Multimedia Tools and Applications (2023) 82:21243–21277
https://doi.org/10.1007/s11042-022-14006-4

Redefining food safety traceability system through blockchain: findings, challenges and open issues

Ashish Singh[1] · Adnan Gutub[2] · Anand Nayyar[3] · Muhammad Khurram Khan[4]

Received: 21 April 2022 / Revised: 2 August 2022 / Accepted: 12 September 2022 /
Published online: 18 October 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
In the last few decades, there has been an increase in food safety and traceability issues. To prevent accidents and misconduct, it became essential to establish Food Safety Traceability System (FSTS) to trace the food from producer to consumer. The traceability systems can help track food in supply chains from farms to retail. Numerous technologies such as Radio Frequency Identification (RFID), sensor networks, and data mining have been integrated into traditional food supply chain systems to remove unsafe food products from the chain. But, these are not adequate for the current supply chain market. The emerging technology of blockchain can overcome safety and tracking issues. This can be possible with the help of blockchain features like transparent, decentralized, distributed, and immutable. Most of the previous works missed the discussion of the systematic process and technology involved in implementing the FSTS using blockchain. In this paper, we have discussed an organized state of research of the existing FSTS using blockchain. This survey paper aims to outline a detailed analysis of blockchain technology, FSTS using blockchain, consensus algorithms, security attacks, and solutions. Several survey papers and solutions based on blockchain are included in this research paper. Also, this work discusses some of the open research issues related to FSTS.

Keywords Food safety traceability systems · Blockchain technology · Consensus algorithms · Security and privacy issues

1 Introduction

Food is the most important necessity for all living beings. The globalization of food supply chains has increased the distance between producers and consumers. Due to this, the FSTS faces many challenges like security, privacy, traceability, and many more [147]. Customers have been concerned about food safety because various food safety accidents and misconduct happened in the last few decades. These incidents are not necessarily microbiological but also due to new technology, pollution, or obstruction in co-production processes.

✉ Anand Nayyar
anandnayyar@duytan.edu.vn

Extended author information available on the last page of the article.

Many of the food safety accidents were identified in paper [98]. The arsenic-contaminated beer scandal in 1900 in England, the mercury poison grain disaster in Iraq in late 1971, the Spanish toxic olive oil incident of 1981, mustard oil poisoning in New Delhi in 1998, aflatoxin-contaminated maize in Kenya in 2004, Chinese milk scandal in 2008, and Mars chocolate contamination with plastic in 2016 are a few examples [25, 48, 53, 112, 118, 125]. The customers raised concerns about crises like Dioxin in food and feed, mad cow disease, foot and mouth disease, and foodborne diseases like Campylobacter and food poisoning [51, 109, 139]. It is essential to resolve consumer concerns regarding food quality and safety because the food industry has changed its focus to customer satisfaction. As a result, an FSTS is needed to provide consumers with high-quality food. FSTS enables food product traceability across the supply chain by tracking all processes from raw material production to manufacturing, usage, and disposal [105, 165].

FSTS provide significant value to consumers by focusing on recalls, removing non-consumable products, and investigating the root causes of food safety issues [29, 71, 154]. The safety solutions restrict fraud's origins and maintain the products' quality. Several countries have adopted numerous norms, legislation, guidelines, and regulations to enhance food safety measures [103]. In India, for example, the Food Safety and Standards Authority of India (FSSAI) was created in 2006 to regulate the food industry [127]. Recent food traceability systems are primarily based on two architectures: centralized and distributed [85]. A third-party official is brought in in a centralised structure to oversee and control traceability. As a result, a single node attack may occur, posing an increased risk of data tampering and disclosure.

RFID technology uses RFID tags in various fields [126], including the food industry. It is a promising technology for food traceability. Several authors [4, 6, 26, 69, 96, 100, 133] discussed the advantages of RFID integration in food supply chain management in the last few years. Feng et al. [42] developed a personal digital assistant for traceability for cattle based on RFID and bar code printer. Catarinucci et al. [24] combined RFID and Wireless Sensor Network (WSN) for white wine traceability from the vineyard. RFID is an ineffective data input system in the food industry in which communication can be inconsistent and the implementation cost can be high [42]. Near field communication (NFC) is an RFID extension that helps traceability and allows shorter distance payment and data retrieval [32]. Several authors suggested supply chain traceability systems using NFC [27, 88, 113, 157, 160]. With the help of stable isotope ratio measurements, food items could be differentiated based on their sources and technical methods [107, 114, 161]. For example, chromatographic methods are used to record the fingerprint of foods. Polymerase chain reaction and deoxyribonucleic acid are used to identify pathogens, damaging acids, and undeclared allergenic products [93, 122, 138]. FSTS based on blockchain [99] can reduce the limitations of traditional systems with the help of decentralization and data tampering prevention techniques. Its decentralized and distributed architecture can eliminate the need for a central entity.

1.1 Comparative analysis of existing survey works

Many recent studies have used blockchain and other cutting-edge technology to ensure security in FSTS. Various research articles that use blockchain as a backbone for food traceability are highlighted in this subsection.

In [9], the authors included blockchain technology to ensure supply chain transparency and transportation contract fulfilment in logistics. A case study and semi-interview were

conducted. The results show that the blockchain in food administration can show the hidden layers of global transportation and food supply. In [144], authors integrated blockchain into the traditional food supply chain structure to overcome food safety issues in China. The research demonstrated how blockchain could ensure transparency, and traceability, protect customers' right to accurate information and assist the government. The incorporation of blockchain in FSTS was also investigated by [94]. It has been demonstrated that blockchain can assist in tracking the origin of food, restricting food theft and adulteration, and eliminating sources of foodborne illness. Future research involves blockchain scalability between retailers and food processors. Galvez et al. [44] looked at the reliability of blockchain technology in the food supply chain and its benefits, obstacles, and future potential. They stated that digital fingerprints, hash trees, and hybrid distributed ledgers enhanced the security of the FSTS. The review article [31] discusses the establishment, applications, and challenges of blockchain combined with other technologies like the Internet of Things (IoT) in the food industry. They have concerns about traceability, security, authentication [140], production, automation, logistics and storage, digital fingerprint, and customer information. Authors in [117] have reviewed blockchain-based supply chain systems challenges by checking blockchain adopters in the USA and India. They proposed a model using a reformed version of the classic unified theory of acceptance. They then evaluated it using partial least squares structural equation modelling, which showed clear adoption practices between India and the USA. The authors [128] conducted a thematic study of the process, benefits, and challenges of blockchain adoption in the online food supply chain.

The authors [110] discussed various case studies related to agricultural food supply chains using blockchain technology and other distributed ledger systems. They have identified how each supply chain is unique and needs an appropriate blockchain structure accordingly. Feng et al. [43] addressed the blockchain-based solutions for food traceability problems that eliminate the centralized structure of conventional IoT systems. They proposed a traceability framework using blockchain IoT to improve the system's performance. The authors [12] addressed the boundary requirements for blockchain technology to be used in FSTS. There are eighteen boundary requirements, some of which are supply chain specific and five explicitly applicable to the blockchain. The adoption of blockchain in the current supply chain of agricultural food was examined by [73]. They were able to validate thirteen blockchain enablers with the help of the decision-making trial, evaluation laboratory approach, and interpretive structural modelling in the context of India. The study found that real traceability can be possible by adopting blockchain, which provides auditability, non-tamperable, and provenance. The implementation of blockchain and IoT technologies in the food supply chain was discussed in [19, 87]. The authors examine a food traceability framework by incorporating IoT sensors and blockchain integration while shipping eggs in the Midwestern-based US.

The above-discussed studies do not cover a systematic review which covers all the aspects of blockchain and FSTS. This motivates us to develop a systematic review on FSTS using Blockchain technology. This work tried to cover all the aspects missing in previous studies. We have focused on the various elements of a blockchain and the need and implementation of a traceability system using this technology. Based on the above observations, we have tabulated and compared several survey papers to enumerate the limitations and novel contributions. The comparative analysis of the survey works is presented in Table 1. This table shows the novelty and contribution made to this article. The comparison is based on discussed topics, blockchain background, security requirements, security and privacy issues, FSTS network architecture, blockchain solutions, consensus algorithm, security attacks, security attacks solutions, and open issues. The table uses three symbols: "–" sign

Table 1 Comparative analysis of survey papers

Paper	Year	Discussed topic	Block chain background	Security requirements	Security & privacy issues	FSTS network architecture	Block chain solutions	Consensus algorithm	Security attacks	Security attacks solutions	Open issues
Badzar et al. [9]	2016	Potential of blockchain in supply chain transparency & sustainable transport contract	✓	✓	–	X	✓	–	X	X	✓
Tse et al. [144]	2017	Application of blockchain in the food supply chain information security	–	✓	–	✓	✓	X	X	X	X
Mohan et al. [94]	2018	Improving traceability of food products with blockchain	✓	–	–	✓	–	✓	X	X	✓
Galvez et al. [44]	2018	Applying blockchain to food traceability system & the future challenges	✓	–	✓	✓	✓	X	X	X	✓
Credyt et al. [31]	2019	Establishment, applications and challenges of blockchain combined with IoT approaches	–	–	X	✓	–	✓	X	X	–
Queiroz et al. [117]	2019	Conflicts in the adoption of blockchain in supply chain	✓	X	–	X	✓	X	X	X	✓
Chen et al. [128]	2020	Thematic analysis of the adoption of blockchain in the supply chain of food	–	X	–	X	✓	X	X	X	✓
Patelli et al. [110]	2020	Different case studies related to agricultural food supply using blockchain and other distributed ledger systems	–	–	X	X	✓	X	X	X	✓

Table 1 (continued)

Feng et al. [43]	2020	Blockchain-based solutions for food traceability problems	✓	✓	✓	✓	✓	X	X	X	✓
Behnke et al. [12]	2020	Boundary conditions for food traceability using blockchain technology	–	X	X	✓	–	X	X	X	✓
Kamble et al. [73]	2020	Adoption of blockchain in Indian agriculture supply chain	–	✓	–	✓	X	X	X	X	–
Bumbla uskas et al. [19]	2020	Application of blockchain and IoT technology in food supply chain	✓	–	X	✓	✓	–	X	X	–
This survey		Blockchain background, security requirements, security & privacy issues, FSTS architecture, blockchain solutions, consensus algorithms, security attacks, attack solutions, and open issues	✓	✓	✓	✓	✓	✓	✓	✓	✓

refers to less discussion of the related topic, "✓" signifies that the subject is covered, and "X" denotes the absence of the concerned domain.

The successive sections elaborate on the below novel contributed points:

- This work studied and compared various survey papers with our survey to build the novelty of the work. In this manner, the research gaps are tabulated in Table 1.
- This survey work provides a thorough study of blockchain, its characteristics, involved technologies, etc. It facilitates the security and privacy requirements in FSTS while blockchain technologies are included.
- The existing solutions based on blockchain have elaborated to establish a secure conceptual system using blockchain in FSTS.
- We have categorized various consensus algorithms and security attacks with their solutions to implement a secure and robust system.
- We have studied the overall FSTS using blockchain and outlined some of the challenges and open issues involved that need to be handled in the future.

The taxonomy of this survey work is presented in Fig. 1. In Section 2, we explore the background of blockchain technology, its architecture, characteristics, etc. The implementation of FSTS using blockchain technology is illustrated in Section 3. In Section 4, we have done a detailed comparative analysis of previous works on solutions for FSTS using blockchain. Section 5 discusses various consensus algorithms. Security attacks and their solutions are discussed in Section 6. Challenges and open issues are listed in Section 7. The paper is finally concluded in Section 8.

2 Background of blockchain

Before discussing FSTS using blockchain, we have discussed the various aspects of this technology. Blockchain technology was first invented by Satoshi Nakamoto in 2008 with the creation of the Bitcoin cryptocurrency [99]. However, now the technology is not limited to finance and is being used in various fields [67, 76, 129]. Therefore, this section will help to understand this technology more descriptively. Here we have discussed the blockchain architecture, layered view, technologies involved, deployment, various entities, and characteristics.

2.1 Blockchain technologies

Blockchain was developed by including leading technologies like P2P networks, Distributed ledger, smart contracts, Consensus, and cryptography [166]. Each technology is discussed and presented in Fig. 2.

