***Review Article***

**Leveraging Blockchain for Food Safety and Traceability in the Digital Age**

**Abstract**

As organizational competition intensifies, supply chains are becoming increasingly competitive, pushing businesses to deliver greater value to their customers. Traceability has emerged as a critical indicator of operational efficiency and customer service within supply chains. This study explores the application of blockchain technology to enhance food safety by reducing contamination risks, improving recall effectiveness, and building consumer trust. The several proposed blockchain-based models enable comprehensive traceability by recording and managing all stakeholder transactions and interactions within the supply chain using smart contracts. Transactions are securely logged in a decentralized Interplanetary File System (IPFS), ensuring data integrity and tamper-proof audit trails. It is worth to mention that IPFS (Inter Planetary File System) is a decentralized storage system that allows files to be stored and shared across a network of nodes. This architecture supports a transparent, accurate, and cost-effective supply chain system. Performance evaluations of the model show a convergence differential time and a throughput of varied transactions per second, demonstrating its effectiveness in agricultural product traceability. The blockchain system utilizes a consensus algorithm to generate a nonce value during the initial collection and segregation of data from various supply chain stakeholders. This value helps determine the suitability of food items based on established storage and handling standards provided by food safety authorities. By maintaining an immutable and transparent record from farm to table, the blockchain system guarantees product authenticity, freshness, and compliance with food safety standards. This study highlights both the advantages and challenges of implementing blockchain in food supply chains and discusses its potential future developments in the digital age. The findings underscore blockchain’s capacity to create a reliable, traceable, and tamper-resistant supply chain, ultimately enhancing food quality and safety.

Key words: Blockchain, Decentralized Ledger, Digital age, Food safety, Online Food delivery.

**Introduction**

Blockchain is one of the most significant technological developments of the twenty-first century.

Initially created to support digital currencies like Bitcoin, blockchain is now being used in many different fields. At its core, blockchain is a way to securely record and share information across multiple computers, making it nearly impossible to alter or hack. This technology is important because it can make processes faster, cheaper, and more secure in areas like finance, supply chains, and healthcare. The manner that we grow, prepare, and eat food has changed dramatically in the digital age. The food sector has grown more intertwined with the advent of social media, e-commerce, and online meal delivery. Although there are many advantages to this digital revolution, like easier accessibility and convenience, there are also new difficulties in maintaining food safety. The likelihood of contamination and food borne illnesses has increased with the complexity and globalization of food production and distribution (Van de Venter, 2000).

Thus, by removing the need for middlemen and providing a trustworthy system for transactions, blockchain is changing the way we do business and handle information in today’s world and in order to improve food safety regulations and safeguard the public's health, it is imperative to make use of digital technology, data analytics, and creative solutions. A distributed database that is shared via a computer network is called a blockchain. By digitally preserving data, blockchain makes guarantee that transactions are secure (Ministry of Electronics & Information Technology, 2024). According to Toufaily *et al*. (2021), it is known as a distributed ledger technology (DLT) and is based on five fundamental principles: decentralisation, integrity, cryptography, security, and inclusivity. The rise of blockchain technology has been hailed as the next big thing that will change how companies operate, including their size and structure as well as how transactions are carried out (Behnke and Janssen, 2020). Blockchain systems allow for the storage of data that is difficult to alter, the introduction of tokens that can be transferred between parties without the need for an intermediary or trusted third party, and the automatic execution of "smart contracts" in response to predetermined conditions (Marsal-Llacuna, 2018; Janssen *et al.,* 2020). Among the many difficulties facing the global food sector are food fraud, contamination, and waste (Lal *et al.,* 2022). Blockchain technology provides a transparent, traceable, and unchangeable record of food production, processing, and distribution, which presents a revolutionary way to improve food safety. Through the use of blockchain technology, food product authenticity and quality may be guaranteed by stakeholders, lowering the possibility of contamination and enhancing public health.

**Importance of food safety**: Food safety is a fundamental human right because food is vital for survival. Unsafe food threatens billions of people worldwide, leading to millions of illnesses and hundreds of thousands of deaths each year. Numerous techniques are employed globally to measure food insecurity, including the Food Insecurity Experience Scale (FIES), which documents individual experiences of food-related problems, and the Prevalence of Undernourishment (PoU), which evaluates dietary energy deficit (FAO, 2023; Samadder *et al.,* 2025). The food supply chain spans from farm to table, encompassing microbiological, chemical, personal, and environmental hygiene issues (Fung *et al.,* 2018). Food safety is crucial to the food sector in a number of ways, including evaluating management systems, achieving certifications for specific safety and quality standards, ensuring legal compliance, and assessing the condition of premises and products. The growing consumer concern for food safety, largely driven by recent food crises, has prompted both public and private sectors to adopt various food safety standards (Kotsanopoulos et al., 2017). These guidelines are essential for safeguarding customers from common allergies and foodborne diseases such botulism, salmonellosis, listeriosis, and campylobacteriosis. Blockchain technology is significantly enhancing food safety by offering detailed and transparent tracking of food products throughout the supply chain. Blockchain provides a digital ledger that records every transaction related to a food product, from its origin to its final destination. Each time the product changes hands be it harvested, processed, packaged, or sold an entry is made in the blockchain. This record is permanent, tamper-proof, and accessible to all authorized participants in the supply chain. In the event of a food safety issue, time is critical. Traditional methods of tracing contaminated products can be slow and labor-intensive, involving paperwork and communication across multiple entities. Food fraud, such as mislabeling or counterfeiting, is a significant concern in the industry. Blockchain helps combat this by providing a secure and verifiable record of a product’s history. Blockchain also simplifies compliance with food safety regulations. It automatically logs all necessary data, such as temperature control during transportation or organic certification, making it easier for companies to prove compliance during audits. Concerns over the safety and provenance of food are growing among consumers. Blockchain allows them to verify the authenticity and safety of products before purchasing. For example, they can use a smartphone app to scan a product’s QR code and see detailed information about its source, processing, and journey. This transparency builds trust and can even become a selling point for brands that prioritize food safety.

**Food safety programs**

In order to guarantee that food is produced, handled, processed, and delivered in a way that minimises contamination and lowers the risk of foodborne illnesses, food safety programs are organised systems. These initiatives cover a variety of legislative, preventative, and remedial actions taken at every point of the food supply chain, from the farm to the table (Flynn, 2019). Motivated by the need to uphold customer confidence, adhere to legal requirements, and safeguard public health. There are some programs listed below:

Fig. 1: Food Safety Programs

HACCP: Biological, chemical, and physical risks are analysed and controlled in the HACCP management system from raw material production, procurement, and handling to manufacture, distribution, and final product consumption to ensure food safety (FDA,2022). Adopted in 1993, the Codex guidelines on the use of HACCP underwent updates in 1995, 1997, and 2003.

