [47] when the chip's PUF is queried by an entity/stakeholder, CRP verifications resulting in confidence levels above the threshold confidence level receive the highest confidence the chip is uncloned and authentic.Verification results below the threshold are considered to be cloned. Chaudhary et al. [9] use CRPs in the authentication process. ''AuthenticateDevice'' is a function which receives the CRP hash from blockchain, which in turn is used as input to IPFS to get back the original stored CRP. Now the hardware instance is called from this interface to collect the response from a particular chip currently attached to this peer node. The hash of responses received from the IPFS and hashed responses received from the blockchain are matched, and the authenticity of the chip is decided based on a comparison of results. [67] incorporate PUFs along with IBE to avoid the explicit storing of the CRPs explicitly at the verifier's end. Hence they propose an enhanced blockchain protocol titled 'BLIC', BLockchain protocol for IC manufacturing and supply chain management. This model gives an insight about IC authentication without storing challenge-response pair.

This section begins with providing deeper knowledge regarding PUFs and it's types, along with the use of challenge-response authentication. An overview of the papers that have opted to employ challenge-response pairs for authenticity testing and verification has also been covered.

VI. OPEN ISSUES AND CHALLENGES

This section highlights the various open issues and challenges for the use of blockchain in the electronics industry for supply chain management:

- Sustainability concerns: Current blockchain networks have massive energy requirements. It is essential to be mindful of the technology's environmental impact, particularly with energy-intensive consensus mechanisms. Applying blockchain technology to any supply chain system will definitely drive up its energy consumption.

- Transactional latency: Blockchain network latency is the time between submitting a transaction to a network and the first confirmation of acceptance by the network. Supply chain networks have a huge number of transactions, so it is important for the network to be able to scale with a high throughput and low latency. As peers are added to the supply chain, this only becomes more of a challenge.
- Real-world applications: While several protocols and platforms have been proposed, there is a gap when it comes to real-world implementation and testing of these ideas. It is unclear how these solutions will be adopted to industries with multiple stakeholders. Most blockchain services are typically offered with limited revenue models and are initially tested on a pilot scale within corporate settings. Evaluating the suitability of any architecture should involve real-life testing to ensure its performance in the context of supply chain traceability, considering diverse cost structures and operational requirements.
- Evaluation and benchmarks: Each blockchain-based solution makes use of different platforms and transaction types. They provide their results in the form of approximate gas fees and transaction times. However, these values will vary outside of the experimental setup. There is a need for standardised benchmarks to promote further advancements in this field.
- Complexity of adoption: Blockchain technologies are still new and unfamiliar for most industries. This could lead to hesitancy in adoption. The technological challenges of shifting to a blockchain-based solution for supply chain management are massive. Different devices and processes need to be integrated into the supply chain. Supply chain systems are very complex and involve many stakeholders. The practicality is unknown due to limited real-life applications. In addition to this, user feedback is needed to improve any blockchain-based solution. The solution must be easy to understand and use.
- Establishing user verification and the role of central authorities: Depending on the specific blockchain framework employed, varying privacy requirements arise. Consequently, it becomes essential to integrate a verification methodology to address potential incidents and attribute accountability. Notably, some approaches offer complete anonymity, which presents practical challenges. Another open issue involves the role of central authorities and their impact on the network's structure. One critical aspect pertains to verifying participants' identities. The central authority can assume the responsibility of verifying participant identities to establish accountability. This is particularly relevant when striving to strike a balance between privacy and traceability. However, it's crucial to tread carefully in this regard, as excessive information provided to the central authority can lead to a more centralised and less trustless system. Revealing too much detail about participants might compromise the decentralised essence of the blockchain, potentially undermining the inherent benefits of transparency and immutability.
- Managing Penalties: Legal Steps in Supply Chains: Another significant open issue within the scope of blockchain-based supply chains revolves around legal considerations and the necessary actions to be taken in the event of penalties. As these supply chains operate within existing legal frameworks, it becomes imperative to establish protocols for addressing non-compliance and penalties.