- *Smart contracts:* Smart contract is a small digital computer program stored in the blockchain network in distributed ledger fashion. These smart contracts do not require the involvement of third parties. It is a self-executing digital agreement between buyers and sellers. It automatically runs when predetermined conditions have been met and verified. This makes the system more efficient, trusty, and transparent. All participants can immediately know the outcome of the contracts [11, 61, 63, 150]. Ethereum blockchain was specially programmed to support smart contracts.
- *Consensus:* A Consensus is a type of analysis process for a group of users where these individuals have a common agreement with some decisional statements. In the

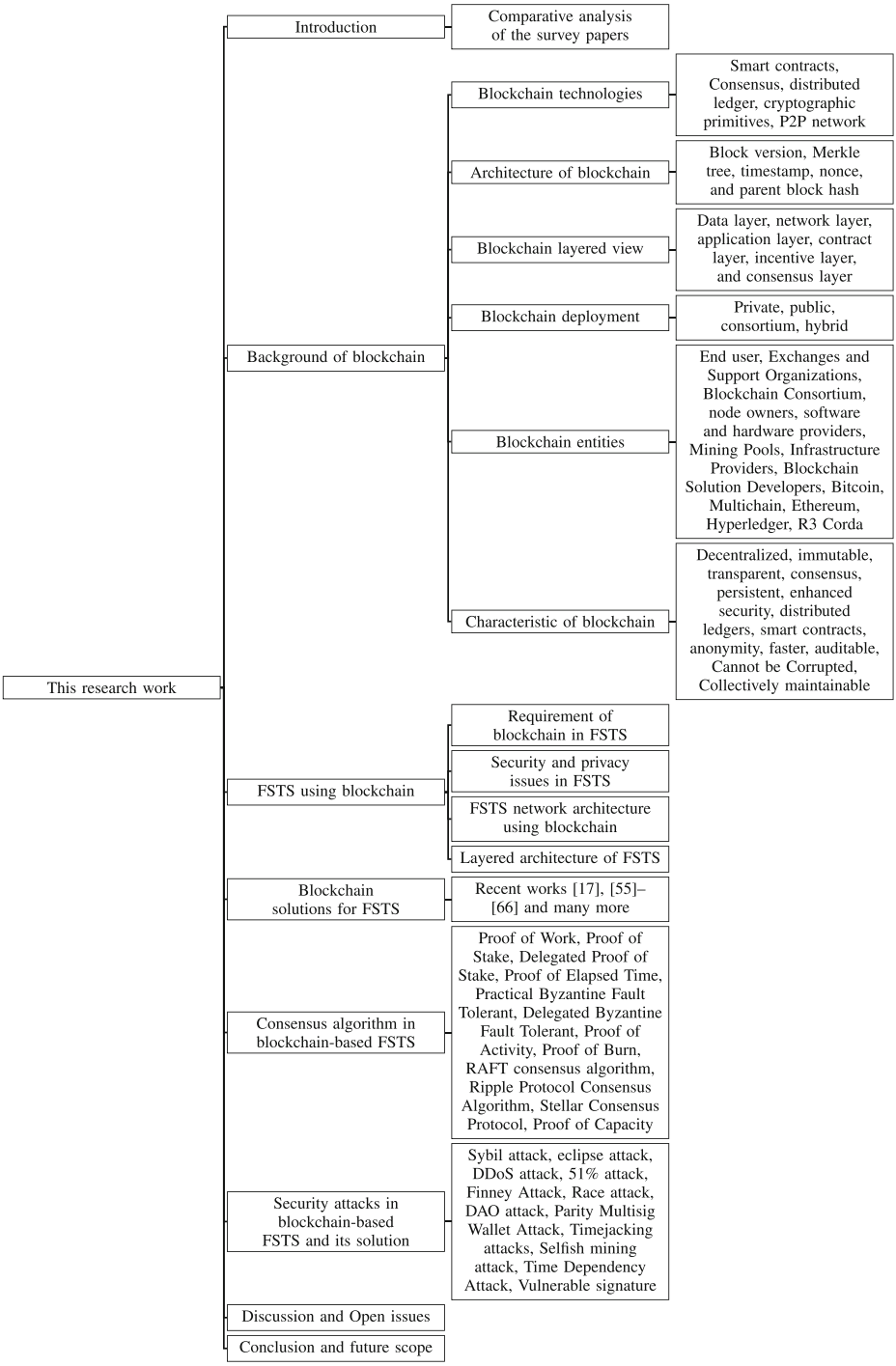

Fig. 1 A taxonomy of this survey work

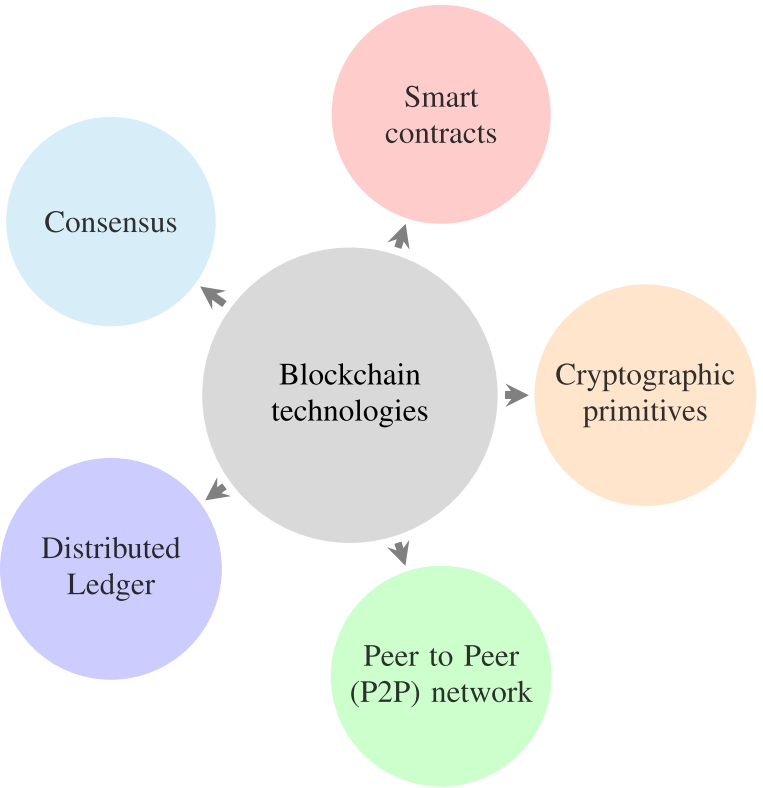

Fig. 2 Blockchain technologies

blockchain, all the nodes in the distributed network should agree on the proposed transaction state. In the blockchain, various algorithms help the nodes to reach a consensus on the transaction history [39]. The algorithm has two goals: first, to protect the network from malicious nodes and second, to tackle the competing chains.

- *Distributed ledger:* The distributed ledger refers to shared databases. It is used for storing the history of transactions in the network. It can store static and dynamic data and private or public [89]. Since the distributed ledger is not centralized, the data is kept consistent with the help of consensus algorithms which help ensure data integrity and prevent attacks and frauds.
- *Cryptographic primitives:* Cryptographic constraints ensure the security of transactions, data immutability, reliability, and data integrity. Blockchain technology uses cryptographic techniques like public/private key cryptography, ring signature, asymmetric-key cryptography, hash functions, zero-knowledge proofs of knowledge, and many more [7, 8, 92, 148, 151, 164].
- *Peer to Peer (P2P) network:* A P2P network is simply a distributed network of devices that exchange information without a central authority. Each participant in the network is called a node or a peer. Each node has an identical copy of the network's data. Blockchain technology is built on a P2P network for establishing a decentralized system so that participants can make transactions and information can be transferred worldwide without the need of an intermediary [34, 37].

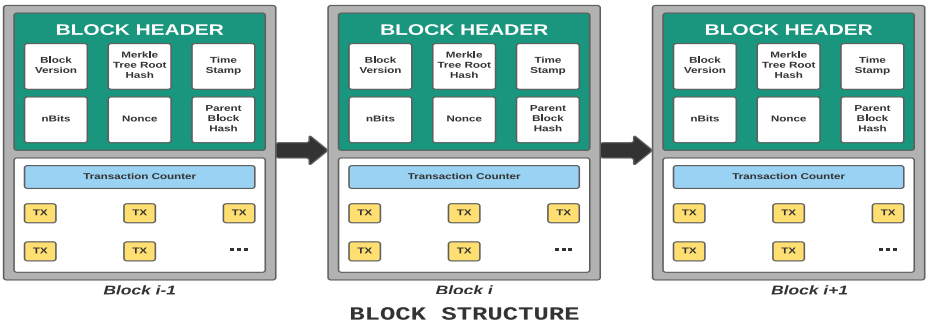

Fig. 3 Blockchain architecture

2.2 Architecture of blockchain

Blockchain is made up of blocks that contain a complete list of transactions [102]. The configuration of a block in the blockchain is depicted in Fig. 3. The first block in the chain is called the genesis block and it has no parent block [162]. Each block contains the following information:

- Block version: It specifies the 4-byte long version number that defines the validation rules or protocol followed by a set of blocks.
- Merkle tree root hash: A Merkle tree is a 32-bytes field binary tree in which the leaf node stores one transaction detail and the non-leaf node stores the concatenation of the hash of its child nodes. The 256-bit root hash of the Merkle tree is used to check the integrity of the transactions in a block.
- Timestamp: A small digitally recorded moment stored at the time when the block was created.
- nBits: It is a 4-bytes field that defines the complexity while adding the block in the blockchain.
- Nonce: A 4-byte field used for the proof-of-work algorithm. It begins with 0 and increases with each hash calculation maximum of 2^{32}.
- Parent block hash: It is a 256-bit hash block that refers to the previous block.
- Transaction counter: The block body comprises a transaction counter which defines the total number of transactions stored in the block. The maximum number of transactions determines the block size and the size of each transaction.

2.3 Blockchain layered view

There are six layers in a blockchain, including the data layer, network layer, application layer, contract layer, incentive layer, and consensus layer. The data layer ensures no tampering with the data in the block. It summarizes the underlying data and basic algorithms. The network layer contains the propagation protocols and data verification techniques. The application layer handles user situations and cases with the developed user applications. The contract layer performs programmability and operability into the network. It also encapsulates a variety of script algorithms in smart contracts to make transactions automatically.

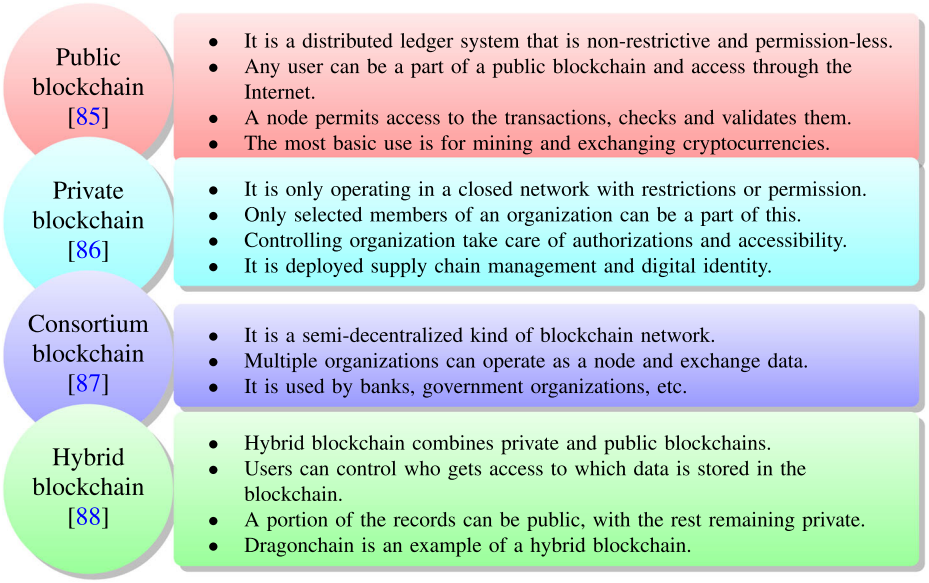

Fig. 4 Different blockchain deployments and their brief explanation

The incentive layer integrates economic considerations into the blockchain framework. It encourages each node to participate in the validation and security verification process. The consensus layer enables all nodes to achieve a fast consensus for block data verification.

2.4 Blockchain deployment

The blockchain included a variety of flavours depending on the requirement and uses. It depends on the stored information in the block and activities performed by the various participants. It mainly has four deployment models: public, private [115], consortium, and hybrid blockchain [119]. A brief explanation of each model is shown in Fig. 4.

2.5 Blockchain entities

The blockchain network has different entities that play various roles, like regulating, monitoring networks, and mining the networks. This subsection tabulates various blockchain network participants/entities with their roles and responsibilities in Table 2. The category of blockchain entities included consumers, resource providers, developers, frameworks, miners, and owners.

2.6 Characteristics of blockchain

Blockchain Technology has gained much popularity over the past few years [162]. The list of characteristics that make it different from other technologies is shown in Fig. 5.