Safe Quality Food (SQF): A strict and reliable programme for food safety and quality is the Safe Quality Food (SQF) Programme. Ensure that food has been handled, prepared, and manufactured in accordance with the most widely accepted guidelines. Show that you are dedicated to high-quality procedures and ongoing development (NSF,2024). The food facility demonstrates its ability to handle food items in accordance with recognised industry, governmental, and SQF norms by following the SQF auditing requirements (Odugbemi, 2017).

Good Agricultural Practices (GAPs) and Good Manufacturing Practices (GAPs): The fundamental principles of Good Manufacturing Practices (GMPs) and Good Agricultural Practices (GAPs) are intended to reduce hazards to food safety at every stage of the supply chain, from production to processing and distribution. Together, GAPs and GMPs create a thorough food safety system that covers the whole food supply chain. Every step is essential to guaranteeing product safety, from the choice of raw materials and supplier qualifications to processing, packaging, and supply. Additionally, the relationship between customers and manufacturers, which is based on accountability, openness, and compliance—reinforces consumer confidence in food safety procedure.

 The food and culinary industries have to deal with a variety of challenges when it comes to food safety, from poor sanitation and unclear labeling to unskilled workers and hazardous food storage (Yen, 2024). The most prevalent food safety issues to be mindful of in the culinary scene of 2024:

 Fig. 2. Current issues in Food safety

Food borne illness: One of the most common food safety problems in the world is food contamination, which can be brought on by bacteria, parasites, viruses, or chemical compounds. Numerous food borne infections carry the risk of permanent harm or even death.

Fig. 3. Cycle of food borne illness

Risk assessment: A risk evaluation of a product or component includes risk characterization, exposure assessment, and hazard identification and characterization. This gets the reader ready to decide whether or not this substance or product merits taking legal action to prevent harm (Henson, 1999).

Fig. 4: Components of Risk assessment in Food Industry

**Food safety management**

To guarantee that food is safe for consumption, food organisations employ a thorough, methodical methodology called a Food Safety Management System (FSMS) to identify, assess, regulate, and monitor food safety threats. To efficiently manage food safety hazards and guarantee adherence to legal and regulatory requirements, FSMS unifies policies, processes, practices, and resources at all organisational levels. Individual food enterprises have diverse arrangements for their FSMS, which are subject to external inspections or audits, such as government inspections or third-party audits. Improvements must be done following an audit or inspection in order to meet the requirements set forth by these outside parties (Jacxsens *et al*., 2009; Jacxsens *et al.,* 2011).

Fig. 5: Structure of Food safety management system

Hazards: Hazards are biological, chemical, or physical agents that have a reasonable probability of causing disease or harm if they are not controlled (Lawley *et al.,*2012).

Any biological, chemical, or physical substance that can result in disease or harm when present in food is referred to as a hazard in the context of food safety (Lawley, 2015). A fundamental aspect of food safety and a need for guaranteeing food security is recognising and controlling these risks. They are mainly classified into four categories, 1.Biological, 2.Chemical, 3. Physical, and 4. Allergenic.

**Physical hazards**

Physical risks are foreign materials that could inadvertently get into food while it's being produced, processed, packaged, or handled. This could lead to choking or other injuries. Like unsafe equipment, improperly used equipment, and cutlery.

**Chemical hazards**

In the context of food safety, chemical hazards are dangerous or potentially dangerous materials that could be found in food as a result of contamination, incorrect handling, or the purposeful or inadvertent use of chemicals during the manufacturing, processing, or packaging of food. Consumers may be at significant risk for acute poisoning, chronic illnesses like cancer, and developmental or reproductive disorders as a result of these hazards.

**Biological hazards**

**Biological hazards** are microorganisms or toxins produced by microorganisms that can contaminate food and cause food borne illnesses. These are considered the most common and serious threats to food safety. For instance, humans, animals, birds, plants, bacteria, insects, and viruses (Nemmers, 2018).

**Allergens**

Food allergens are compounds that, even in minute levels, can cause severe immunological reactions in sensitive people. These substances are known as allergenic risks. For instance egg, milk etc.

Blockchain technology has significantly converted the digital geography by enhancing effectiveness, perfecting system security, and fostering invention. In moment's connected world, advancements in mobile technologies, IoT (Internet of Things), social media, data analytics, and cloud computing have contributed to smarter decision-making and stronger consumer engagement. Blockchain complements these technologies by introducing a new sublevel of transparency, trustworthiness, and decentralization. Although originally popularized through its association with Bitcoin, blockchain extends far beyond cryptocurrencies (Ahram et al., 2017). At its core, blockchain is a distributed ledger composed of a chain of data blocks. Each block contains information secured through cryptographic hash functions, timestamps, and a reference to the former block—ensuring data integrity and traceability (Crosby et al., 2016). One of blockchain’s most important features is its capability to facilitate peer-to-peer deals without the need for intermediaries. It allows for secure data storage that's resistant to tampering and supports the automatic execution of "smart contracts"—self-executing agreements triggered by predefined conditions (Marsal-Llacuna, 2018). These capabilities make blockchain a foundational technology for building more transparent and effective digital systems across various industries. A token is an asset. Although Ethereum and Bitcoin are also technically tokens, the term "token" is commonly used to describe any cryptocurrency other than those two. It's helpful to have a term to characterize the universe of other coins because Bitcoin and Ethereum are by far the two largest cryptocurrencies (Coinbase, 2024).

The seminal study "New Directions in Cryptography," which was published in 1976, is where blockchain technology first emerged, laying the foundation for secure digital communication. Another significant influence was the conception of "electronic cash" or "digital currency," introduced through a model developed by David Chaum. This idea evolved further in 1997 when Adam Back introduced "Hashcash," a system originally designed to combat email spam by taking proof-of-work, which would later become integral to blockchain protocols. Building on these early inventions, Wei Dai proposed the conception of "b-money," which envisaged the creation of digital currency through a decentralized, peer-to-peer network—an idea that explosively influenced future developments. Still, blockchain technology as we know it today is widely attributed to the pseudonymous creator Satoshi Nakamoto, who published the Bitcoin white paper in 2008. This marked the dawn of a new era in digital finance. Bitcoin's rise captured global attention, and by 2013, investors began heavily funding startups in the cryptocurrency space. The innovation continued with the launch of Ethereum in 2015, a platform that expanded the functionality of blockchain by enabling decentralized applications and smart contracts. These contracts assured the automatic fulfillment of agreements between parties, offering a faster, more secure, and efficient system. Ethereum’s innovation played a pivotal part in mainstreaming blockchain technology across various industries (Sarmah, 2018).

Fig. 6: History of Blockchain technology Development

Block chain technology made-up of total 7 components.

Fig. 7: Seven main components of Blockchain Technology

Node: Record of every transaction. It is of 2 types.

1.Complete Node, it keeps an entire record of every transaction. It is able to verify, approve, and decline transactions and 2. Partial Node, because it doesn't keep an entire copy of the blockchain ledger, it is sometimes referred to as a Lightweight Node.