In conclusion, the integration of blockchain technology in the electronic industry's supply chain presents many challenges, including environmental sustainability, scalability, real-world implementation issues etc. These challenges underscore the need for rigorous testing and the development of innovative solutions to fully harness the potential of blockchain in this critical sector. Addressing these issues will be pivotal in realising the benefits that blockchain will provide when used in the supply chain management.

VII. FUTURE RESEARCH SCOPE

The identified open issues challenges pave the way for a robust future research agenda that can steer the evolution of blockchain technology in the context of supply chain management. Addressing these issues on a priority basis holds the potential to unlock transformative solutions and elevate the efficacy of blockchain-enabled supply chains. The future research scope has been identified as follows:

- The energy consumption of a proposed system has to be optimised, encouraging adoption from an environmental standpoint.
- Research on scalability and low-latency solutions is important and hence facilitates a larger number of transactions in the supply chain network.
- Another key area of research could be understanding multiple stakeholder's perspectives in the practical sense while proposing new solutions so they can be adaptable even in the real world. Since blockchain is a complex technology to adopt, solutions must be easy to understand and use.
- There is a need for standardised benchmarks and evaluation metrics to promote further advancements in this field.
- Ensuring user anonymity while maintaining accountability without compromising decentralisation: Supply chain systems need to be able to maintain accountability when a mishap happens, while preserving privacy and user anonymity. The role of central authorities should be balanced.
- Another open issue is the integration of legal structures and blockchain based supply chain technology. Collaborations between academia, industry stakeholders, and policymakers will be instrumental in shaping the evolution of blockchain technology within supply chain contexts.

By focusing on these priority areas, the research community can pave the way for sustainable, efficient, and impactful blockchain-driven supply chain solutions that address the complex challenges of today's interconnected global markets.

VIII. CONCLUSION OF SURVEY PAPER

In conclusion, this paper delves into the use of blockchain in the electronics industry for supply chain management. The survey is organised into four comprehensive sections, each contributing valuable insights. A brief historical context tracing the evolution of supply chain practices and blockchain is presented. This is followed by a comparative analysis between traditional supply chain methods and the advanced architectures enabled by blockchain technology. Lastly a taxonomy diagram effectively captures the interconnected nature and distinctive attributes of each schema. This paper serves as a valuable resource for understanding the transformative potential of blockchain in enhancing supply chain dynamics within the electronics sector. It covers all aspects of using blockchain in supply chain: representation of unique identity, testing authenticity, CRPs, centralised authority presence, cost of implementation, data security and availability, encryption mechanisms, blockchain network, working implementation and security of frameworks. The main review findings found that there was a need for better evaluation metrics to test and judge these methodologies. It is also required to lessen hardware and computation burden by decreasing complexity and latency whilst still providing scalability. Blockchain technology comes with its set of benefits, but the platform would need to be changed to fit the high thoughput needs of global supply chains, which is an area that still needs to be addressed in future work.

DECLARATION OF COMPETING INTERESTS

The authors affirm that they have no known financial or interpersonal conflicts that might have influenced the research presented in this study.

REFERENCES

[1] C. P. Kirk and L. S. Rifkin, "I'll trade you diamonds for toilet paper: Consumer reacting, coping and adapting behaviors in the COVID-19 pandemic," *J. Bus. Res.*, vol. 117, pp. 124–131, Sep. 2020.

[2] K. Katsaliaki, P. Galetsi, and S. Kumar, "Supply chain disruptions and resilience: A major review and future research agenda," *Ann. Oper. Res.*, vol. 319, no. 1, pp. 965–1002, Dec. 2022.

[3] A. Raj, A. A. Mukherjee, A. B. L. D. S. Jabbour, and S. K. Srivastava, "Supply chain management during and post-COVID-19 pandemic: Mitigation strategies and practical lessons learned," *J. Bus. Res.*, vol. 142, pp. 1125–1139, Mar. 2022.