Table 2 List of blockchain entities, their category and responsibilities

Entities	Category	Role & responsibilities
End User	Consumer	End users could be investment businesses looking to profit from previously established blockchain networks. They may be unaware of the blockchain's capabilities.
Blockchain exchanges and support organizations	Resource providers	The support organization provides resources to the end users. Coinbase, Binance, and Bitfinex are some instances of bitcoin exchanges [68].
Blockchain Consortium [36]	Developers	The blockchain consortium helps the progress of blockchain technology in specific industries by coordinating activities such as conferences, open-source projects, and workshops.
Blockchain node owners	Owner	The groups, individuals, or organizations that construct, administer, and monitor the entire nodes in the blockchain.
Blockchain mining Software and Hardware (S&H) providers	Miner	The providers provide customised and dedicated S&H for the mining process. This will leads to more rewards than commodity S&H. This attracts industry people to facilitate blockchain-based software, chipsets, and various implementation services, which leads to a financial reward for nodes.
Blockchain mining pools	Resource provider	Blockchain mining pools provide miners to pool their resources to get the puzzle solved [86]. Some examples of mining pools are bitclub, Btc.com, and blockchain.com.
Blockchain infrastructure providers	Resource providers	They provide packaged or individual products consisting of network, infrastructure, mining software, servers, etc., to the groups or organization that wants to utilize the power of blockchain for the best result [130].
Blockchain solution developers	Developers	A pool of blockchain-skilled people, system consultants, and integrators from organizations or freelancers. They help to define and implement use cases and prepare meaningful and understandable solutions.
Bitcoin	Framework	Bitcoin is a cryptocurrency payment network that uses cryptographic techniques to guard money and transactions [99]. It is a public and non-permissioned blockchain network.
Multichain	Framework	MultiChain is a platform that helps create private or consortium blockchain networks in a simple way [52]. MultiChain is based on blockchain protocol and software used in bitcoin. But it has significant mining and privacy differences. It allows permissions to be defined at the network level.
Ethereum	Framework	Ethereum is a open-source decentralized technology [20]. It enables users to build operations and is a forum for various blockchain applications.
Hyperledger	Framework	Hyperledger Fabric is a permissioned distributed ledger platform and designed for enterprises [21]. It introduces sharing concepts where ledger sharing can happen in only selected participants.
R3 Corda	Framework	Corda is an open-source distributed ledger platform that empowers businesses' private interactions. Corda's design is different from a traditional blockchain system as it does not use a chain of blocks linked by hash to store data [59].

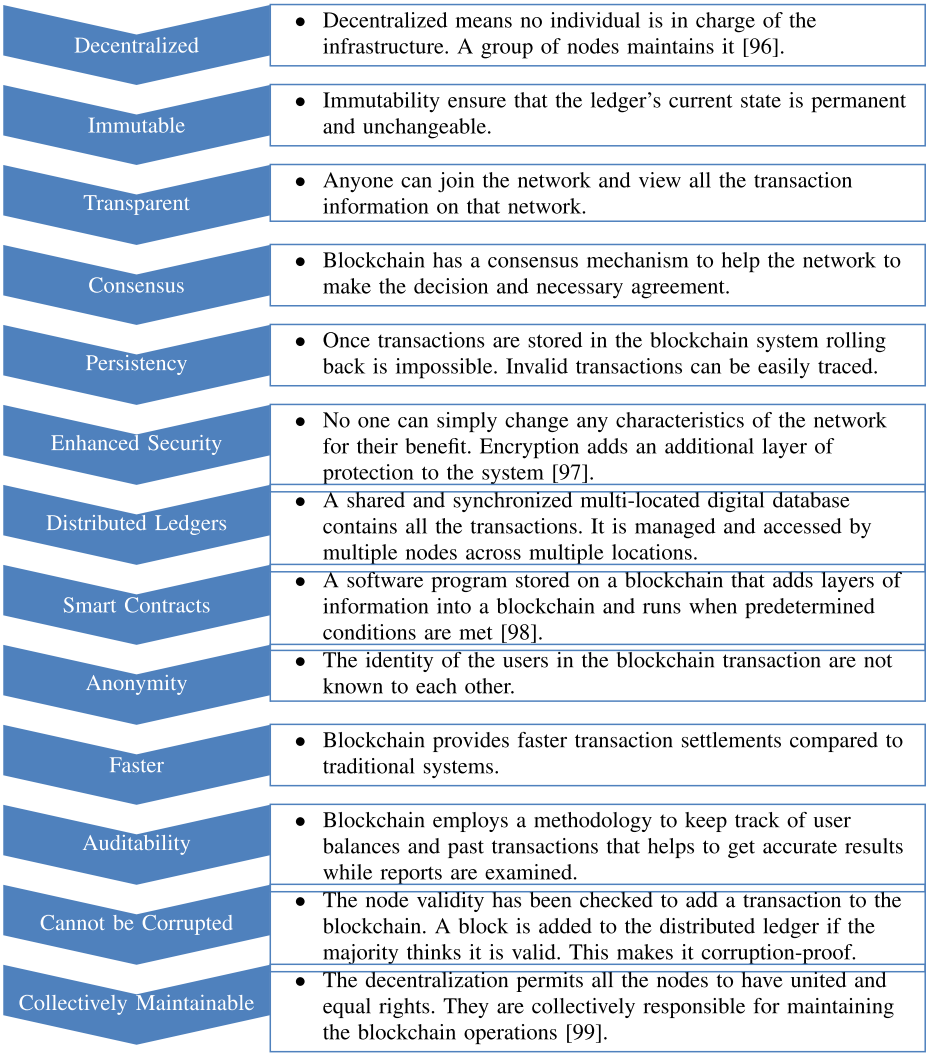

Fig. 5 Characteristics of blockchain

3 FSTS using blockchain

It has become necessary to establish FSTS to track food status in the supply chain with growing food safety issues [46, 145]. In this section, we discuss FSTS using the technology of blockchain. Here, we have analyzed the blockchain integration of FSTS, the security and privacy issues involved, and finally, the network and layered architecture of the implementation of FSTS using blockchain technology.

3.1 Requirements of blockchain in FSTS

Although IoT and other technologies [47, 55] have already been used in FSTS. But, these technologies do not provide complete food safety, including transparency, auditability, and traceability. This subsection discusses some of the important requirements of blockchain in FSTS.

1) The blockchain is used for automated record keeping and tracking information of food products in the global food industry. It is becoming increasingly popular due to the ability to track a food product's entire life cycle from start to finish. Consumers can track their food information from "origin to final" using a QR code or barcode. The blockchain features such as consensus algorithm, smart contract, and irreversible time vector can revolutionize the food safety traceability framework.
2) Blockchain can identify the source of contamination in the system and quickly correct any errors. The food industry will use the openness of blockchain to check and confirm the origin of supplies and modernize trademark credibility. Other advantages include improved protection, outbreak correction, and fraud prevention.
3) The blockchain integration in FSTS enhances real-time monitoring of food location, transportation and storage conditions in the warehouse or during transmission. They involve participants who can automatically get notifications about non-compliant food logistics or conditions.
4) The blockchain can reduce the time to trace food products. According to Fortune, an indoor team required six days, 18 hours, and 26 minutes to monitor a pack of mangoes. This time can be reduced to less than two seconds to track the sliced mangoes using blockchain [72].
5) Blockchain is an immutable distributed ledger of digital transactions in which data is authenticated in real-time and added to the chain as a new transaction. Since no single authority has power over the information. This facilitates no one to change the data, ensuring data trustworthiness over the given information. As a result, it removes the need for third-party processors while ensuring the efficiency and transparency of suppliers, retailers, and counter-parties.
5) The government authority brings some exciting concepts after seeing the technology in blockchain, such as strengthening their dominant management weaknesses. Blockchain will ensure product quality for businesses and allow fast responses to changing market conditions. Additionally, blockchain will secure consumer rights through smart contracts and allow a transparent audit trail for the food supply chain documents.

3.2 Security and privacy issues in blockchain for FSTS

Nowadays, everyone is interested in blockchain technology for the development of FSTS. Security and privacy issues in FSTS remain a concern that needs to be addressed as soon as possible, even though blockchain has provided easy and dependable services. Several authors have published numerous studies on blockchain privacy and security concerns for FSTS [54, 56, 65, 70, 74, 95, 104]. The following are some of the blockchain security concerns for FSTS:

1) *51% security issue:* The biggest threat in the blockchain is the "51% attack". In this attack, a group of miners can reverse or halt the new transactions by controlling

more than 50% of the network resources. This may create a double-spending problem. Blockchain technology in FSTS faces such issues in which some miners control transactions.

2) *Phishing and social engineering:* The most widespread scams in blockchain are phishing and social engineering scams. An attacker can create fake blocks in FSTS, which may be invalid [1, 152]. The attacker misleads users by creating fake identities. The entire identity is copied, including email signatures, social media handles, URL design, and website design.
3) *Security of the blocks:* Highly decentralized blockchain technology in FSTS faces this security issue. The transaction blocks in FSTS can be stolen. Stolen data blocks create data leaking issues in the traceability system. Using a wallet password is the best solution to protect the system from block theft. A wallet password protects all legal transactions so no one can extract the information even if data blocks are stolen.
4) *Scalability:* The validation of the transactions is an important technical process in blockchain networks. The validation process of transactions takes much time, which reduces the transaction efficiency and system throughout. The FSTS might become slow if the number of transactions increases exponentially.
5) The blockchain-based FSTS is a decentralized technology in which data are distributed among peers. Any user can join the network and perform the transactions. This may reduce the resiliency of the food supply network. A more intelligence and automation joining system is needed in which only the authorized parties can join the network and perform the transactions.
6) *Security of smart contracts and execution codes:* The security of smart contracts is the most critical issue in FSTS. The vulnerabilities present in the smart contract may destroy the complete FSTS. These vulnerabilities include re-entrance, transaction inconsistency, failed exception handling, tempering timestamps, and many more.
7) *Security of transactional and operational data:* A insecure data exchange and storing the operational information insecure way have succeeded in various cyberattacks and fraud. FSTS transactional and operational data security can be implemented using a contract among various participants.
8) The unauthorized access of smart contracts' source codes, code errors, invalid transactions, and mining attacks might create significant financial losses for FSTS actors.

3.3 FSTS network architecture using blockchain

The architecture of food traceability using blockchain is shown in Fig. 6. The food supply chain entirely relies on the transaction information between the parties and product data. Consensus processes between supply chain users, internal members, governments, and regulatory authorities are used to maintain the entire blockchain structure. It instantly stores details on each node in the blockchain network. It ensures data immutability and authenticity in the food supply chain. The required data is held in a blockchain system with a traceable database. Regulatory authorities supervise the traceability database. The ultimate goal of creating the traceability database is to provide the confidentiality of data and distinguish it from the original digital abstract on the blockchain.

The primary goal of food traceability is to determine the correct product information. This can be possible when effective monitoring and tracing are done. The data carriers like RFID and barcode are also used to identify logistics information like positions, members, and objects. The blockchain-based FSTS allow the writing of quality-controlled data in the blockchain. Other nodes in the FSTS network validate these transactional data.

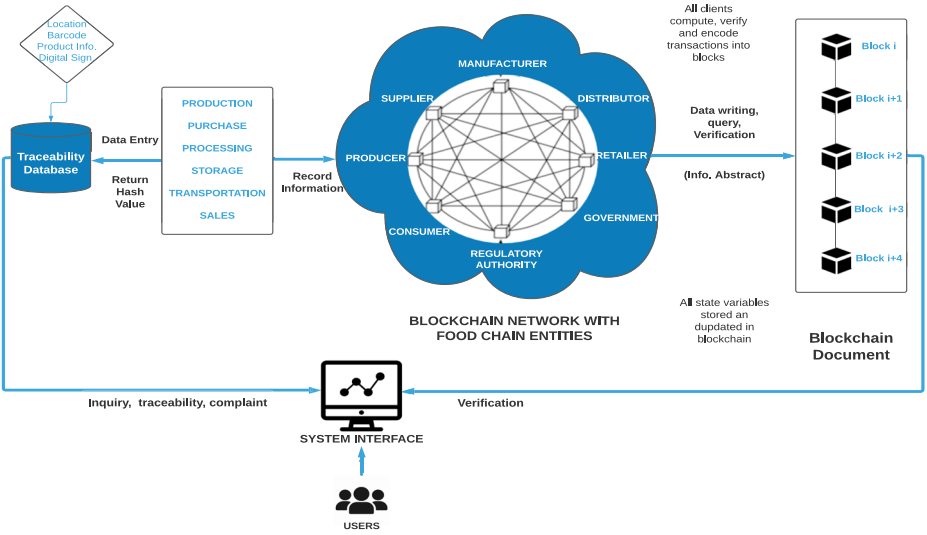

Fig. 6 FSTS network architecture using blockchain

- The smart contracts are used to examine the safety conditions, food quality, and data format. The analyzed data is measured as a digital abstract and transmitted over the P2P network. After checking, the data information is transferred to the trading pool for verification before packaging. The sender's private key and both parties need to reach a consensus for signing the transaction information. In the blockchain network, the transaction data is validated by each node in the system. Finally, the transaction information is placed in the blockchain.
- After saving the necessary details in the block, it still needs to be verified through each node in the system. In the blockchain, the verified block is linked in chronological order. After that, the blockchain technology returns the identical hash value for the entered detailed data information. The returned value is a query index to validate whether the information stored has been altered or not. In conclusion, every data and index is saved in the traceability database guaranteeing that the stored data is not modified.