 Ledger: This digital database provides information. Since the money being transmitted between nodes is digital, or cryptocurrency, the term "digital" is used here. There are three types of ledgers. They're

a. The public ledger is transparent and accessible to anyone. Content can be written or accessed by anybody with access to the blockchain network.

b. Each node in the distributed ledger keeps a local copy of the database. In this case, multiple nodes work together to complete tasks like adding blocks to the blockchain and verifying transactions.

c. in decentralised ledger, no single node or group of nodes has central authority in this ledger. Each node takes part in carrying out the task.

Wallet: users can store their cryptocurrency in this digital wallet. In the blockchain network, a wallet is present on every node. Public and private key pairs are used in blockchain networks to protect wallet privacy. Currency conversion is not necessary while using a wallet because the money within is accepted anywhere. Wallets for cryptocurrencies mostly come in two varieties:

a. Hot Wallet, these wallets are utilised for regular online transactions that are linked to the internet. Because this wallet is linked to the internet, hackers could target it.

b.Cold Wallet, these wallets don't have an internet connection. Hackers are unable to breach its security. The user purchases these wallets. Examples are hardware wallets and paper wallets.

Nonce: A unique, randomly generated 32-bit integer called a nonce—short for "number used once"—is appended to a blockchain's hashed or encrypted block. It is essential for transaction validation and for making new blocks possible.

.

Hash: The technique of mapping data to a preset size is called hashing. In the field of cryptography, it is essential. A blockchain network uses a transaction's hash value as an input for subsequent transactions. The hash function's properties like Collision resistant, Hiding etc.

A timestamp is a brief piece of information that is uniquely serialised and saved in each block of a blockchain. This information determines when block mining started and was approved by the blockchain network. It's interesting to note that timestamps were first used in the past when people were looking for ways to track and authenticate papers.

Merkel tree: A "Merkle tree" is a type of tree data structure used for cryptocurrencies in computer science applications and cryptography. Another name for it is "Binary Hash tree." (Bosamia, *et al*., 2018). In a blockchain network, the hash of every transaction that makes up a block is known as the Merkle tree.

**Basic Principles of Blockchain:** The list of all the blockchain technologies that have been developed to date would be neither exhaustive nor comprehensive given the current complex dynamic of the blockchain's architectural evolution. Consequently, an overview of the blockchain is conducted by examining its fundamental tenets (Aste *et al.,* 2017; Tasca *et al*., 2017).

Fig 8: Principles of Blockchain technology

**Decentralisation**: Blockchain is a peer-to-peer (P2P) network where all users partake power and no single user or party controls the sale. This suggests that the chain of blocks cannot be closed, manipulated, addressed, or shut down by any one party. This blockchain network's distributed (decentralised) armature makes it impervious to fraud and hacking. Integrity: The only source of the necessary trust in the system is user suspicion, and each member of the blockchain-powered network has the authority to make judgements. Strict honesty is apparent in both the way this entire P2P network functions and how each user is compensated for their contributions. **Cryptography**: This fundamental idea of blockchain armature is to give users an extremely high degree of security and authenticity. It makes use of cryptography's strength to give nearly knit security and data integrity. While the Blockchain sale system is profitable and economic for genuine users, it can be extremely chastising on careless users. This indicates that everyone who uses the blockchain system duly and behaves well will admit fair prices. Still, you'll still face consequences if you use it inaptly.

**Security**: Because blockchain is a distributed network, there is not a single point of failure, and no careless user may jeopardise the network as a whole. A single person will be the only one harmed by any word hacking prevalence. When you use the blockchain's PKI (Public Key Infrastructure) encryption medium, your network sale is relatively safe, until you reveal your private key, for which there is not a technological solution yet. As a result, you can generally count on Blockchain technology to ensure that your deals are carried out securely. Inclusive: Everyone can share freely in the global economy without encountering prejudice thanks to the Blockchain, an inclusive technology. Bitcoin makes it possible for everyone, rich or poor, to invest as much as they can and take part in the global economy because it fully does away with the necessity for a bank account. They can choose to do business with anybody they choose and pay extremely little or no sale costs when no third party is involved.

**Distributed ledger technology**: Blockchain and other distributed ledger technologies (DLTs) provide a safe, decentralised method of conducting and documenting transactions involving digital assets. DLT is called "distributed" because copies of the ledger are shared and synchronised by numerous users (individuals, companies, etc.) within a computer network. New transactions are added in a way that is permanent, secure with cryptography, and accessible to all users almost instantly. The reason distributed ledgers don't require a central, reliable authority is that new transactions are added and validated by a consensus procedure. Because every "block" of transactions on a blockchain is cryptographically connected to the one before it, any changes would notify all other users, guaranteeing the validity of the ledger. Once users have reached a consensus over that history, they can proceed with a fresh transaction knowing exactly who is in possession of what. Distributed ledgers come in two varieties: 1. Unpermitted ledgers, which are usually public, let any participant complete a transaction. 2. Only trustworthy users can execute transactions on permissioned ledgers, which may or may not be made public (GAO, 2019).

**Smart Contracts**: The terms and conditions (T&C) of a smart contract are written in blockchain-specific programming languages like Solidity, and they're a digital agreement that's inked, saved on a blockchain network, and that runs automatically when certain criteria are met. Another way to think of smart contracts is as blockchain programs that let each party complete their portion of a sale. Smart contract-powered apps are generally called "decentralized applications," or "dapps." A set of digital commitments is defined by a smart contract (Zhang et al., 2019). Based on blockchain technology, the Ethereum system's smart contract is a program control protocol for digital currency assets (Rouhani et al., 2019). When seen from a computer's point of view, a smart contract is a member of law that deals with associated business deals and algorithms. An affiliated agreement is what the general public perceives as a smart contract. The smart contract is validated and executed automatically as soon as the preset criteria are met. In numerous other spheres of social life, including agrarian wisdom and specialized advancements, the Internet of effects, and other disciplines, smart contracts are employed in addition to fiscal deals (Wu et al., 2022).

**Consensus algorithm in blockchain technology:** The consensus technique, also referred to as the consensus mechanism, enables a network of computers, or nodes, to collaborate in order to accomplish the objective of acquiring identical copies of the distributed database files. In blockchain technology, consensus algorithms are primarily used for "Proof of Work" (PoW) and "Proof of Stakes" (PoS) (Patel et al., 2023)

**Proof of work:** Markus Jakobsson and Ari Joels coined the phrase "proof of work" in a 1999 paper. The Proof-of-Work, or PoW, consensus technique was initially employed in a blockchain network. To validate transactions and add new blocks to the chain, users trade digital tokens with one another. In order to get rewards, every miner or validator participates in this process by closely reviewing and validating every transaction on the network. All of the network's verified transactions are collected and arranged into blocks by the distributed ledger. This technique is known as mining. A method called proof of work is used to stop cyberthreats like distributed denial-of-service attacks (DDoS), which attempt to deplete computer resources by sending out a large number of bogus requests (Sheikh et al., 2018).