[4] M. A. N. Agi and A. K. Jha, "Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption," *Int. J. Prod. Econ.*, vol. 247, May 2022, Art. no. 108458.

[5] P. Budwal, "Supply chain resilience and customer satisfaction: A thematic analysis," 2022.

[6] Y. Wei, "Blockchain-based data traceability platform architecture for supply chain management," in *Proc. IEEE IEEE 6th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), Int. Conf. High Perform. Smart Comput., (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2020, pp. 77–85.

[7] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 7081–7093, Nov. 2020.

[8] A. U. R. Khan and R. W. Ahmad, "A blockchain-based IoT-enabled E-waste tracking and tracing system for smart cities," *IEEE Access*, vol. 10, pp. 86256–86269, 2022.

[9] C. K. Chaudhary, U. Chatterjee, and D. Mukhopadhayay, "Auto-PUFChain: An automated interaction tool for PUFs and blockchain in electronic supply chain," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, Dec. 2021, pp. 1–4.

[10] S. M. H. Bamakan, S. G. Moghaddam, and S. D. Manshadi, "Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends," *J. Cleaner Prod.*, vol. 302, Jun. 2021, Art. no. 127021.

[11] S. Johny and C. Priyadharsini, "Investigations on the implementation of blockchain technology in supplychain network," in *Proc. 7th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, vol. 1, Mar. 2021, pp. 1–6.

[12] X. Xu, N. Tian, H. Gao, H. Lei, Z. Liu, and Z. Liu, "A survey on application of blockchain technology in drug supply chain management," in *Proc. IEEE 8th Int. Conf. Big Data Analytics (ICBDA)*, Mar. 2023, pp. 62–71.

[13] S. Aich, S. Chakraborty, M. Sain, H.-I. Lee, and H.-C. Kim, "A review on benefits of IoT integrated blockchain based supply chain management implementations across different sectors with case study," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 138–141.

[14] A. Mohammed, V. Potdar, M. Quaddus, and W. Hui, "Blockchain adoption in food supply chains: A systematic literature review on enablers, benefits, and barriers," *IEEE Access*, vol. 11, pp. 14236–14255, 2023.

[15] M. A. Muzafar, A. Bhargav, A. Jha, and P. Nand, "Counterfeit protection in supplychain using blockchain: A review," in *Proc. Int. Conf. Advancement Technol. (ICONAT)*, Goa, India, Jan. 2023, pp. 1–6.

[16] S. Yasmin and G. S. Devi, "Blockchain and cloud-based technology in automotive supply chain," in *Proc. 5th Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Tirunelveli, India, Jan. 2023, pp. 771–775.

[17] M. Wang, Y. Wu, B. Chen, and M. Evans, "Blockchain and supply chain management: A new paradigm for supply chain integration and collaboration," *Oper. Supply Chain Manag., Int. J.*, vol. 14, pp. 111–122, Dec. 2020.

[18] T. K. Dasaklis, T. G. Voutsinas, G. T. Tsoulfas, and F. Casino, "A systematic literature review of blockchain-enabled supply chain traceability implementations," *Sustainability*, vol. 14, no. 4, p. 2439, Feb. 2022.

[19] S. E. Chang and Y. Chen, "When blockchain meets supply chain: A systematic literature review on current development and potential applications," *IEEE Access*, vol. 8, pp. 62478–62494, 2020.

[20] D. Shakhbulatov, J. Medina, Z. Dong, and R. Rojas-Cessa, "How blockchain enhances supply chain management: A survey," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 230–249, 2020.

[21] N. Etemadi, Y. Borbon-Galvez, F. Strozzi, and T. Etemadi, "Supply chain disruption risk management with blockchain: A dynamic literature review," *Information*, vol. 12, no. 2, p. 70, Feb. 2021.

[22] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *Int. J. Res. Eng. Technol.*, vol. 5, no. 9, pp. 1–10, Sep. 2016.