3.4 Layered architecture of FSTS

The architecture of FSTS based on blockchain consists mainly of three layers, as shown in Fig. 7. The function of each layer is defined below:

1) Data gathering layer: This layer is mainly responsible for collecting operational data. This layer included data sources that are used for tracking and security purpose. In this layer, multiple sources (entities) provide operational data. The following entities reside on the data gathering layer and produce the operational data.

   - Production: Operator, production base, quantity, implementation time, variety, medication, inspector, inspection date, environment, planting enterprise, certificate number.
   - Purchase: quantity, unit, variety, environment, the purchaser

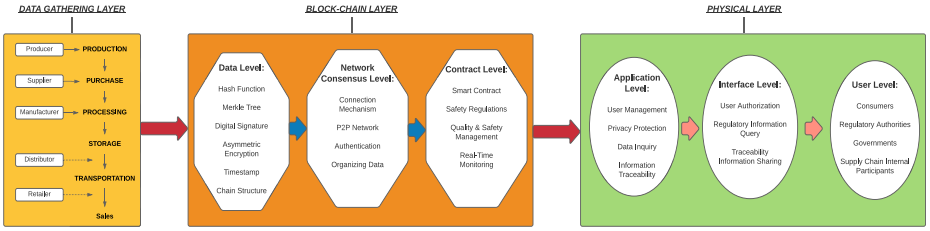

Fig. 7 FSTS layered architecture

- Processing: processing process, date, operator, batch quantity, processing enterprise, ingredient.
- Storage: quality grade, operator, storage environment, specification quantity, shelf life.
- Transportation: GPS information, transporter, distribution enterprise, transport vehicle, arrival time, receiving enterprise, weight, consignee, quantity, environment.
- Sales: sales status, shelf time, salesperson, purchase time, environment, sales method.

2) Blockchain Layer: The blockchain layer mainly contains the smart contract, transactional hash data, and consensus mechanisms.

- Data level: It comprises blockchain data like hash function, Merkle tree value, chain structure, and many more. All the timestamped blocks are connected in a chain. The information stored in blocks cannot be tampered or altered by unauthorized parties.
- Network consensus level: It executes the Consensus and data verification which assures the data verification and validity.
- Contract level: At the smart contract level, the agriculture management and safety regulations are embedded to determine the human mismatch activities. The smart contract will help to develop standard management rules and protocols.

3) Physical Layer: The physical layer includes the application level, interface level, and user level. The interface and application levels provide the corresponding permissions or interfaces for different users according to users needs. This shows the essential data information. The user level illustrates organizations and individuals like supply chain consumers, internal participants, governments, and regulatory authorities.

4 Blockchain solutions for FSTS

There are many solutions proposed for FSTS using blockchain [3, 78, 81, 82, 123, 156, 158, 163]. A detailed comparison of the existing solutions are presented in Table 3.

In [141], a Chinese FSTS that uses blockchain and RFID technology was discussed. The RFID helps in data collection, tracking, and monitoring and blockchain ensures a secure and decentralized framework. The main challenges of this system are the high cost of RFID and the scale of the newly emerging blockchain. Biswas et al. [14] defined an FSTS for wine supply. It was built on blockchain technology to eradicate fraud, adulteration, and

Table 3 A comparative analysis of the previous works with the present work

Paper	Year	Working environment	Aim of the work	Proposed approach	Blockchain technology
Tian et al. [141]	2016	FSTS for agri-food supply chain in China	Establish decentralized, reliable system and efficient data tracking	Implemented using Blockchain and RFID tags	
Biswas et al. [14]	2017	Wine supply chain traceability system	To enhance transparency, security & traceability in wine supply chain	Using blockchain where transactions are stored in immutable blocks	Private blockchain implemented in Multichain named "Multichain WSC"
Tian et al. [142]	2017	Supply Chain Traceability System for Food Safety	Build reliable, decentralized system to deliver real-time data to all the system entities	Developed using blockchain, RFID, HACCP, and BigChainDB database	Integrated Smart contracts
Hong et al. [62]	2018	Agri-product traceability system	Develop reliable, trustworthy traceability system	Implemented using blockchain and IoT technologies like RFID tags and GPS	Integration of Consortium blockchain using HyperLedger and smart contracts.
Westerkamp et al. [153]	2018	Supply chain traceability system	Model the production process as token recipes to enhance provenance	Blockchain approach is used for modelling of the manufacturing process as digital token recipes	Smart contracts are implemented on Ethereum Virtual Machine (EVM)
Lin et al. [84]	2018	Food Traceability System	To propose a reliable and ecological system involving all entities of smart agriculture chain	Based on the blockchain, IoT, and Enterprise Resource Planning (ERP)	Implemented using a virtual Trusted Trade Blockchain Network Cloud Platform
Bordel et al. [17]	2018	Digital Food Product Traceability system	To enhance international commerce of food products	Implemented using blockchain, RFID tags, REST interfaces, Javascript and MongoDB NoSQL database	Smart contracts deployed on Ethereum blockchain
Caro et al. [22]	2018	Traceability solution for agricultural food supply chain named AgriBlockIoT	Develop decentralized secure system using two blockchain systems and perform comparison among theme	AgriBlockIoT: Integrating blockchain and IoT sensor devices	Implemented on Ethereum and HyperLedger Sawtooth platform
Suzuki et al. [136]	2018	Food Supply Chain Management System for Product History	To trace history of products in food supply chain	Implemented using blockchain, IC cards and NFC tagged QR codes	Private blockchain with own PoP concept
Hayati et al. [58]	2018	Traceability System in Food Supply Chain	To build an integrated, decentralized, reliable system to track supply chain	FoodTrail Blockchain: Blockchain-based system with four abstractions layers	Implemented on Hyperledger Sawtooth, uses PoET consensus and depth-first search algorithm for tracing

Table 3 (continued)

Paper	Year	Working environment	Aim of the work	Proposed approach	Blockchain technology
Leng et al. [79]	2018	Agricultural supply chain system	To achieve matching mechanism & adaptive rent-seeking for public service platforms	Based on the public blockchain and dual chain	Using smart contracts and algorithms based on PoS
Huang et al. [64]	2019	Food Supply Chain Traceability Scheme	To ensure food safety, traceability & eliminate data explosion	Integration of blockchain with EPC and IPFS technology	Using Ethereum blockchain and smart contracts for trading on-chain data
Lin et al. [85]	2019	Food Safety Traceability System	To prevent food safety issues, data tampering and data explosion	Integrating blockchain with EPCIS technology	Using Ethereum Geth 1.8.2 platform & smart contract designed by Solidity language
Tsang et al. [143]	2019	Food traceability system	To track food supply chain and ensure food quality	Blockchain, IoT, fuzzy logic for food traceability system	Smart contracts and Proof of Supply Chain Share (PoSCS) consensus algorithm
Wang et al. [149]	2019	Product traceability system	Ensure entity reliability, maintain transaction history & decentralization	Decentralized application developed using blockchain & HTML, CSS, Javascript for web interface	Smart contracts for transaction update, product registration, batch addition and Truffle Ethereum framework
Surasak et al. [135]	2019	Thai agriculture products traceability system	To strengthen the security, transparency and data integrity	Implemented using Blockchain, IoT sensors, OurSQL database	PoW consensus algorithm is used
George et al. [49]	2019	FSTS prototype for restaurants	Enhance traceability and grade food based on identifiers for quality consumption	Achieved using blockchain and FQI algorithm to measure food quality	Implemented using Permissioned blockchain
Salah et al. [120]	2019	Soybean traceability system	To efficiently track and trace soybean across agriculture supply chain	With the use of blockchain technology for transactions and IPFS for storage	EVM is used to execute smart contracts
Baralla et al. [10]	2019	Agri-food supply chain traceability system	Integrate current “farm to fork” model for European Union countries	Achieved Using blockchain, REST APIs, QR code technology, user stories, and UML for agile model	Uses smart contract called transaction processors and Hyperledger Sawtooth framework
Gao et al. [45]	2019	Food supply chain trading & traceability System	To build a system that traces the real food source along the supply chain	Integrating blockchain with CouchDB, RESTful APIs & HTTP server	Using Hyperledger fabric with three smart contracts: storage, trading, and traceable

Table 3 (continued)

Paper	Year	Working environment	Aim of the work	Proposed approach	Blockchain technology
Shahid et al. [124]	2020	FSTS for agriculture and food items	To sustain the trustworthiness of the supply chain entities & the quality of the food products	Developed using blockchain & IPFS to maintain transactions	Smart contracts: Registration Contract, Add to Lot Contract & Add Transaction Contract, deployed on Ethereum testnet "Rinkeyby"
Hao et al. [57]	2020	Food Safety Risk Traceability	Build distributed and non-tamperable model for food safety risks	Combination of blockchain and visualization technology	Based on Hyperledger Fabric and heat maps for visualization
Prashar et al. [116]	2020	Traceability and Visibility system for agricultural products	Perform real-time monitoring of food supply chain	Implemented using blockchain as a base layer, IPFS file system & AWS for testing	Smart contracts based on Ethereum and Istanbul Byzantine Fault-Tolerant algorithm
Lin et al. [83]	2020	Food supply chain system	Propose a solution for an economy post-COVID-19	Integrating blockchain with machine learning methods and AI for sales prediction	Smart contracts for uploading retailer and customer data
Zhang et al. [159]	2020	Grain supply chain safety management system	Ensure safety, make tempered proof data and traceability in grain supply chain	Implemented using blockchain, EPC technology & cloud-based database	Using smart contracts on Hyperledger Sawtooth platform

harmful chemical additions. The current RFID systems do not prevent forgery, so this system deployed a private blockchain to achieve stable, open, and non-tampered wine tracing. The paper [142] proposed a decentralized FSTS based on blockchain, IoT, hazard analysis and critical control points system. The system uses real-time information for tracing with more security and transparency. This work uses the BigChainDB database to address blockchain's scalability issues. In the paper [62], the authors developed a traceability system for agri-products based on blockchain and IoT technology. The blockchain makes it decentralized and IoT makes it credible and reliable. They proposed the system structure, architecture, and lifecycle management and used consortium blockchain to reduce the operating costs between entities. Westerkamp et al. [153] proposed a decentralized FSTS based on blockchain. The system was implemented on Ethereum Virtual Machine using smart contracts. The production process is considered a token recipe. In [84], the author proposed an FSTS based on blockchain and IoT technology. It involves blockchain into a Low-power WAN IoT to make the system faster and more efficient. The IoT devices reduce human intervention and blockchain ensures protection and verification. This system creates a safe, transparent, and environmentally friendly smart agriculture system. Participants use smart contract technology to create automatic alert codes to monitor device issues. The authors of [17] proposed an FSTS based on blockchain and RFID tags, allowing only authorised users to enter in the system securely. The solution is implemented using REST API, Javascript, and the NoSQL database. Arduino hardware nodes, virtual blockchain networks, and WiFi were used to deploy the actual system prototype. The success rate was 100% with almost 1800 readers in the system. Its future scope includes developing real blockchain networks, focusing on Algorand blockchain networks, and smart contract improvements.

In [22] discussed a practically implemented FSTS based on decentralized blockchain and IoT named AgriBlockIoT. First, a classical use case was defined after the development of the system. After that, Hyperledger Sawtooth and Ethereum blockchain is implemented. The latency, cost-effectiveness, CPU load, consensus algorithm, and network usage shows Hyperledger Sawtooth has better performance than Ethereum. Suzuki et al. [136] proposed a product history management system in the food supply chain using a private blockchain, IC cards. They also use an unspent transaction output strategy for history management using the Proof of Proof (PoP) mechanism. Its practical implementation was conducted in the organic farm products market, showing the system's feasibility. The future scope includes integrating the system with IoT sensor devices to enhance data reliability. The paper [58] proposed a blockchain-based FSTS named FoodTrail Blockchain. The system uses four blockchain abstraction layers. It is implemented on Hyperledger Sawtooth with Proof of Elapsed Time consensus. This is achieved using a depth-first search algorithm. Results show that the system is distributive, immutable, and verifiable. But, sometimes, transactions are slow due to limited server capacity. Leng et al. [79] proposed an FSTS for agri-food that is based on blockchain. The system follows a dual chain architecture to utilize business resources and consensus algorithms. It uses a public blockchain with two chain structures: "transaction chain" and "user information chain". It enhances the credibility of public service platforms. Huang et al. [64] proposed an FSTS based on blockchain with Electronic Product Code Information Services (EPCIS) and InterPlanetary File System (IPFS) techniques. EPCIS encoded the data and IPFS prevented data explosion, providing a secure, transparent, and efficient system. The system is implemented using Ethereum smart contracts.