 **Every transaction is kept track of in a block**

(Every transaction in a blockchain system is safely stored in a digital structure known as a "block," which includes the transaction data along with a date, a unique cryptographic hash, and a reference to the block before it)

 **Each block's transactions are verified by miners**

(Before being added to the chain, a collection of transactions in each block of a blockchain system must be confirmed and certified by specialised participants called "miners.")

 **Proof-of-work problems in mathematics are solved by miners and validators.**

 (Miners solve mathematical challenges by utilising sophisticated cryptography methods)

**As the first winner to resolve a transaction running in each block, the miner/validator receives compensation.**

(The first miner or validator to successfully solve the cryptographic issue related to a block (in Proof-of-Work) or be chosen to validate transactions (in Proof-of-Work) gets compensated in blockchain networks. Usually, this payment is made in the form of transaction fees paid by users who are part of that block and/or freshly created cryptocurrency (block rewards). Participants are encouraged to donate computational resources by the incentive mechanism.)

**Eventually, verified transactions are added to the public blockchain.**

(Transactions are organised into blocks once they have been validated by miners or validators using consensus processes. The block is added to the current blockchain and cryptographically linked to the previous block once it has been verified and complies with all protocol requirements. The validated transactions become a permanent, impenetrable public record when this updated version of the blockchain is disseminated and synchronised among all nodes (computers) in the network. All participants may see the recently added transactions due to the blockchain's decentralised and transparent nature, which guarantees accountability and system confidence.)

 Fig. 9: Steps of Proof of Work

**Proof of Stake:** The PoS system allows users to mine and certify block transactions based on their stake value. The more stakes a user has, the more benefits they will receive from the system. Users must stake a certain number of tokens to be selected for validation of transaction blocks, and they will receive rewards for validating the blocks (Saad et al., 2020). PoS makes an effort to address the issue with energy expenditure that PoW caused. In order to achieve this, PoS chooses participants at random to add to the blockchain, taking the place of PoW's rival. The Follow-the-Satoshi (FTS) algorithm, the simplest PoS implementation, has each blockchain branch choose uniformly and at random from the collection of native coins (Saleh, 2021).

**Hash function in Blockchain technology**: Hash functions are sometimes referred to as message digests, fingerprints, compression functions, one-way functions, and message authentication codes (MACs) (Damanik, 2017). A mathematical function called a hash function takes input of different sizes and outputs, typically a fixed length hexadecimal. Usually, a mix of letters (a to f) and numbers (0 to 9) is used to write hash.

**Types of Blocks in Blockchain system**

 Genesis block: The initial block of a blockchain is called the "genesis block," which is appropriately titled since it implies "origin." It is possible for the blockchain to start building its history of transactions because of the genesis block. This building block allows the newly created block to be connected to an earlier state. This connection allows the blockchain to guarantee its immutability (Hanif et al., 2024; Dutta, 2021).

Valid block: All of these mined and added to the blockchain blocks are considered valid blocks. Each mined block needs network authorization in order to report as a block that has resolved the specified cryptographic problem and become a valid block. The block is uploaded to the blockchain and sent to every node after the network obtains consensus. As a result, each node in the network has a fresh block and serves as the block's verification point. These blocks permit every activity and transaction that takes place in a cryptocurrency (Zheng et al., 2018).

Orphan block: Since orphan blocks are not a part of the blockchain network, their names are also appropriate. These are typically produced by two miners mixing blocks nearly simultaneously, although an attacker with sufficient processing power may also be to blame if they want to reverse any transaction. At this stage, the network consensus process is used to decide which blocks will be orphaned and which will be validated and added to the chain. Generally speaking, the longest blockchain with the greatest number of transactions and data will be chosen. Thus, simplifying the security procedure (Sharifian et al., 2023; Dutta, 2021).

**Blockchain architecture**

A number of procedures are included in the blockchain architecture to guarantee safe and authentic transactions. The best way to conceptualize blockchain design is as a decentralized, tiered system, with each layer carrying out distinct tasks that enhance the network's overall functioning, security, and transparency. Data structures, cryptography, consensus processes, and network protocols are some of the essential layers. Fundamentally, the data structure layer arranges the blockchain as a connected series of blocks, each of which contains a list of confirmed transactions and information like a timestamp, a nonce, the hash of the previous block, a Merkle tree root, and the transaction list. Because these blocks are cryptographically linked, it is nearly hard to tamper with them without changing each block that comes after. Through hash functions like SHA-256, which create distinct digital fingerprints for every block, and public-key cryptography, which allows users to sign transactions using private keys and validate them using public keys, guaranteeing authenticity and non-repudiation, the cryptography layer provides security and integrity. Merkle trees allow for the quick and safe verification of transaction contents, which further improves data integrity. By demanding unanimity among nodes, the consensus mechanism layer ensures consistency and trust throughout the decentralised network. Typical protocols include Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), Proof of Work (PoW), where miners solve cryptographic puzzles, and Proof of Stake (PoS), where validators are chosen based on the cryptocurrency they hold. Without centralised control, these procedures guarantee equitable validation and avoid duplication of expenditure. Last but not least, the network protocol layer controls peer-to-peer (P2P) networking and node synchronisation.

**Application of block chain technology in food safety**: While blockchain technology (BCT) is primarily used for supply chain traceability in the food sector, it also plays a key role in detecting food fraud and ensuring food safety from farm to fork (Raj *et al.,* 2024). BCT enables secure, real-time sharing of critical product data—such as batch numbers, origin, certifications, and hygiene status—thereby increasing transparency and consumer trust (Galvez *et al.,* 2018). Traditional food supply chains are prone to inefficiencies and fraud due to intermediaries and poor documentation (Lierow *et al.,* 2017; Tripoli *et al.,* 2020). Technologies like RFID, NFC, and sensors help capture real-time data, which can be recorded on the blockchain through consensus and smart contracts (Epelbaum *et al*., 2014; Kamilaris *et al*., 2019). Smart contracts also enforce compliance with food safety standards, and automatically reject non-compliant products (Casino *et al*., 2020; Mao *et al*., 2018). Consumers can scan QR codes to access full product histories, boosting transparency and food safety. All stakeholders in the supply chain—from producers to retailers—act as nodes, accessing shared data without exposing private information (Kshetri *et al.,* 2018; Patel *et al.,* 2023).