[23] K. Siba and A. Prakash, "Block-chain: An evolving technology," *Global J. Enterprise Inf. Syst.*, vol. 8, no. 4, pp. 29–35, Apr. 2017.

[24] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019.

[25] S. Aich, S. Chakraborty, M. Sain, H.-I. Lee, and H.-C. Kim, "A review on benefits of IoT integrated blockchain based supply chain management implementations across different sectors with case study," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 138–141.

[26] G. Blossey, J. Eisenhardt, and G. J. Hahn, "Blockchain technology in supply chain management: An application perspective," in *Proc. Hawaii Int. Conf. Syst. Sci.*, 2019, pp. 6885–6893.

[27] M. Reda, D. B. Kanga, T. Fatima, and M. Azouazi, "Blockchain in health supply chain management: State of art challenges and opportunities," *Proc. Comput. Sci.*, vol. 175, pp. 706–709, Jan. 2020.

[28] S. F. Wamba and M. M. Queiroz, "Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities," *Int. J. Inf. Manag.*, vol. 52, Jun. 2020, Art. no. 102064.

[29] S. E. Chang and Y. Chen, "When blockchain meets supply chain: A systematic literature review on current development and potential applications," *IEEE Access*, vol. 8, pp. 62478–62494, 2020.

[30] L. Herrgoß, J. Lohmer, G. Schneider, and R. Lasch, "Development and evaluation of a blockchain concept for production planning and control in the semiconductor industry," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manag. (IEEM)*, Dec. 2020, pp. 440–444.

[31] *Industrial Revolution: From Industry 1.0 to Industry 4.0*.

[32] L. D. Galindo, "The challenges of logistics 4.0 for the supply chain management and the information technology," Ph.D. thesis, Norwegian Univ. Sci. Technol., Norway, May 2016.

[33] *Supply Chain 4.0: The Next Generation Digital Supply Chain*, 2016.

[34] E. Frazzon, C. Rodriguez, M. Pereira, M. C. Pires, and I. R. Uhlmann, "Towards supply chain management 4.0," *Brazilian J. Oper. Prod. Manag.*, vol. 16, pp. 180–191, May 2019.

[35] *The New Normal for Supply Chains*, 2022.

[36] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, 2008," Jun. 2018.

[37] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptol.*, vol. 3, no. 2, pp. 99–111, Jan. 1991.

[38] D. Bayer, S. Haber, and W. Scott Stornetta, "Improving the efficiency and reliability of digital time-stamping," in *Sequences II: Methods in Communication, Security and Computer Science*. New York, NY, USA: Springer, 1993, pp. 329–334.

[39] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, no. 37, pp. 1–2, 2014.

[40] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Bus. Rev.*, vol. 95, no. 1, pp. 118–127, 2017.

[41] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 1–15, 2009.

[42] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Ver. 2.3, Tech. Rep., 2007.

[43] P. Cui, J. Dixon, U. Guin, and D. Dimase, "A blockchain-based framework for supply chain provenance," *IEEE Access*, vol. 7, pp. 157113–157125, 2019.

[44] T. Zhang, F. Rahman, M. Tehranipoor, and F. Farahmandi, "FPGA-chain: Enabling holistic protection of FPGA supply chain with blockchain technology," *IEEE Des. Test.*, vol. 40, no. 2, pp. 127–136, Apr. 2023.

[45] M. N. Islam, V. C. Patii, and S. Kundu, "On IC traceability via blockchain," in *Proc. Int. Symp. VLSI Design, Autom. Test (VLSI-DAT)*, Apr. 2018, pp. 1–4.

[46] M. M. Hossain, N. Vashistha, J. Allen, M. Allen, F. Farahmandi, F. Rahman, and M. Tehranipoor, "Thwarting counterfeit electronics by blockchain," Tech. Rep., 2022.