An FSTS prototype was developed using blockchain and EPCIS technology by [85]. It developed a management model that uses on-chain and off-chain data and smart contracts at the enterprise level. It solves trust, data explosion, and sensitive information leakage

problems. The paper [143] proposed an FSTS based on blockchain and IoT technology that tracks the food supply chain and ensures food quality. It deployed IoT technologies under traceable resource units (TRUs), Proof of Supply Chain Share (PoSCS) consensus algorithm, lightweight blockchain network, and fuzzy food quality assurance. Further, at the enterprise level, PoSCS is extended by integrating flows in the supply chain. In [149], a blockchain-based FSTS has been proposed to utilize smart contracts. It includes an event response mechanism to check the involved parties reliability. The event is stored in permanent logs and transaction history is stored in a distributed ledger. A decentralized system prototype is developed using the Truffle framework. They deployed and tested the framework using TestRpc. They also created a web page based on their prototype. The future scope includes the integration of IoT and QR code technology. Surasak et al. [135] developed a Thai-based agri-products traceability system using blockchain and IoT technology. The IoT technology is used for real-time data gathering. It uses the OurSQL mechanism so unauthorized parties cannot change the data. There are no block creation fees and user queries are executed efficiently. The system can also track the humidity and temperature of the product. The paper [49] proposed an FSTS for restaurants based on blockchain technology and the Food Quality Index (FQI). The FQI algorithm uses standard storage rules and regulations to generate FQI values. These values provide the quality assurance of the food. It also helps to identify the quality of food intake by consumers.

Salah et al. [120] proposed a solution based on blockchain for tracing soybean. The solution was implemented using Ethereum smart contracts and IPFS for recording and storing transactions. It alleviates the use of a centralized system and ensures traceability, transparency, and integrity of involved entities. Baralla et al. [10] developed a blockchain-based FSTS, which enhances the reliability and traceability of the European Union's current "farm to fork" model. The system is based on the Hyperledger Sawtooth blockchain framework. The customers can know the whole product history by scanning the QR code. Gao et al. [45] proposed a blockchain-based FSTS that also tracks supply chain trading among enterprises. It is implemented on HyperLedger Fabric using three smart contracts: Storage, Trading & Traceability, along with the CouchDB database and REST APIs.

In the paper [124], an end-to-end solution for agri-food supply has been proposed using blockchain. The FSTS fulfils traceability, trading, delivery, and reputation services using blockchain and Ethereum smart contracts. It ensures credibility between the entities participating in the supply chain activities. The authors in [57] proposed an FSTS based on blockchain. They also proposed visualization methods that highlight the risks and their causes. The visualisation risks are developed with the help of heat maps. The traceability analysis is performed using migration and force-oriented graphs. The authors focus on a quantitative rather than qualitative analysis to assess safety risk. In paper [116], an agricultural products traceability and visibility system has been proposed based on blockchain. The solution uses Ethereum-based smart contracts and private blockchain. The proposed system is secure, cost-efficient, transparent, and tamper-free. The solution was effective and provided 161 transactions/second. In the paper [83], the authors have discussed blockchain's basic principles and applications in the current agriculture sector. The technical aspects include consensus algorithms, data structures & cryptography. The authors reviewed and identified critical challenges like scalability, security, and integration. They also demonstrated an improved solution based on the post-COVID-19 situation, which uses Artificial Intelligence to predict retail sales. Zhang et al. [159] proposed an FSTS for grains using blockchain, EPC technology, and a cloud database. The system uses smart contracts on Hyperledger Sawtooth that combine blockchain and node databases to achieve a multimode data storage mechanism. It guarantees safe traceability and data security.

4.1 Advantages of related literature

From the above works, we have identified the following technical merits of blockchain integration in FSTS.

- The immutability, smart contracts, decentralized, transparency and data integrity features of blockchain improve the trust among different entities.
- The blockchain-based tracking system can securely track the source of various food items and assets starting from the farm.
- The blockchain plays an essential role in controlling the risk in the FSTS.
- Other technical merits include improved food safety, customer service satisfaction, fast query resolution, fulfilling customer demand, and many more.

4.2 Limitations of related literature

Much work has been done in the previous years, including blockchain and other related technologies with the FSTS. Regarding the survey article, several limitations of the related literature are tabulated in Table 1. Other limitations of the related literature are as follows:

- The blockchain integration in FSTS may slow the network functionality. Most of the article does not focus on this issue.
- The technological growth in the FSTS attracts many new types of attacks which are lightly focused on by most of the related literature.
- A common security framework applicable to all the platforms is missing in the literature. This creates interoperability, compatibility, and standardization issues.
- A lack of proper implementation knowledge is a barrier to integrating blockchain in FSTS.

5 Consensus Algorithm in blockchain-based FSTS

Consensus refers to an agreement in which all the nodes in the distributed network should agree on the proposed transaction state. Various algorithms help the nodes to reach an agreement on the transaction history. In this section, we will be reviewing some of the commonly known consensus algorithms.

- *Proof of Work (PoW)* PoW was first implemented in Bitcoin and introduced by Satoshi Nakamoto. But, now, it is used in other blockchain technology like Ethereum and Litecoin. In a blockchain network, the decentralized nodes are miners. The miners in a network try to compete and solve a cryptographic puzzle. Once a miner finds the solution, they can broadcast the block into the network. The other miners verify whether the solution is correct or not. This whole process is called mining. The main issue with PoW is that mining requires costly computing hardware and high power.
- *Proof of Stake (PoS)* PoS was first proposed by a BitcoinTalk forum in 2011. It follows the concept that a node is chosen randomly to validate the next block based on the number of coins they have [101]. The validators are chosen based on coins they fixed deposit in the network. The high fixed deposit creates a higher chance they have of becoming a validator. The validator checks all the transactions within the block are valid or not. If the transaction is valid, then it is added to the chain. They earn reward fees after successful validation. The approval of any fraudulent transaction will lose more

costs than they gain. This consensus mechanism is used in Peercoin and Nxt blockchain [111].

- *Delegated Proof of Stake (DPoS)* This consensus method is a variant and democratic version of PoS introduced in 2014 by Daniel Larimer [77]. Here, the nodes elect delegates for validating blocks in the network. The stakeholders of the network vote together for several delegates. These delegates then validate blocks and get rewards. They are assigned fixed time slots for producing new blocks in the chain. This reduces computational power consumption as only the delegates are involved in block creation. The delegates who perform malicious acts will lose credibility and be removed and replaced by a new representative. Some DPoS systems require delegates to deposit funds which will be seized if the delegates indulge in fraud. Bitshares blockchain uses this algorithm. Thus DPoS is considered fair, democratic, and efficient compared to PoW and PoS consensus.
- *Proof of Elapsed Time (PoET)* Intel introduced the PoET consensus algorithm with the main aim of developing an efficient consensus. It is low-cost and energy efficient. In this mechanism, each node in the network is assigned a random wait time. The node with the shortest waiting time will wake up first and win the block. The winning node is elected as the validator and adds the following block in the blockchain [28]. PoET is said to be like a fair lottery game where the chances of winning are equal and proper for every participant. This algorithm is mainly used in permissioned blockchain.
- *Practical Byzantine Fault Tolerant (pBFT)* pBFT was proposed in 1999 by Miguel Castro and Barbara Liskov [23]. Byzantine general's problem illustrates how a group of generals with their armies can have conflicts while deciding their next move. In terms of blockchain, a general represents a node in the network that needs to reach Consensus. The BFT feature of the system provides tolerance against faulty nodes and pBFT is an algorithm that optimizes BFT in asynchronous networks. In this mechanism, a new block is confirmed when more than 66% of the validators agree. It is faster and cheaper than PoW, but a central authority elects the validators. Hyperledger Fabric and Zilliqa currently use pBFT [134].
- *Delegated Byzantine Fault Tolerant (dBFT)* Delegated BFT is an improved version of PBFT. It was introduced by NEO Foundation and called "Ethereum of China". dBFT is an algorithm used to achieve Consensus through proxy voting. This voting system enables large-scale participation in the same way as DPoS. Proxy voting means that NEO token holder can delegate their votes to representatives that are consensus nodes. In every round, a group of nodes is selected and then use the BFT mechanism to reach a consensus. DBFT is considered suitable for permissioned blockchains with several nodes because of its scaling capability [30]. The other nodes in the network behave as ordinary nodes that can receive and verify those nodes. It is a bit complex and confusing, but one of the largest cryptocurrency exchanges Binance uses this mechanism.
- *Proof of Activity (PoAc)* PoAc was developed in 2014 [13]. The PoAc system combines PoW and PoS techniques. When the mining process begins, the system follows the PoW approach. After successfully mining the block, it switches to the PoS system. The PoW method included several miners competing against each other with high computing power to add a new block. After the block is mined, the system follows the PoS approach with the mined block containing a header and address for rewards. A group of validators is selected randomly based on header details. The validators then validate the new block. Decred (DCR) is a popular cryptocurrency that uses PoAc consensus.

- *Proof of Authority (PoAu)* This consensus algorithm is a hybrid of both PoS and BFT. It is a prominent algorithm because it offers fault tolerance and increased performance concerning typical BFT algorithms [108]. The private networks of the Ethereum blockchain platform first proposed PoAu. PoAu is a modified version of PoS where the stake is not financial; instead, the real identity and reputation of the authority are at stake. This eliminates any misuse of the blockchain network as the participant can face real-world repercussions if they indulge in fraudulent behaviour. Parity and VeChain are the blockchain implementations that use PoAu algorithms for permissioned blockchain. PoAu prioritizes availability over consistency [33].
- *Proof of Burn (PoB)* PoB was proposed in 2012 [132]. This algorithm uses distributed Consensus. It is an alternative to PoS and PoW. In PoB, the validators are selected through a random process. Then they 'burn' the native or mined cryptocurrencies such as Bitcoin. The rewards received are in the native cryptocurrency of the blockchain. They send some portion of coins to a wallet whose address is not reachable and irretrievable. This makes it impossible to spend those coins. PoB uses less hardware and energy. The rewards are based on entrepreneurial risks rather than wealth [75].
- *RAFT consensus algorithm* RAFT is a distributed consensus algorithm developed in 2014. It is an alternate solution to the Paxos algorithms [106]. It primarily focuses on the consistency of log replication and maintaining minimum failures. RAFT divides the Consensus into three essential elements: leader election, log replication and safety, and three states (leader, follower, and candidate). One leader is elected from a distributed cluster if a follower node can't reach the leader. Then, the leader becomes a candidate and a new leader selection process starts.
- *Ripple Protocol Consensus Algorithm (RCPA)* Ripple is an open-source system developed in 2014 for making transactions and reaching Consensus within the Ripple internet [121]. All the transactions are stored in a distributed ledger. In RCPA, each node votes for the nodes they trust within the network, creating a Unique Node List (UNL). Each node sends its transaction list to other validating nodes. Then each validating node needs to reach a consensus on the transaction with nodes in the UNL. If the validating node finds an identical one in its local transaction set, that transaction will get one vote. If the transaction receives more than 80% votes, the decision is finalized, and the transaction is recorded in the ledger. This protocol is efficient in terms of speed and energy.
- *Stellar Consensus Protocol (SCP)* David Mazières introduced this consensus method in 2015 [90]. SCP is a decentralized alternative to BFT in a federated Byzantine agreement system. The Stellar payment network uses it. In SCP, each validator elects a few other trusted validators listed as 'quorum slice'. These slices overlap each other to form a network-wide transaction. SCP favours safety and fault tolerance. It has low latency due to no mining process. Thus transactions get validated every few seconds. In case of fraudulent activity, the network's progress is paused until Consensus can be restored.
- *Proof of Capacity (PoC)* Dziembowski proposed this Consensus in 2013. It is also called Proof of Space or Proof of Storage [40]. PoC is based on the proof of work consensus except that instead of computation speed, storage is used. In this consensus algorithm, the miners are selected for validating a new block in the network based on the remaining storage of their hard drive space. It involves two processes: the plotting of the hard drive and the actual mining process. It is efficient against PoS and PoW. Burstcoin, SpaceMint, and Storj cryptocurrencies use this consensus mechanism.

6 Security attacks in blockchain based FSTS and its solution

The rapid evolution and digitization of FSTS and integration of blockchain technology in FSTS bring new types of attacks. The FSTS contains several emerging attacks, such as masquerade, tracing, forgery, template, malicious code, repudiation, spoofing, and botnet attacks that may damage or compromise the system. These attacks lead to serious security issues in the global food market. The most common attacks are cybersecurity, data integrity, data loss, unauthorized access, and authentication [16, 50, 80]. The digitization and internet-based device-specific features attract more attacks. The blockchain-based security solution attacker's main aim is to attack the blockchain. Once the blockchain is hacked, the FSTS is automatically hacked. Thus, some of the security attacks are directly related to attacks on blockchain. These security attacks can be used to hamper blockchain features such as P2P networks, smart contracts, Consensus, ledger, mining, and wallet. The Decentralized Autonomous Organization (DAO) hack was one of the most significant attacks due to a code bug. This leads to a loss worth 70 million dollars at the time [35]. The first hack occurred in 2011 with a loss of 25,000 Bitcoins [15]. Various vulnerabilities, like time dependency, signatures, immutable bugs, etc., can lead to significant losses [5]. These significant attacks can be possible in FSTS, resulting in financial losses and leaked sensitive data. This section analyzes all the security attacks in blockchain-based FSTS, which can be complicated and cause huge damage. Also, some of the countermeasures are addressed to prevent the system from such attacks.