**A workable method for ensuring food safety:**

The progress of information technology has made it possible to construct a blockchain-based food traceability system (Franz, 2025). Blockchain will improve transparency, food quality, and safety in addition to managing food loss, waste, and timely supply (Lal *et al*., 2024). In several countries, traceability systems have been implemented to better monitor and manage the food supply chain, both in their day-to-day operations and in cases of food safety events. These technologies allow for the tracking of food at various stages, from the farm, which is the primary producer, to the end user. To regulate the quality and safety of the whole food supply chain, these systems, however, primarily rely on a centralized structural design. A reputable company collects, stores, and oversees the full process from manufacturing to sales. Since the major company maintains the databases where the data are kept, it has the authority to add, edit, and remove data as it sees fit. Due to a small number of individuals controlling the information, the traceability system is opaque and information about product quality, safety, or processing parameters is manipulated (Fu and Ying, 2016). For instance, the blockchain technology enables the prompt recall of unsafe food items in the event that food safety issues are discovered. In fact, microbial contamination from unhygienic product handling practices and pest infestations is the primary cause of food recalls (Perboli, Musso, and Rosano, 2018).

 Major food companies like Nestlé and Carrefour have adopted blockchain to improve traceability. For instance, Nestlé partnered with OpenSC to track milk from New Zealand farms to Middle Eastern facilities, and collaborated with Carrefour to integrate Mousline Purée into the IBM Food Trust network, allowing consumers to scan product barcodes for detailed sourcing information (IBM, 2019). These initiatives aim to increase transparency, reduce food waste, and ensure quality control. IBM Food Trust highlights blockchain's ability to address key supply chain issues—such as lack of data access and delayed responses—through a secure, decentralized ledger. By facilitating permission-based data sharing, blockchain connects all stakeholders while maintaining data ownership. Nestlé’s use of both private and public blockchain systems, including OpenSC (built on Ethereum and co-founded by WWF-Australia), reflects a broader commitment to ethical, transparent supply chains (Nestlé, 2019; Sergeevic, 2023).

 Walmart has been a strong advocate of blockchain technology, using IBM’s Food Trust platform built on Hyperledger Fabric to enhance transparency in its supply chain (Sharma et al., 2021). This system allows food products to be traced back to the farmers, enabling consumers to verify product origin before purchase. IBM Food Trust is a key example of how blockchain can improve risk assessment in the food industry by providing end-to-end traceability. It allows all supply chain participants to share reliable data, helping to quickly identify hazards and manage recalls in cases of contamination or quality issues. This collaborative approach strengthens food safety by involving all stakeholders in risk mitigation.

 A typical case of blockchain application, Wuhan, China quickly emerged as the epicentre of the COVID-19 pandemic that swept the world in late 2019 (Sheth & Dattani, 2019). The Wuhan administration has acted decisively to lessen traffic in the city. At last, the outbreak is under control. On June 12, 2020, it was discovered that the employees at the Beijing Xinfadi Market were infected with COVID-19. Studies showed that salmon exposure was a factor in COVID-19 infection. During this procedure, the blockchain system records data about each customer's salmon purchase. Consequently, the authorities implemented the blockchain technology to promptly identify all afflicted individuals within the Xinfadi Market. Every step of the process is documented by the blockchain system, including the origination data for sea farming, feed purchases, distribution, processing, and retail. From farming, to processing, refrigeration, packing, and consumer delivery, every piece of salmon is equipped with an RFID tag that can automatically gather data on the salmon and upload it in real time to the blockchain (Galvez et al., 2018).

 **Blockchain in online food delivery:**

It is common knowledge that India offers a sizable population as well as tremendous development and success potential for food enterprises. Very soon, India is anticipated to hold the title of nation with the greatest GDP. Simultaneously, though, agriculture—which currently accounts for 50% of the workforce and 13.7% of India's GDP—is progressively dwindling. Concerns about food security have been under intense attention recently.

 The complex and priceless global food supply chain is essential to ensuring food security, safety, and sustainability. The industry for online meal delivery has expanded quickly in India, where major competitors like Swiggy and Zomato are transforming how people get food. One of the main causes of the rise in popularity of meal delivery services is the COVID-19 epidemic, but there are other important factors as well, such as the quick development of technology. About 65 of the 72 food testing labs run by the Food Safety and Standards Authority of India (FSSAI) were allegedly operating illegally, according to a study published in December 2017 (Ministry of Health and Family Welfare Report, Union Government, 2017). 10,500 hotels and restaurants were kicked out of the food service industry in October 2018 by well-known food companies like Zomato, Swiggy, and Food Panda because the food quality in these establishments did not meet the standards set by the Food Safety and Standards Act of 2006 (FSS Act) (FSSAI, 2020). Furthermore, these locations lacked the Indian government's fundamental food safety controller certifications. It's crucial to remember that the idea of online meal delivery is not new, and business owners looking to get into the food delivery industry face a number of obstacles pertaining to data security, transparency, and trust. Therefore, as technology advances, this constantly changing scene unquestionably needs an upgrade. Blockchain technology has become a "ultra-legend" among several businesses, capable of providing the best answers to the problems that a specific industry faces. Blockchain technology can optimize critical areas of the delivery process and improve the entire user experience by using the principles of immutability, decentralisation, and transparency (Babukuttan, 2024). Technologies based on blockchain have the potential to completely change the food delivery industry. People are no longer content when they receive a complimentary pizza delivery in less than 30 minutes. Nowadays' customers need speed and ease of use. Over the past five years, meal delivery businesses have experienced significant growth as a result of digitization. "Wooberly Eats" is one of the newest technologies available; it combines blockchain and machine intelligence. An open-source UI framework called "Flutter" is used by Wooberly to offer a number of features, such as data exchange with the customer, driver, restaurant, and system administrator. There are two categories of online meal delivery services (Yeo *et al*., 2017). The first is a restaurant-to-customer delivery company, like McDonald's or Kentucky Fried Chicken, which may provide online meal delivery services directly or via affiliate businesses. The other is a platform for delivery services used by customers, like Foodpanda, Uber Eats, and Hungrynaki. Due to erratic ordering patterns and disgruntled patrons caused by the meal delivery apps' disregard for food safety and timeliness, the restaurant's image suffers. Restaurants may use smart contracts and blockchain technology to tackle these issues, which will also be a safe way to conduct transactions. The concept is based on blockchain technology and is designed to solve a number of valid issues with current online meal delivery platforms. It facilitates bitcoin transactions, which, as was said in the study discussion, offer security and decentralisation. Every transaction is protected by smart contracts. A smart contract is a computer program that regulates data transfers according to preset guidelines. No one, not even the administrator, can alter the data stored in Blockchain thanks to smart contract management. Smart contracts are implemented using known ledgers and protocols. For the reasons mentioned above, blockchain-based systems are more secure than conventional database-based applications (Talukde *et al*., 2022).

**CONCLUSION**

Using blockchain technology to identify food safety risk points in real time can improve the recall procedure for affected product batches and reduce food fraud and contamination. Though it has some demerits but technology has an inherent ability to evolve and overcome obstacles, paving the way for a brighter future for blockchain adoption. This study advances knowledge, practice, and research on blockchain applications in food safety control by offering a thorough analysis of the technology's uses in this area. Food safety concerns can be addressed with the aid of blockchain technology, but putting this promise into action would involve overcoming a number of significant roadblocks and difficulties. Nonetheless, using blockchain technology to regulate food safety is promising. This study does, however, have certain limitations and is based on a review of the literature. The suggested rules and framework should be further evaluated and validated as they are based on existing literature. The recommendations made here are supported by the literature and need more research. This constraint offers opportunities for further study and application in the future.