[47] J. Vosatka, A. Stern, M. M. Hossain, F. Rahman, J. Allen, M. Allen, F. Farahmandi, and M. Tehranipoor, "Tracking cloned electronic components using a consortium-based blockchain infrastructure," in *Proc. IEEE Phys. Assurance Inspection Electron. (PAINE)*, Dec. 2020, pp. 1–6.

[48] N. Vashistha, M. M. Al Hasan, N. Asadizanjani, F. Rahman, and M. Tehranipoor, "Trust validation of chiplets using a physical inspection based certification authority," in *Proc. IEEE 72nd Electron. Compon. Technol. Conf. (ECTC)*, May 2022, pp. 2311–2320.

[49] Y. Zhang and U. Guin, "End-to-end traceability of ICs in component supply chain for fighting against recycling," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 767–775, 2020.

[50] N. Vashistha, M. M. Hossain, M. R. Shahriar, F. Farahmandi, F. Rahman, and M. M. Tehranipoor, "EChain: A blockchain-enabled ecosystem for electronic device authenticity verification," *IEEE Trans. Consum. Electron.*, vol. 68, no. 1, pp. 23–37, Feb. 2022.

[51] M. N. Islam and S. Kundu, "Enabling IC traceability via blockchain pegged to embedded PUF," *ACM Trans. Design Autom. Electron. Syst.*, vol. 24, no. 3, pp. 1–23, Apr. 2019.

[52] M. Sigwart, M. Borkowski, M. Peise, S. Schulte, and S. Tai, "A secure and extensible blockchain-based data provenance framework for the Internet of Things," *Pers. Ubiquitous Comput.*, vol. 24, pp. 1–15, Jun. 2020.

[53] X. Xu, F. Rahman, B. Shakya, A. Vassilev, D. Forte, and M. Tehranipoor, "Electronics supply chain integrity enabled by blockchain," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 24, no. 3, pp. 1–25, May 2019.

[54] M. Demir, O. Turetken, and A. Ferwom, "Blockchain and IoT for delivery assurance on supply chain (BIDAS)," in *Proc. IEEE Int. Conf. Big Data*, Dec. 2019, pp. 5213–5222.

[55] Anthony, M. C. Lee, R. R. Pearl, I. S. Edbert, and D. Suhartono, "Developing an anti-counterfeit system using blockchain technology," *Proc. Comput. Sci.*, vol. 216, pp. 86–95, Jan. 2023.

[56] A. Kulkarni, N. A. Hazari, and M. Niamat, "A blockchain technology approach for the security and trust of the IC supply chain," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Jul. 2019, pp. 249–252.

[57] H. Watanabe, K. Saito, S. Miyazaki, T. Okada, H. Fukuyama, T. Kato, and K. Taniguchi, "Proof of authenticity of logistics information with passive RFID tags and blockchain," in *Proc. Int. Conf. Electron. Commun., Internet Things Big Data (ICEIB)*, Dec. 2021, pp. 213–216.

[58] I. A. Omar, R. Jayaraman, K. Salah, M. Debe, and M. Omar, "Enhancing vendor managed inventory supply chain operations using blockchain smart contracts," *IEEE Access*, vol. 8, pp. 182704–182719, 2020.

[59] N. Anita, M. Vijayalakshmi, and S. M. Shalinie, "Blockchain-based anonymous anti-counterfeit supply chain framework," *Sādhanā*, vol. 47, no. 4, p. 208, Oct. 2022.

[60] Y. Cao, F. Jia, and G. Manogaran, "Efficient traceability systems of steel products using blockchain-based industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6004–6012, Sep. 2020.

[61] S. S. Rekha, K. Suraj, and K. Sudeendra Kumar, "A holistic blockchain based IC traceability technique," in *Proc. IEEE Int. Symp. Smart Electron. Syst. (iSES)*, Dec. 2021, pp. 307–310.

[62] T. K. Dasaklis, F. Casino, and C. Patsakis, "A traceability and auditing framework for electronic equipment reverse logistics based on blockchain: The case of mobile phones," in *Proc. 11th Int. Conf. Inf., Intell., Syst. Appl. (IISA*, Jul. 2020, pp. 1–7.