- *Sybil attack:* In this attack, the attacker tries to affect the whole network by creating multiple identities/nodes, just like making various fake accounts on social media [38]. This attack hampers the security and reputation of FSTS by accessing multiple resources simultaneously using multiple active identities. These attacks affect the honest nodes, block other nodes, and lead to double-spending. This attack can be restricted using Consensus like PoW, PoS, and DPoS [137].
- *Eclipse attack:* The attacker node targets a specific user in the FSTS. The attacker tries to isolate the victim node from the FSTS network and eclipses his view of the network [60]. The attacker controls the IP addresses of the victim nodes. This can lead to double spending, a fork in the ledger, self-mining, etc. The solution for this attack is limiting the number of outgoing connections and allowing limited connections from the same IP [66].
- *Distributed Denial of Service (DDoS) attacks:* The attacker influences the network and brings down the resources and servers by sending a massive amount of traffic and requests to the FSTS node [146]. The decentralized FSTS reduced the chances of attack. Several anti-DDoS software and tools like Project Shield and Cloudflare are available to mitigate the risks of DDoS attacks.
- *51 percent attack:* 51% attack occurs when a single or group of nodes (miners) can acquire more than 50% of the hash rate of the blockchain network (PoW-based systems). Once the miners in FSTS have control, they can prevent, modify, and reverse the transactions. Also, they can prevent block validation and fork the blockchain-based FSTS network [155]. The only way of prevention is to ensure that no minor or group of miners attain more than 51% computational power of FSTS.
- *Finney attack:* This attack is a double-spending threat. In this attack, the miner or attacker mines his transaction into a block, keeps it secret, and then creates another transaction before the pre-mined block gets confirmed into the blockchain network [131]. Thus, the second transaction gets invalidated. The risks of this attack can be

reduced if the FSTS actors wait for multiple confirmations before providing the product to the users.

- *DAO attack:* The DAO hack was one of the most potent attacks in cryptocurrency history. It was launched on the Ethereum blockchain in 2016. An attacker found a loophole in the code where Ether was retrieved without updating balance when the split function was called. This loophole turned into a vulnerability. The hacker called the split function recursively to extract funds. This is called recursive call exploit [91]. The attacker was able to retrieve 3.6 million Ether worth 70 million USD.
- *Timejacking attacks:* Timejacking attacks are based on the timestamps of blocks. The attacker places nodes in the network with fake timestamps and forces the victim node to enter an alternative network. This will lead to double spending. Malicious peers can be put in the network using the Eclipse attack. This attack can be prevented by synchronized clocking, using the node's system time, not the network time, and allowing only trustworthy peers [18].
- *Selfish mining attack:* This attack is a mining pool threat. Here, instead of publishing a block immediately after its generation, a miner(s) keeps it secret and then tries to put out only selected blocks or publish all of them at once, making it the longest chain. The selfish miner has the greed of receiving more significant rewards and making others waste their resources [41]. The other miners will lose their blocks. It is possible to prevent this attack by assigning the miners randomly to the pool branches or choosing the more recent timestamp block.
- *Time dependency attack:* This attack is a vulnerability in the smart contracts-based blockchain. Most applications use a timestamp to decide on actions in the contract in the blockchain. Here, the attacker tries to influence the timestamp of transactions as the time is set according to the miner's local clock.
- *Vulnerable signature:* In FSTS, due to lack of randomness, actors use the same nonce more than once in the transactions. This may allow attackers to compute private keys. This flaw is still an open issue.

7 Discussion and open issues

An FSTS based on blockchain technology is discussed in this survey-based article. This paper provides a comprehensive overview of blockchain technology which helps to develop the FSTS system. The work's main theme starts with conceptualising FSTS using blockchain technology, followed by existing solutions for FSTS. The blockchain consensus algorithms are discussed, which makes the system achieve a common agreement. Several security attacks and their solutions were also discussed. Finally, we depicted some significant issues and challenges that could be barriers to developing blockchain-based FSTS. All the necessary information about food is stored in the blockchain. Only the authorized user can access the stored food information from the blockchain. This will ensure authentic product information and guarantee the food's quality. The FSTS typically uses smart contracts at the enterprise level to secure sensitive food data rather than conventional transaction records. The smart contracts verify the enterprise identity and protect the system from spam attacks. It will take appropriate measures to ensure food data protection. The discussed FSTS using blockchain technology provides 1) privacy protection, 2) tamper-proof ability, 3) immutability in chain data, and 4) the degree of decentralization. It also reduced the cost value of the traceability system for small and medium-scale food businesses. The literature

covered the FSTS solutions regarding trading, traceability, credibility, and distribution using the current model.

FSTS using blockchain still has problems and open issues that must be addressed in the future for improved food traceability and protection [97]. The following are some research directions where improvements are required to strengthen the FSTS.

- *Optimization of P2P network*: The knowledge about the food products in the system is an essential factor that can improve the FSTS system's efficiency. The system cannot achieve complete traceability if the network have lack details. A fragmented blockchain network can be used to solve this problem. We can split the P2P network into different fragments or regions. Each area will be able to store information about food products in various categories. Any super nodes will then be in control of these regions/areas. As a result, this will help the network's better organization and optimization.
- *Information security*: A consensus mechanism validates the reliability and transactions of the information. The scalability, security and trust are required more attention n the context of the global food chain. Thus, the system required standard security protocols to handle transactions and accessibility-related issues and provide security to consensus algorithms.
- *Optimization of consensus algorithm*: Consensus algorithms help to reach a common decision and validate the transaction FSTS. But they can slow down the data rate. As a result, it is essential to keep optimizing the consensus algorithms to increase the FSTS output and speed up the data uploading method.
- *Blockchain complexity*: A transaction in the blockchain is complex, distributed, and encrypted. It may take extra time to process the transactions compared to traditional systems like debit or cash transactions. The integration of blockchain in FSTS may degrade system efficiency. Thus, some solutions need to maintain the FSTS efficiency after integrating blockchain.
- *Concerns of identity and quality-preservation*: An active RFID tag in the food supply chain provides information about environmental features such as humidity, temperature, etc. These features measure the product's quality and lifetime and trace any information about the product at any stage [2]. It can provide real-time routing and sizing of fresh food supplies and information on biodegradable products. Such real-time information is also needed in blockchain, which is still an open issue.
- The system performance is an open challenging issue that needs to be addressed in future. The food industry contains a bulk of biodegradable products that are required proper tracing. The researcher must develop a database that supports blockchain integration in FSTS with proper tracing and lower latency.
- This is a new emerging technology with advanced features. Most people are unaware of the blockchain infrastructure. Thus, it is not fully accepted by all people. It is challenging to develop a fully supported blockchain infrastructure that meets all requirements in FSTS.
- The blockchain development required significant capital investments. The digitalization of supply chain processes requires huge infrastructure costs, knowledge, expert people, and skills. The initial set-up and maintenance costs might outweigh the benefits of FSTS.
- The compatibility and standardization of blockchain technology among different types of FSTS are important. A standard architecture that supports blockchain-based FSTS with interoperability features is needed.

8 Conclusion and future scope

FSTS is implemented using several technologies like RFID, NFC, data mining, etc. However, blockchain is integrated into these systems due to security, transparency, and immutability shortcomings. The decentralized, distributed, and transparent characteristics of blockchain help to track and authenticate food product origin and improve credibility. Some concerns about security and privacy may be overcome by including P2P architecture, consensus algorithms, and other cryptographic techniques.

In this systematic review, we have developed a conceptual framework of FSTS using blockchain technology that covers all aspects. A blockchain-based FSTS is conceptualized with a detailed explanation of its requirement, architecture, and a few associated security issues. The background of blockchain includes its architecture, technologies, entities, deployment, characteristics, and advantages. Subsequently, this survey paper presented a comparative analysis of the previous proposed works based on blockchain. The merits and demerits of the previous works are listed in mind while developing such systems. Further, we have discussed various consensus mechanisms for the system and examined possible security attacks and their solutions. At last, we have discussed some of the open issues that need to be solved in the future. However, this survey-based research study has certain limitations. Future work will investigate a common standardization and protocol for product recognition. The discussed blockchain frameworks should be further tested and empirically need to validate with accuracy. Future studies try to build a trusted FSTS in which access will be regulated based on participants' trust. In the future, technology should be focused on hardware deployment, storage space, and time complexity to execute the transactions.

Funding The authors did not receive support from any organization for the submitted work.

Data Availability We declare that all the data associated with the manuscript is mentioned in the manuscript.

Declarations

Competing interests There is no Conflict of Interest.

Ethics approval We did not use animals and Human participants in the study reported in this work.

Informed Consent For this type of study informed consent is not required.

Consent for Publication For this type of study consent for publication is not required.

References

1. AA Andryukhin (2019) Preventions in blockchain based projects. In: 2019 Phishing attacks International Conference on Engineering Technologies and Computer Science (EnT). IEEE, pp 15–19
2. Abad E, Palacio F, Nuin M, De Zarate AG, Juarros A, Gómez JM, Marco S (2009) Rfid smart tag for traceability and cold chain monitoring of foods: demonstration in an intercontinental fresh fish logistic chain. J Food Eng 93(4):394–399
3. Aldrighetti A, Canavari M, Hingley MK (2021) A delphi study on blockchain application to food traceability. Int J Food Syst Dynamics 12(1):6–18
4. Alfian G, Rhee J, Ahn H, Lee J, Farooq U, Ijaz MF, Alex Syaekhoni M (2017) Integration of rfid, wireless sensor networks, and data mining in an e-pedigree food traceability system. J Food Eng 212:65–75

5. Alkhalifah A, Ng A, Kayes A, Chowdhury J, Alazab M, Watters PA (2020) A taxonomy of blockchain threats and vulnerabilities. In: Blockchain for cybersecurity and privacy. CRC Press, pp 3–28
6. Angeles R (2005) Rfid technologies: supply-chain applications and implementation issues. Inform Syst Manag 22(1):51–65
7. Armknecht F, Bohli J-M, Karame GO, Li W (2017) Sharding pow-based blockchains via proofs of knowledge. IACR Cryptol ePrint Arch 2017:1067
8. Aydar M, Cetin SC, Ayvaz S, Aygun B (2019) Private key encryption and recovery in blockchain. arXiv:1907.04156
9. Badzar A (2016) Blockchain for securing sustainable transport contracts and supply chain transparency-an explorative study of blockchain technology in logistics
10. Baralla G, Pinna A, Corrias G (2019) Ensure traceability in european food supply chain by using a blockchain system. In: 2019 IEEE/ACM 2nd international workshop on emerging trends in software engineering for blockchain (WETSEB). IEEE, pp 40–47
11. Bartoletti M, Pompianu L (2017) An empirical analysis of smart contracts: platforms, applications, and design patterns. In: International conference on financial cryptography and data security. Springer, pp 494–509
12. Behnke K, Janssen M (2020) Boundary conditions for traceability in food supply chains using blockchain technology. Int J Inf Manag 52:101969
13. Bentov I, Lee C, Mizrahi A, Rosenfeld M (2014) Proof of activity Extending bitcoin's proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Perform Eval Rev 42(3):34–37
14. Biswas K, Muthukkumarasamy V, Tan WL (2017) Blockchain based wine supply chain traceability system. In: Future technologies conference (FTC) 2017. The science and information organization, pp 56–62
15. Bitcoin Forum (2014) Bitcoin Forum. List of major bitcoin heists, thefts, hacks, scams, and losses. https://bitcointalk.org/index.php?topic=83794. Accessed 19 July 2021
16. Boireau O (2018) Securing the blockchain against hackers. Netw Secur 2018(1):8–11
17. Bordel B, Lebigot P, Alcarria R, Robles T (2018) Digital food product traceability: using blockchain in the international commerce. In: The 2018 international conference on digital science. Springer, pp 224–231
18. Boverman A (2011) Timejacking & Bitcoin The Global Time Agreement Puzzle. Available at: http://culubas.blogspot.com/2011/05/timejacking-bitcoin_802.html. Accessed 20 Feb 2022
19. Bumblauskas D, Mann A, Dugan B, Rittmer J (2020) A blockchain use case in food distribution: do you know where your food has been? Int J Inf Manag 52:102008
20. Buterin V et al (2014) A next-generation smart contract and decentralized application platform. White paper, vol 3(37)
21. Cachin C et al (2016) Architecture of the hyperledger blockchain fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers. Chicago, IL, vol 310
22. Caro MP, Ali MS, Vecchio M, Giaffreda R (2018) Blockchain-based traceability in agri-food supply chain management: a practical implementation. In: 2018 IoT vertical and topical summit on agriculture-tuscany (IOT Tuscany). IEEE, pp 1–4
23. Castro M, Liskov B (1999) Practical byzantine fault tolerance. In: OsDI, vol 99, no. 1999, pp 173–186
24. Catarinucci L, Cuinas I, Exposito I, Colella R, Gay Fernandez JA, Tarricone L (2011) Rfid and wsns for traceability of agricultural goods from farm to fork: electromagnetic and deployment aspects on wine test-cases. In: SoftCOM 2011, 19th international conference on software, telecommunications and computer networks. IEEE, pp 1–4
25. Centers for Disease Control (2004) Prevention (CDC others outbreak of aflatoxin poisoning–eastern and central provinces, kenya, January-July 2004. MMWR. Morb Mortal Wkly Rep 53(34):790–793
26. Chen R-S, Chen CC, Yeh KC, Chen Y-C, Kuo CW et al (2008) Using rfid technology in food produce traceability. WSEAS Trans Inform Sci Appl 5(11):1551–1560
27. Chen Y-Y, Wang Y-J, Jan J-K (2014) A novel deployment of smart cold chain system using 2g-rfid-sys. J Food Eng 141:113–121
28. Chen L, Xu L, Shah N, Gao Z, Lu Y, Shi W (2017) On security analysis of proof-of-elapsed-time (poet). In: International symposium on stabilization, safety, and security of distributed systems. Springer, pp 282–297
29. Cocco L, Mannaro K, Tonelli R, Mariani L, Lodi MB, Melis A, Simone M, Fanti A (2021) A blockchain-based traceability system in agri-food sme. Case study of a traditional bakery. IEEE Access
30. Crain T, Gramoli V, Larrea M, Raynal M (2018) Dbft: efficient leaderless byzantine consensus and its application to blockchains. In: 2018 IEEE 17th international symposium on network computing and applications (NCA). IEEE, pp 1–8