**DISCLAIMER (ARTIFICIAL INTELLIGENCE)**

The authors hereby state that no generative AI tools, including text-to-image generators and large language models (ChatGPT, COPILOT, etc.), were utilised in the creation or editing of this work.

**CONSENT**

Prior to their participation in the study, each subject gave their informed consent. Over the course of the study, participants were guaranteed anonymity and confidentiality, and participation was entirely voluntary.

**ACKNOWLEDGEMENTS**

Sincere thanks are extended by the authors to all the academics and researchers whose work has advanced our knowledge of blockchain technology in the food supply chain. Their insightful information, case studies, and data have greatly influenced the direction of this review.

**COMPETING INTERESTS**
The authors have stated that there are no conflicting interests.

**References**

A. Kamilaris, A. Fonts, F.X. Prenafeta-Boldύ, The rise of blockchain technology in agriculture and food supply chains, Trends Food Sci. Technol. 91 (2019) 640–652

Adams, R.; Kewell, B.; Parry, G. Blockchain for Good? Digital Ledger Technology and Sustainable Development Goals. In *Handbook of Sustainability and Social Science Research*; Leal Filho, W., Marans, R.W., Callewaert, J., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 127–140. ISBN 978-3-319-67121-5. [[Google Scholar](https://scholar.google.com/scholar_lookup?title=Blockchain+for+Good?+Digital+Ledger+Technology+and+Sustainable+Development+Goals&author=Adams,+R.&author=Kewell,+B.&author=Parry,+G.&publication_year=2018&pages=127%E2%80%93140)]

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)* (pp. 137-141). IEEE.

Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.".

Antonopoulos, A.M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*; O’Reilly Media, Inc.: Newton, MA, USA, 2014. [[Google Scholar](https://scholar.google.com/scholar_lookup?title=Mastering+Bitcoin:+Unlocking+Digital+Cryptocurrencies&author=Antonopoulos,+A.M.&publication_year=2014)]

Aste T., P. Tasca, and T. di Matteo, Computer, 50, 18 (2017)

B. S. Riza, “Blockchain Dalam Pendidikan: Lapisan Logis di Bawahnya,” ADI Bisnis Digit. Interdisiplin J., vol. 1, no. 1, pp. 41–47, 2020

Babukuttan,A.(2024). How blockchain Integration transformation online food delivery scripts?. Medium. Stable URL: [https://medium.com/@aparnababukuttan/how-can-blockchain-integration-transform-online-food-delivery-scripts-cb5cf6d8d5b0#:~:text=From%20order%20placement%20to%20delivery,enhancing%20the%20overall%20user%20experience](https://medium.com/%40aparnababukuttan/how-can-blockchain-integration-transform-online-food-delivery-scripts-cb5cf6d8d5b0#:~:text=From%20order%20placement%20to%20delivery,enhancing%20the%20overall%20user%20experience).

Behnke, K., & Janssen, M. F. W. H. A. (2020). Boundary conditions for traceability in food supply chains using blockchain technology. *International Journal of Information Management*, *52*, 101969.

Bihn, E. A., & Gravani, R. B. (2006). Role of good agricultural practices in fruit and vegetable safety. *Microbiology of fresh produce*, 21-53.Blockchain & Distributed ledger technology .(2019). GAO. U.S

Bosamia, M., & Patel, D. (2018). Current trends and future implementation possibilities of the Merkel tree. *International Journal of Computer Sciences and Engineering*, *6*(8), 294-301.

Coinbase,2024. Stable URL: <https://www.coinbase.com/learn/crypto-basics/what-is-a-token>

Components of block chain.(2022). Geeks for geeks. Stable URL: <https://www.geeksforgeeks.org/components-of-blockchain-network/>

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied innovation*, *2*(6-10), 71.

D. Mao, F. Wang, Z. Hao, H. Li, Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain, Int. J. Environ. Res. Publ. Health 15 (8) (2018) 1627.

Dutta. B. (2021). 3 Types of Block in a Blockchain Network. Analytic steps.

F. Casino, V. Kanakaris, T.K. Dasaklis, S. Moschuris, S. Stachtiaris, M. Pagoni, N.P. Rachaniotis, Blockchain-based food supply chain traceability: a case study in the dairy sector, Int. J. Prod. Res. (2020) 1–13

F. Tian, 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, 2017, pp. 1–6.

F.M.B. Epelbaum, M.G. Martinez, The technological evolution of food traceability systems and their impact on firm sustainable performance: a RBV approach, Int. J. Prod. Econ. 150 (2014) 215–224.

Feng, Z., Zhang, T., Wang, J., Huang, W., Wang, R., Xu, J., ... & Gao, G. (2020). Spatio-temporal features of microplastics pollution in macroalgae growing in an important mariculture area, China. *Science of the Total Environment*, *719*, 137490.

Food and Drug Administration. Guidance for Industry: Guide to minimize microbial food safety hazards for fresh fruits and vegetables. 1998. U.S. Department of Health and Human Services, Washington, DC. Available from: <https://www.fda.gov/media/117408/download>.

Food Traceability; Carefour, A Blockchain Pioneerin Europe, has joined .The IBM Food trust platform to take action on a global scale. (2018). Stable URL: <https://www.carrefour.com/en/news/food-traceability-carrefour-blockchain-pioneer-europe-has-joined-ibm-food-trust-platform-take>

Fortuna, F., & Risso, M. (2019). Blockchain technology in the food industry. *Symphonya. Emerging Issues in Management*, (2), 151-158.

Franz, S. (2025). A GPN perspective on the adoption of blockchain technology in global supply chains. *Progress in Economic Geography*, 100043.

Fung, F., Wang, H. S., & Menon, S. (2018). Food safety in the 21st century. *Biomedical journal*, *41*(2), 88-95.

Galvez, J. F., J. C. Mejuto, and J. Simal-Gandara. 2018. Future chal-lenges on the use of blockchain for food traceability analysis. TRACTrends in Analytical Chemistry 107:222–32. doi: 10.1016/j.trac.2018.08.011.

GAO. (2019). Blockchain & Distributed ledger teachnology. Stable URL: <https://www.gao.gov/products/gao-19-704sp>

H. Chen, S. Liu, Y. Chen, C. Chen, H. Yang, Y. Chen, Food safety management systems based on ISO 22000: 2018 methodology of hazard analysis compared to ISO 22000: 2005, Accred Qual. Assur. 25 (1) (2020) 23–37.