[63] J. Vosatka, A. Stern, M. M. Hossain, F. Rahman, J. Allen, M. Allen, F. Farahmandi, and M. Tehranipoor, "Confidence modeling and tracking of recycled integrated circuits, enabled by blockchain," in *Proc. IEEE Res. Appl. Photon. Defense Conf. (RAPID)*, Aug. 2020, pp. 1–3.

[64] F. M. Bencic, P. Skocir, and I. P. Žarko, "DL-tags: DLT and smart tags for decentralized, privacy-preserving, and verifiable supply chain management," *IEEE Access*, vol. 7, pp. 46198–46209, 2019.

[65] P. Pandey and R. Litoriya, "Securing E-health networks from counterfeit medicine penetration using blockchain," *Wireless Pers. Commun.*, vol. 117, no. 1, pp. 7–25, Mar. 2021.

[66] S. Oi, K. Kaneda, and K. Iwamura, "Implementation of supply chain management system to prevent counterfeit using IoT device and blockchain," in *Proc. 2nd Int. Conf. Image Process. Robot. (ICIPRob)*, Mar. 2022, pp. 1–6.

[67] S. Bose, M. Raikwar, D. Mukhopadhyay, A. Chattopadhyay, and K.-Y. Lam, "BLIC: A blockchain protocol for manufacturing and supply chain management of ICS," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1326–1335.

[68] C.-T. Huang, L. Njilla, and T. Geng, "Detecting counterfeit ICs with blockchain-based verification framework," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Sep. 2020, pp. 1–8.

SHRUTI JADON received the B.Tech. degree from U. P. Technical University, the M.Tech. degree from Banasthali Vidyapith, and the Ph.D. degree from NIT Allahabad, in 2019.

She is currently an Associate Professor with PES University, Bengaluru, India. She has published many papers in various journals and conferences. Her research interests include real-time systems, cryptography, and blockchain.

ANAGHA RAO is currently pursuing the B.Tech. degree in computer science with PES University, Bengaluru, India.

During the Summer of 2023, she interned with the PESU Centre for Information Security, Forensics and Cyber Resilience (C-ISFCR). Her research interests include blockchain, data analytics, web and information retrieval, and database systems.

NETRA JAGADISH received the Diploma degree in data science from IIT Madras. She is currently pursuing the B.Tech. degree in computer science with PES University, Bengaluru, India.

She is an intern with Fortune 500 Company, Bengaluru. Previously, she interned with Adobe, Bengaluru. Her research interests include machine learning, distributed systems, blockchain, and cloud computing.

SHRISTI NADAKATTI is currently pursuing the B.Tech. degree in computer science with PES University, Bengaluru, India.

During the Summer of 2023, she interned with the PESU Centre for Information Security, Forensics and Cyber Resilience (C-ISFCR). Her research interests include distributed systems, blockchain, and cloud computing.

THANUSHREE R. is currently pursuing the B.Tech. degree in computer science with PES University, Bengaluru, India.

She is an intern with Fortune 500 Company, Bengaluru. She has previously interned with the IEEE Computer Society Bangalore Chapter in the blockchain domain. Her research interests include distributed systems and computing, blockchain, and big data.

PRASAD B. HONNAVALLI received the B.E. degree from UVCE, Bangalore University, and the M.B.A. degree from The University of Melbourne, Australia.

He is currently a Professor with PES University, Bengaluru, India. He is also the Director of the PESU Centre for Information Security, Forensics and Cyber Resilience (C-ISFCR) and the PESU Centre for Internet of Things with a Focus on Security (C-IoT). He leads the teaching, research, executive education, and industry partnership, and a consultancy in the areas of focus. He has authored and coauthored a number of research papers in leading journals and conferences. His research interests include information security, such as network and cloud security, software and web security, mobile application security, cryptography and blockchain, the IoT, SCADA, and Industry 4.0.