31. Creydt M, Fischer M (2019) Blockchain and more-algorithm driven food traceability. Food Contr 105:45–51
32. Curran K, Millar A, Garvey CM (2012) Near field communication. Int J Electr Comput Eng 2(3):371
33. De Angelis S, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V (2018) Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain
34. Delgado-Segura S, Pérez-Solà C, Herrera-Joancomartí J, Navarro-Arribas G, Borrell J (2018) Cryptocurrency networks: a new p2p paradigm. Mob Inf Syst, vol 2018
35. Dhillon V, Metcalf D, Hooper M (2017) The dao hacked. In: Blockchain enabled applications. Springer, pp 67–78
36. Dib O, Brousmiche K-L, Durand A, Thea E, Hamida EB (2018) Consortium blockchains: overview, applications and challenges. Int J Adv Telecommun 11(1&2):51–64
37. Donet Donet JA, Pérez-Sola C, Herrera-Joancomartí J (2014) The bitcoin p2p network. In: International conference on financial cryptography and data security. Springer, pp 87–102
38. Douceur JR (2002) The sybil attack. In: International workshop on peer-to-peer systems. Springer, pp 251–260
39. Du M, Ma X, Zhe Z, Xiangwei W, Qijun C (2017) A review on consensus algorithm of blockchain. In: 2017 IEEE international conference on systems, man, and cybernetics (SMC). IEEE, pp 2567–2572
40. Dziembowski S, Faust S, Kolmogorov V, Pietrzak K (2015) Proofs of space. In: Annual cryptology conference. Springer, pp 585–605
41. Eyal I, Sirer EG (2014) Majority is not enough: bitcoin mining is vulnerable. In: International conference on financial cryptography and data security. Springer, pp 436–454
42. Feng J, Fu Z, Wang Z, Xu M, Zhang X (2013) Development and evaluation on a rfid-based traceability system for cattle/beef quality safety in china. Food Contr 31(2):314–325
43. Feng H, Wang X, Duan Y, Zhang J, Zhang X (2020) Applying blockchain technology to improve agri-food: traceability a review of development methods, benefits and challenges. J Clean Prod 260:121031
44. Galvez JF, Mejuto JC, Simal-Gandara J (2018) Future challenges on the use of blockchain for food traceability analysis. TrAC Trends Anal Chem 107:222–232
45. Gao K, Liu Y, Xu H, Han T (2019) Hyper-ftt: a food supply-chain trading and traceability system based on hyperledger fabric. In: International conference on blockchain and trustworthy systems. Springer, pp 648–661
46. Garaus M, Treiblmaier H (2021) The influence of blockchain-based food traceability on retailer choice: the mediating role of trust. Food Contr:108082
47. Gaurav A, Psannis K, Peraković D (2022) Security of cloud-based medical internet of things (miots): a survey. Int J Softw Sci Computat Intell (IJSSCI) 14(1):1–16
48. Gelpí E, De la Paz MP, Terracini B, Abaitua I, Gómez De la Cámara A, Kilbourne EM, Bénoit Nemery CL, Philen RM, Soldevilla L (2002) The spanish toxic oil syndrome 20 years after its onset: a multidisciplinary review of scientific knowledge. Environ Health Perspectives 110(5):457–464
49. George RV, Harsh HO, Ray P, Babu AK (2019) Food quality traceability prototype for restaurants using blockchain and food quality data index. J Clean Prod 240:118021
50. Ghosh A, Gupta S, Dua A, Kumar N (2020) Security of cryptocurrencies in blockchain technology state-of-art, challenges and future prospects. J Netw Comput Appl 163:102635
51. Gould LH, Demma L, Jones TF, Hurd S, Vugia DJ, Smith K, Shiferaw B, Segler S, Palmer A, Zansky S et al (2009) Hemolytic uremic syndrome and death in persons with escherichia coli o157: H7 infection, foodborne diseases active surveillance network sites, 2000–2006. Clin Infect Dis 49(10):1480–1485
52. Greenspan G (2015) Multichain private blockchain-white paper. http://www.multichain.com/download/MultiChain-White-Paper.pdf. Accessed 10 March 2022
53. Greenwood MR (1985) Methylmercury poisoning in iraq. an epidemiological study of the 1971—1972 outbreak. J Appl Toxicology 5(3):148–159
54. Gupta N (2020) Security and privacy issues of blockchain technology. In: Advanced applications of blockchain technology. Springer, pp 207–226
55. Gupta BB, Li K-C, Leung VC, Psannis KE, Yamaguchi S et al (2021) Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. IEEE/CAA J Automatica Sinica 8(12):1877–1890
56. Halpin H, Piekarska M (2017) Introduction to security and privacy on the blockchain. In: 2017 Introduction to IEEE european symposium on security and privacy workshops (euros&PW). IEEE, pp 1–3
57. Hao Z, Mao D, Zhang B, Zuo M, Zhao Z (2020) A novel visual analysis method of food safety risk traceability based on blockchain. Int J Environ Res Public Health 17(7):2300

58. Hayati H, Baskara Nugraha IGB (2018) Blockchain based traceability system in food supply chain. In: 2018 International seminar on research of information technology and intelligent systems (ISRITI). IEEE, pp 120–125
59. Hearn M (2016) Corda: a distributed ledger. Corda Tech White Paper, vol 2016
60. Heilman E, Kendler A, Zohar A, Goldberg S (2015) Eclipse attacks on bitcoin's peer-to-peer network. In: 24th {$USENIX$}, security symposium ({$USENIX$} security, vol 15), pp 129–144
61. Hewa T, Ylianttila M, Liyanage M (2020) Survey on blockchain based smart contracts: applications, opportunities and challenges. J Netw Comput Appl:102857
62. Hong W, Cai Y, Yu Z, Yu X (2018) An agri-product traceability system based on iot and blockchain technology. In: 2018 1st IEEE international conference on hot information-centric networking (HotICN). IEEE, pp 254–255
63. Hu Y, liyanage M, Mansoor A, Thilakarathna K, Jourjon G, Seneviratne A (2018) Blockchain-based smart contracts-applications and challenges. arXiv:1810.04699
64. Huang H, Zhou X, Liu J (2019) Food supply chain traceability scheme based on blockchain and epc technology. In: International conference on smart blockchain. Springer, pp 32–42
65. Huynh TT, Nguyen TD, Tan H (2019) A survey on security and privacy issues of blockchain technology. In: 2019 International conference on system science and engineering (ICSSE). IEEE, pp 362–367
66. Ismail H, Germanus D, Suri N (2015) Detecting and mitigating p2p eclipse attacks. In: 2015 IEEE 21st ICPADS). IEEE, pp 224–231
67. Jaoude JA, Saade RG (2019) Blockchain applications–usage in different domains. IEEE Access 7:45360–45381
68. Ji Q, Bouri E, Kristoufek L, Lucey B (2019) Realised volatility connectedness among bitcoin exchange markets. Fin Res Lett, p 101391
69. Jones P, Clarke-Hill C, Shears P, Comfort D, Hillier D (2004) Radio frequency identification in the uk: opportunities and challenges. Int J Retail Distrib Manag
70. Joshi AP, Han M, Wang Y (2018) A survey on security and privacy issues of blockchain technology. Math Found Comput 1(2):121
71. Juan Y, Fang T, Cheng Z (2021) A food safety traceability system based on blockchain. Modern Industr IoT Big Data Supply Chain Proc IIoTBDSC 2020(218):313
72. Kamath R (2018) Food traceability on blockchain: walmart's pork and mango pilots with ibm. J British Blockchain Assoc 1(1):3712
73. Kamble SS, Gunasekaran A, Sharma R (2020) Modeling the blockchain enabled traceability in agriculture supply chain. Int J Inf Manag 52:101967
74. Karame G, Capkun S (2018) Blockchain security and privacy. IEEE Secur Privacy 16(04):11–12
75. Karantias K, Kiayias A, Zindros D (2020) Proof-of-burn. In: International conference on financial cryptography and data security. Springer, pp 523–540
76. Lai R, Kuo Chuen DL (2018) Blockchain–from public to private. In: Handbook of blockchain, digital finance, and inclusion. Elsevier, vol 2, pp 145–177
77. Larimer D (2014) Delegated proof-of-stake (dpos). Bitshare Whitepaper 81:85
78. Lee M-J, Luo J-T, Shao J-J, Huang N-F (2021) A trustworthy food resume traceability system based on blockchain technology. In: 2021 International conference on information networking (ICOIN). IEEE, pp 546–552
79. Leng K, Bi Y, Jing L, Fu H-C, Nieuwenhuyse IV (2018) Research on agricultural supply chain system with double chain architecture based on blockchain technology. Futur Gener Comput Syst 86:641–649
80. Li X, Jiang P, Chen T, Luo X, Wen Q (2020) A survey on the security of blockchain systems. Futur Gener Comput Syst 107:841–853
81. Li S, Qin D, Wu X, Li J, Li B, Han W (2022) False alert detection based on deep learning and machine learning. Int J Semantic Web and Inform Syst (IJSWIS) 18(1):1–21
82. Li Z, Wu H, King B, Miled ZB, Wassick J, Tazelaar J (2018) A hybrid blockchain ledger for supply chain visibility. In: 2018 17th International symposium on parallel and distributed computing (ISPDC). IEEE, pp 118–125
83. Lin W, Huang X, Fang H, Wang V, Hua Y, Wang J, Yin H, Yi D, Yau L (2020) Blockchain technology in current agricultural systems: from techniques to applications. IEEE Access 8:143920–143937
84. Lin J, Shen Z, Zhang A, Chai Y (2018) Blockchain and iot based food traceability system. Int J Inf Technol 24(1):1–16
85. Lin Q, Wang H, Pei X, Wang J (2019) Food safety traceability system based on blockchain and epcis. IEEE Access 7:20698–20707
86. Liu X, Wang W, Niyato D, Zhao N, Wang P (2018) Evolutionary game for mining pool selection in blockchain networks. IEEE Wireless Commun Lett 7(5):760–763