Hanif, M., & Song, H. (2019, November). Blocks' Network: Redesign Architecture Based on Blockchain Technology. In *2019 IEEE International Conference on Industrial Internet (ICII)* (pp. 34-39). IEEE.

Hanif, S., Khan, A., Mustafa, E., Ali, M., Shuja, J., & Hasan, M. H. (2024, May). Ensuring Integrity of Quranic Verses using Hyperledger Fabric Framework under IBM Blockchain Platform. In *2024 IEEE 14th Symposium On Computer Applications & Industrial Electronics (ISCAIE)* (pp. 505-510). IEEE.

Hazard Analysis Critical Control Point (HACCP). FDA. (2022).

Henson, S., & Caswell, J. (1999). Food safety regulation: an overview of contemporary issues. *Food policy*, *24*(6), 589-603.

IBM Think Blog (2019). Carrefour and Nestlé Partner with IBM to Extend Use of Blockchain to New Food Categories. IBM Corporation. Stable URL: <https://www.ibm.com/blogs/think/2019/04/tracing-your-mashed-potatoes-on-ibm-blockchain/>

Ismail, L., & Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, *11*(10), 1198.

J.F. Galvez, J.C. Mejuto, J. Simal-Gandara, Future challenges on the use of blockchain for food traceability analysis, TrAC, Trends Anal. Chem. 107 (2018) 222–232

Jacxsens, L., Devlieghere, F., & Uyttendaele, M. (2009). Quality management systems in the food industry. Book in the framework of Erasmus. ISBN 978-90-5989-275.

Jacxsens, L., Luning, P. A., Marcelis, W. J., van Boekel, T., Rovira, J., Oses, S., ... & Uyttendaele, M. (2011). Tools for the performance assessment and improvement of food safety management systems. *Trends in Food Science & Technology*, *22*, S80-S89.

Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International journal of information management*, *50*, 302-309.

Khan, K. M., J. Arshad, and M. M. Khan. 2018. Secure digital votingsystem based on blockchain technology. International Journal ofElectronic Government Research 14 (1):53–62. doi: 10.4018/IJEGR.2018010103

Kotsanopoulos, K. V., & Arvanitoyannis, I. S. (2017). The role of auditing, food safety, and food quality standards in the food industry: A review. *Comprehensive reviews in food science and food safety*, *16*(5), 760-775.

L. Zhang, B. X. Liu, R. Y. Zhang, B. X. Jiang, and Y. J. Liu, ‘‘Overview of blockchain technology,’’ Comput. Eng., vol. 45, no. 5, pp. 1–12, May 2019.

Lal, S. P., Mahendra, A. & Singh, A. (2022). Dietary analysis of traditional food cultures in India: An overview of 2600 BCE to the 21st century. *Toros University Journal of Nutrition and Gastronomy-JFNG, 1* (1), 119-127. E-ISSN: 2979-9511. Stable URL:

 <https://doi.org/10.58625/jfng-1885>

Lal, S. P., Borah, A., Pundir, S., Das, L. & Srivastava, D. (2024). Origin and History of AI, IoT and Blockchain Technology and their Pertinence in Food Supply Chain Management. In Pandey, K., Jain, S., Pandey, D. & Kaiwartya, O. (Eds.), The Future of Agriculture: IoT, AI and Blockchain Technology for Sustainable Farming (pp. 100-118). Bentham Science, UAE. ISBN: 978-981-5274-35-6 (Print). ISBN: 978-981-5274-34-9 (Online). DOI: 10.2174/97898152743491240101. URL: <https://benthambooks.com/book/9789815274349/>

Lawley, R., Curtis, L., & Davis, J. (2012). *The food safety hazard guidebook*. Royal Society of Chemistry.

Lengsfeld. J. (2019). Definition of digital age. Stable URL: <https://joernlengsfeld.com/en/definition/digital-age/>

M. Lierow, C. Herzog, P. Oest, Blockchain: the backbone of digital supply chains. Oliver Wyman, Available at: https://tinyurl.com/yxye47e5, 2017.

M. Tripoli, J. Schmidhuber, Optimising traceability in trade for live animals and animal products with digital technologies, Rev. Sci. Tech. Off. Int. Epiz 39 (1) (2020) 235–244.

M.L. Tamplin, Integrating predictive models and sensors to manage food stability in supply chains, Food Microbiol. 75 (2018) 90–94.

[Mallick](https://www.spiceworks.com/user/about/chiradeepbasumallick). B.C .(2023). What Are Smart Contracts? Types, Benefits, and Tools. Spicework;Stable URL: <https://www.spiceworks.com/tech/innovation/articles/what-are-smart-contracts/>

Marsal-Llacuna, M. L. (2018). Future living framework: Is blockchain the next enabling network?. *Technological Forecasting and Social Change*, *128*, 226-234.

MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY,NATIONAL INFORMATICS CENTRE,CENTRE OF EXCELLENCE IN BLOCKCHAIN TECHNOLOGY. (2024). Stable URL: <https://blockchain.gov.in/Home/Home>

Ministry of Health and Family Welfare Report No. 37 of 2017; Implementation of Food Safety and Standards Act 2006; Union Government, Govt. of India: Delhi, India, 2017; pp. 1–102.

MLJ. FSSAI. Available online: https://fssai.gov.in/cms/food-safety-and-standards-act-2006.php (accessed on 10 April 2020).

Montecchi, M., Plangger, K., & Etter, M. (2019). It’s Real, Trust Me! Establishing Supply Chain Provenance Using Blockchain. Business Horizons, 62 (3), 283-293

N. Kshetri, Blockchain’s roles in strengthening cybersecurity and protecting privacy, Telecommun. Pol. 41 (10) (2017) 1027–1038.

Nemmers, P. (2018). Types of Hazards. NASP Professionals. Stable URL: <https://naspweb.com/blog/types-of-hazards/#:~:text=Biological%3A%20Bacteria%2C%20insects%2C%20viruses,lifting%2C%20repetitive%20movements%2C%20etc>.

Nestle (2019). Nestlé breaks new ground with open blockchain pilot. Stable URL:<https://www.nestle.com/media/pressreleases/allpressreleases/nestle-open-blockchain-pilot>

Odugbemi, A. A. (2017). *Safe Quality Food Certification and Producing Safe and Quality Food Products* (Doctoral dissertation, Walden University).

Patel, A. S., Brahmbhatt, M. N., Bariya, A. R., Nayak, J. B., & Singh, V. K. (2023). Blockchain technology in food safety and traceability concern to livestock products. *Heliyon*, *9*(6).

Patel, A. S., Brahmbhatt, M. N., Bariya, A. R., Nayak, J. B., & Singh, V. K. (2023). Blockchain technology in food safety and traceability concern to livestock products. *Heliyon*, *9*(6).

Perboli, G., Musso, S., & Rosano, M. (2018). Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. *Ieee Access*, *6*, 62018-62028.