87. Lu J, Shen J, Vijayakumar P, Gupta BB (2021) Blockchain-based secure data storage protocol for sensors in the industrial internet of things. IEEE Trans Industr Inform 18(8):5422–5431
88. Mainetti L, Patrono L, Stefanizzi ML, Vergallo R (2013) An innovative and low-cost gapless traceability system of fresh vegetable products using rf technologies and epcglobal standard. Comput Electr Agriculture 98:146–157
89. Maull R, Godsiff P, Mulligan C, Brown A, Kewell B (2017) Distributed ledger technology: applications and implications. Strateg Chang 26(5):481–489
90. Mazieres D (2015) The stellar consensus protocol: a federated model for internet-level consensus. Stellar Dev Foundation, vol 32
91. Mehar MI, Shier CL, Giambattista A, Gong E, Fletcher G, Sanayhie R, Kim HM, Laskowski M (2019) Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack. J Cases Inform Technol (JCIT) 21(1):19–32
92. Mercer R (2016) Privacy on the blockchain: unique ring signatures. arXiv:1612.01188
93. Meyer R, Candrian U (1996) Pcr-based dna analysis for the identification and characterization of food components. LWT-Food Sci Technol 29(1-2):1–9
94. Mohan T (2018) Improve food supply chain traceability using blockchain pennsylvania state university
95. Mohanta BK, Jena D, Panda SS, Sobhanayak S (2019) Blockchain technology: a survey on applications and security privacy challenges. Internet Things 8:100107
96. Mohsen Attaran (2007) Rfid: an enabler of supply chain operations. Supply Chain Manag Int J
97. Monrat AA, Schelén O, Andersson K (2019) A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access 7:117134–117151
98. Montet D, Dey G (2017) History of food traceability. In: Food traceability and authenticity, pp 1–30. CRC Press
99. Nakamoto S, Bitcoin A (2008) A peer-to-peer electronic cash system. Bitcoin. https://bitcoin.org/bitcoin.pdf, vol 4
100. Ngai EWT, Cheng TCE, Au S, Lai K-H (2007) Mobile commerce integrated with rfid technology in a container depot. Decis Support Syst 43(1):62–76
101. Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E (2019) Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access 7:85727–85745
102. Nguyen GN, Viet NHL, Elhoseny M, Shankar K, Gupta BB, El-Latif AAA (2021) Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with resnet model. J Parallel Distrib Comput 153:150–160
103. Northcutt JK, Parisi MA (2013) Major food laws and regulations. Guide US food laws and regulations Chishester: Wiley Blackwell:73–96
104. Oksiiuk O, Dmyrieva I (2020) Security and privacy issues of blockchain technology. In: 2020 IEEE 15th international conference on advanced trends in radioelectronics, telecommunications and computer engineering (TCSET). IEEE, pp 1–5
105. Olsen P, Borit M (2013) How to define traceability. Trends Food Sci Technol 29(2):142–150
106. Ongaro D, Ousterhout J (2014) In search of an understandable consensus algorithm. In: 2014 $\{USENIX\}$, Annual Technical Conference ($\{USENIX\}\{ATC\}$ 14), pp 305–319
107. Ortea I, Gallardo JM (2015) Investigation of production method, geographical origin and species authentication in commercially relevant shrimps using stable isotope ratio and/or multi-element analyses combined with chemometrics An exploratory analysis. Food Chem 170:145–153
108. POA Network (2017) Proof of authority: consensus model with identity at stake
109. Parzefall W (2002) Risk assessment of dioxin contamination in human food. Food Chem Toxicol 40(8):1185–1189
110. Patelli N, Mandrioli M (2020) Blockchain technology and traceability in the agrifood industry. J Food Sci 85(11):3670–3678
111. Peercoin (2014) Introduction to Peercoin. https://www.peercoin.net/docs/overview. Accessed 29 Aug 2021
112. Pei X, Tandon A, Alldrick A, Giorgi L, Huang W, Yang R (2011) The china melamine milk scandal and its implications for food safety regulation. Forest Ecol Manage 36(3):412–420
113. Pigini D, Conti M (2017) Nfc-based traceability in the food chain. Sustainability 9(10):1910
114. Podio NS, Baroni MV, Badini RG, Inga M, Ostera HA, Cagnoni M, Gautier EA, García PP, Hoogewerff J, Wunderlin DA (2013) Elemental and isotopic fingerprint of argentinean wheat. Matching soil, water, and crop composition to differentiate provenance. J Agricultural Food Chem 61(16):3763–3773. PMID: 23531021

115. Pongnumkul S, Siripanpornchana C, Thajchayapong S (2017) Performance analysis of private blockchain platforms in varying workloads. In: 2017 26th International conference on computer communication and networks (ICCCN). IEEE, pp 1–6
116. Prashar D, Jha N, Jha S, Lee Y, Joshi GP (2020) Blockchain-based traceability and visibility for agricultural products: a decentralized way of ensuring food safety in india. Sustainability 12(8):3497
117. Queiroz MM, Wamba SF (2019) Blockchain adoption challenges in supply chain: a empirical investigation of the main drivers in india and the usa. Int J Inf Manag 46:70–82
118. Quinn B, Butler S, Smithers R, Guardian T (2016) Mars recalls chocolate bars in 55 countries after plastic found in product. The Guardian
119. Ray PP, Dash D, Salah K, Kumar N (2020) Blockchain for iot-based healthcare: background, consensus, platforms, and use cases. IEEE Syst J
120. Salah K, Nizamuddin N, Jayaraman R, Omar M (2019) Blockchain-based soybean traceability in agricultural supply chain. IEEE Access 7:73295–73305
121. Schwartz D, Youngs N, Britto A et al (2014) The ripple protocol consensus algorithm. Ripple Labs Inc White Paper 5(8):151
122. Sforza S, Corradini R, Tedeschi T, Marchelli R (2011) Food analysis and food authentication by peptide nucleic acid (pna)-based technologies. Chem Soc Rev 40(1):221–232
123. Shahbazi Z, Byun Y-C (2021) A procedure for tracing supply chains for perishable food based on blockchain, machine learning and fuzzy logic. Electronics 10(1):41
124. Shahid A, Almogren A, Javaid N, Al-Zahrani FA, Zuair M, Alam M (2020) Blockchain-based agri-food supply chain: a complete solution. IEEE Access 8:69230–69243
125. Sharma BD, Bhatia V, Rathee M, Kumar R, Mukharjee A (2002) Epidemic dropsy: observations on pathophysiology and clinical features during the delhi epidemic of 1998. Tropical Doc 32(2):70–75
126. Sheng QZ, Zeadally S, Mitrokotsa A, Maamar Z (2011) Rfid technology, systems, and applications. J Netw Comput Appl 34:797–798
127. Shukla S, Shankar R, Singh SP (2014) Food safety regulatory model in india. Food Contr 37:401–413
128. Si C, Liu X, Yan J, Hu G, Shi Y (2020) Processes, benefits, and challenges for adoption of blockchain technologies in food supply chains: a thematic analysis. Inform Syst e-Business Manag:1–27
129. Singh A, Chatterjee K (2018) Secevs: secure electronic voting system using blockchain technology. In: 2018 International conference on computing, power and communication technologies (GUCON). IEEE, pp 863–867
130. Singh J, Michels JD (2018) Blockchain as a service (baas): providers and trust. In: 2018 IEEE european symposium on security and privacy workshops (EuroS&PW). IEEE, pp 67–74
131. Sompolinsky Y, Zohar A (2016) Bitcoin's security model revisited. arXiv:1605.09193
132. Stewart I (2012) Proof of burn - Bitcoin Wiki. Available at: https://en.bitcoin.it/wiki/Proof_of_burn
133. Sugahara K (2008) Traceability system for agricultural productsbased on rfid and mobile technology. In: International conference on computer and computing technologies in agriculture. Springer, pp 2293–2301
134. Sukhwani H, Martínez J, Chang X, Trivedi KS, Rindos A (2017) Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric). In: 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). IEEE, pp 253–255
135. Surasak T, Wattanavichean N, Preuksakarn C, Huang SC-H (2019) Thai agriculture products traceability system using blockchain and internet of things. System 14:15
136. Suzuki J, Kono M, Fujii T, Ryugo T, Sato M, Kawahara Y (2018) Food supply chain management system for product history using blockchain. In: Intelligent environments (workshops), pp 186–195
137. Swathi P, Modi C, Patel D (2019) Preventing sybil attack in blockchain using distributed behavior monitoring of miners. In: 2019 10th International conference on computing, communication and networking technologies (ICCCNT). IEEE, pp 1–6
138. Taranto PD (2016) Biomolecular identification of fish species by pcr and analysis of microbiological risk linked to the consumption of ready to eat fishery products
139. Tauxe RV (1997) Emerging foodborne diseases: an evolving public health challenge. Emerging Infect Dis 3(4):425
140. Tewari A, Gupta BB (2020) Secure timestamp-based mutual authentication protocol for iot devices using rfid tags. Int J Semantic Web Inform Syst (IJSWIS) 16(3):20–34
141. Tian F (2016) An agri-food supply chain traceability system for china based on rfid & blockchain technology. In: 2016 13th International conference on service systems and service management (ICSSSM). IEEE, pp 1–6
142. Tian F (2017) A supply chain traceability system for food safety based on haccp, blockchain & internet of things. In: 2017 International conference on service systems and service management. IEEE, pp 1–6

143. Tsang YP, Choy KL, Wu CH, Ho GTS, Lam HY (2019) Blockchain-driven iot for food traceability with an integrated consensus mechanism. IEEE Access 7:129000–129017
144. Tse D, Zhang B, Yang Y, Cheng C, Mu H (2017) Blockchain application in food supply information security. In: 2017 IEEE international conference on industrial engineering and engineering management (IEEM). IEEE, pp 1357–1361
145. Van Der Vorst JG (2006) Product traceability in food-supply chains. Accred Qual Assur 11(1):33–37
146. Vasek M, Thornton M, Moore T (2014) Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. In: International conference on financial cryptography and data security. Springer, pp 57–71
147. Vikaliana R, Raja Mohd Rasi RZ, Pujawan IN (2021) Traceability system on mangosteen supply chain management using blockchain technology: a model design. Studies Appl Econ, vol 39(4)
148. Wang M, Duan M, Zhu J (2018) Research on the security criteria of hash functions in the blockchain. In: Proceedings of the 2nd ACM workshop on blockchains, cryptocurrencies, and contracts, pp 47–55
149. Wang S, Li D, Zhang Y, Chen J (2019) Smart contract-based product traceability system in the supply chain scenario. IEEE Access 7:115122–115133
150. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang F-Y (2019) Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans Syst Man Cybern Syst 49(11):2266–2277
151. Wang L, Shen X, Li J, Shao J, Yang Y (2019) Cryptographic primitives in blockchains. J Netw Comput Appl 127:43–58
152. Weber K, Schütz AE, Fertig T, Müller NH (2020) Exploiting the human factor: social engineering attacks on cryptocurrency users. In: International conference on human-computer interaction. Springer, pp 650–668
153. Westerkamp M, Victor F, Küpper A (2018) Blockchain-based supply chain traceability: token recipes model manufacturing processes. In: 2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). IEEE, pp 1595–1602
154. Yang Z, Li X, He P (2021) A decision algorithm for selecting the design scheme for blockchain-based agricultural product traceability system in q-rung orthopair fuzzy environment. J Clean Prod 290:125191
155. Ye C, Li G, Cai H, Gu Y, Fukuda A (2018) Analysis of security in blockchain: case study in 51%-attack detecting. In: 2018 5th International conference on dependable systems and their applications (DSA). IEEE, pp 15–24
156. Yi W, Huang X, Yin H, Dai S (2021) Blockchain-based approach to achieve credible traceability of agricultural product transactions. In: Journal of physics: conference series. IOP publishing, vol 1864, p 012115
157. Zhang J, Li Z (2016) Design and development of beef and mutton quality safety traceability system based on nfc in xinjiang. J Henan Agricultural Sci 45(4):155–160
158. Zhang Y, Liu Y, Jiong Z, Zhang X, Li B, Chen E (2021) Development and assessment of blockchain-iot-based traceability system for frozen aquatic product. J Food Process Eng:e13669
159. Zhang X, Sun P, Xu J, Wang X, Yu J, Zhao Z, Dong Y (2020) Blockchain-based safety management system for the grain supply chain. IEEE Access 8:36398–36410
160. Zhang L, Yang L, Bai L, Zhang Y, You K (2017) Fresh-water fish quality traceability system based on nfc technology. In: International symposium on intelligence computation and applications. Springer, pp 204–213
161. Zhao Y, Zhang B, Chen G, Chen A, Yang S, Ye Z (2014) Recent developments in application of stable isotope analysis on agro-product authenticity and traceability. Food Chem 145:300–305
162. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData congress). IEEE, pp 557–564
163. Zheng M, Zhang S, Zhang Y, Hu B (2021) Construct food safety traceability system for people's health under the internet of things and big data. IEEE Access
164. Zheng X, Zhu Y, Si X (2019) A survey on challenges and progresses in blockchain technologies: a performance and security perspective. Appl Sci 9(22):4731
165. Zhou Z, Wang M, Ni Z, Xia Z, Gupta BB (2021) Reliable and sustainable product evaluation management system based on blockchain. IEEE Trans Eng Manag
166. Zou Y, Meng T, Zhang P, Zhang W, Li H (2020) Focus on blockchain: a comprehensive survey on academic and application. IEEE Access 8:187182–187201

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Affiliations

Ashish Singh[1] · Adnan Gutub[2] · Anand Nayyar[3] · Muhammad Khurram Khan[4]

Ashish Singh
ashishashish307@gmail.com

Adnan Gutub
aagutub@uqu.edu.sa

Muhammad Khurram Khan
mkhurram@ksu.edu.sa

1 School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, 751024, Odisha, India

2 Computer Engineering Department, Umm Al-Qura University, Makkah, Saudi Arabia

3 School of Computer Science, Duy Tan University, Da Nang, Vietnam

4 Center of Excellence in Information Assurance, College of Computer & Information Sciences, King Saud University, Riyadh, 11653, Saudi Arabia