Porras-Gonzalez, E. R., Martín-Martín, J. M., & Guaita-Martínez, J. M. (2019). A critical analysis of the advantages brought by blockchain technology to the global economy. *International Journal of Intellectual Property Management*, *9*(2), 166-184.

Prashar, D., Jha, N., Jha, S., Lee, Y., & Joshi, G. P. (2020). Blockchain-based traceability and visibility for agricultural products: A decentralized way of ensuring food safety in India. *Sustainability*, *12*(8), 3497.

PTI. Swiggy, Zomato, Others Remove 10,500 Restaurants for Violating Food Safety Law. Press Trust of India, 2018. Available online: <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/swiggy-zomatoothers-remove-10500-restaurants-for-violating-food-safety-law/articleshow/67093466.cms?from=mdr>

R. Damanik, “Pengkodean Pesan Teks Dengan Proses Penerapan Algoritma Kriptografi Secure Hash Algorithm (SHA),” J. Inform. Kaputama, vol. 1, no. 1, pp. 48–57, 2017.

R. Munir, Kriptografi, Bandung: Informatika, 2006.

Raj, R., Kumar, S., Lal, S. P., Singh, H., Pradhan, J., & Bhardwaj, Y. (2024). A Brief Overview of Technologies in Automated Agriculture: Shaping the Farms of Tomorrow. *International Journal of Environment and Climate Change*, *14*(7), 181-209.

Rahardja, U., Hidayanto, A. N., Lutfiani, N., Febiani, D. A., & Aini, Q. (2021). Immutability of Distributed Hash Model on Blockchain Node Storage. *Sci. J. Informatics*, *8*(1), 137-143.

Riza, B. S. (2020). Blockchain Dalam Pendidikan: Lapisan Logis di Bawahnya. *ADI Bisnis Digit. Interdisiplin J*, *1*(1), 41-47.

Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access*, *7*, 50759-50779.

S. Rouhani and R. Deters, ‘‘Security, performance, and applications of smart contracts: A systematic survey,’’ IEEE Access, vol. 7, pp. 50759–50779, 2019

Saad, S. M. S., & Radzi, R. Z. R. M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, *10*(2).

Saad, S. M. S., & Radzi, R. Z. R. M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, *10*(2).

Safe quality food certification. (2024). NSF.U.S. Stable URL: <https://www.nsf.org/food-beverage/sqf>

Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of financial studies*, *34*(3), 1156-1190.

Samadder, S., Lal, S. P., Prakash, S., & Singh, K. M. (2025). Determinants of food insecurity in the Sundarbans: Multinomial logit approach apropos the Food Insecurity Experience Scale. European Journal of Nutrition & Food Safety, 17(4), 204-215. doi: <https://doi.org/10.9734/ejnfs/2025/v17i41692>

Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, *8*(2), 23-29.

Schmit, T. M., Wall, G. L., Newbold, E. J., & Bihn, E. A. (2020). Assessing the costs and returns of on-farm food safety improvements: A survey of Good Agricultural Practices (GAPs) training participants. *PloS one*, *15*(7), e0235507.

Secure Hash Algorithms. Available online: <https://en.wikipedia.org/wiki/Secure_Hash_Algorithms> (accessed on 7 January 2019).

Sergeevic, P. A. (2023). Use of Blockchain Technology in Business Operations.

Sharifian, Z., Saidi, H., Fanian, A., & Gulliver, T. A. (2023). A New Approach to Orphan Blocks in the Nakamoto Consensus Blockchain. *IEEE Transactions on Network Science and Engineering*.

Sharma, M., & Kumar, P. (2021). Adoption of blockchain technology: A case study of Walmart. In *Blockchain technology and applications for digital marketing* (pp. 210-225). IGI Global.

Sheikh, H., Azmathullah, R. M., & Rizwan, F. (2018). Proof-of-work vs proof-of-stake: a comparative analysis and an approach to blockchain consensus mechanism. *International Journal for Research in Applied Science & Engineering Technology*, *6*(12), 786-791.

Sheth, H., & Dattani, J. (2019). Overview of blockchain technology. *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146*.

Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. *Ieee Access*, *9*, 13938-13959.

Stable URL: <https://www.analyticssteps.com/blogs/3-types-block-blockchain-network>

STABLE URL: <https://www.fda.gov/food/guidance-regulation-food-and-dietary-supplements/hazard-analysis-critical-control-point-haccp#:~:text=HACCP%20is%20a%20management%20system,HACCP%20Principles%20%26%20Application%20Guidelines>

Talha Talukder, A. A., Mahmud, M. A. I., Sultana, A., Pranto, T. H., Haque, A. B., & Rahman, R. M. (2022). A customer satisfaction centric food delivery system based on blockchain and smart contract. *Journal of Information and Telecommunication*, *6*(4), 501-524.

Tasca, P., & Tessone, C. J. (2017). Taxonomy of blockchain technologies. Principles of identification and classification. *arXiv preprint arXiv:1708.04872*.

Tella, A., Quardri, F., Bamidele, S. S., & Ajiboye, O. O. (2021). Resource Sharing: Vehicle for Effective Library Information Dissemination and Services in The Digital Age. In *Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing* (pp. 1481-1503). IGI Global.

Tian, F. (2017, June). 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* (pp. 1-6). IEEE.

Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. *Information & Management*, *58*(3), 103444.

Van de Venter, T. (2000). Emerging food-borne diseases: a global responsibility. *Food Nutrition and Agriculture*, (26), 4-13.

Wu, C., Xiong, J., Xiong, H., Zhao, Y., & Yi, W. (2022). A review on recent progress of smart contract in blockchain. *IEEE Access*, *10*, 50839-50863.

Wünsche, J. F., & Fernqvist, F. (2022). The potential of blockchain technology in the transition towards sustainable food systems. *Sustainability*, *14*(13), 7739.

Xu, Y., Li, X., Zeng, X., Cao, J., & Jiang, W. (2022). Application of blockchain technology in food safety control： current trends and future prospects. *Critical reviews in food science and nutrition*, *62*(10), 2800-2819.

Xu, Y., Li, X., Zeng, X., Cao, J., & Jiang, W. (2022). Application of blockchain technology in food safety control： current trends and future prospects. *Critical reviews in food science and nutrition*, *62*(10), 2800-2819.

Yen. O.R. (2024). Common safety issues in 2024. TUV. StableURL: <https://www.tuvsud.com/en-id/resource-centre/blogs/common-food-safety-issues>

Yeo, V. C. S., Goh, S. K., & Rezaei, S. (2017). Consumer experiences, attitude and behavioral intention toward online food delivery (OFD) services. *Journal of Retailing and Consumer Services*, [*35*](https://doi.org/https%3A/doi.org/10.1016/J.JRETCONSER.2016.12.013)([March](https://doi.org/https%3A/doi.org/10.1016/J.JRETCONSER.2016.12.013)), 150–62. <https://doi.org/10.1016/J.JRETCONSER.2016.12.013>

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375.