Privacy-Preserving Techniques in Blockchain-Based Food Supply Chain

Nicola-Paul Stepanov Supervisor: Tianyu Li
Responsible Professor: Zekeriya Erkin
Cyber Security Group
Department of Intelligent Systems
Delft University of Technology
N.P.Stepanov@student.tudelft.nl, {Z.Erkin, Tianyu.Li}@tudelft.nl

27th of June 2021

Abstract

The following paper aims to investigate what and how are the main privacy-preserving methods applied in the blockchain-based supply chain industry scenario, with a primary focus on the food sector. Recent developments, such as the exordium of cryptocurrencies to increment efficiency, are withal addressed. Overviews of key use cases in industry and research are provided. Numerous blockchain projects, such as VeChain, or multiple others established on well-known infrastructures such as Ethereum or Hyperledger Fabric, are being developed, introducing cryptocurrencies to contribute to a future food supply chain network. Therefore, the motivation of this investigation is to discover how privacy is protected in the field of the food supply chain by the latest developments, such as cryptocurrencies. Do these techniques avail towards a more secure future in the field of the food supply chain from a privacy perspective, or do they introduce additional bottlenecks that could lead to incipient challenges? The principal results and conclusions reveal that proper privacy-preserving techniques exist and have a vigorous connection with the existing applications in the aliment supply chain sector. However, as the magnitude of data grows and the adoption of blockchain becomes very relevant in the supply chain, more focus needs to be attributed to the direction of how privacy is preserved and better methods need to be implemented as the field evolves. In addition, a privacy-preserving model proposal is presented, along with some guidelines and views on the future of this field.

1 Introduction

Whether we are eating an apple, raising chickens in order to sell their eggs, working in the delivery sector or simply browsing an e-commerce website for the latest discounts, we are all part of the supply chain. Without it, the world as we know it today would be extremely different and arduous to live in by current standards. Because it makes the world go round, an abundance of attention needs to be given to the supply chain. Making this network more efficient can only benefit everyone, hence incipient technologies are adopted to revolutionize it. One of the latest and most groundbreaking solutions is blockchain technology. Among the multiple advantages that this exhilarating infrastructure institutes, we can enumerate its permanent nature, the accountability, traceability, and precision of transactions contained in the ledger. Since it offers consensus processes to create a true state of fact, blockchain provides a thoroughly decentralized root of confidence that evades central authority, thus inspiriting trust[1]. Because of its decentralized existence, it is extremely difficult to modify transactions until they have been authenticated by the system, granting it the property of immutability[2].

Nonetheless, as with anything else, extensive studies need to be done beforehand to introduce it safely in the supply chain, while keeping the advantage-disadvantage trade-off minimal. In this research paper, we focus on the positives, as well as the challenges of this overlap of fields and what are the major privacy mechanisms.

Moreover, the application through blockchain projects is examined, together with the key use cases from the food sector of the supply chain. The motivation for choosing the victuals sector of the supply chain originated in the idea that this is a field of great significance, present and affecting our quotidian life.

Food has become a hotspot for blockchain initiatives. When blockchain is coupled with other technologies such as the Internet of Things (IoT), it could be acclimated to build a permanent, shareable, and actionable archive of any moment of a product's journey across the supply chain. This boosts efficiency in the entire global economy. [3] suggests that blockchain could be groundbreaking and ameliorate the food sector in regards to *security*, as blockchain would eliminate middlemen in the distribution process, making documents and assets more verifiable and accessible, and allowing businesses to act more efficaciously[4]; *safety*, as the critical demand for more preponderant food traceability in terms of safety and transparency might be met utilizing blockchain technology; and last but not least, *integrity*, as victuals corporations may apply blockchain to combat aliment fraud by promptly identifying and tracing outbreaks back to their origin[5].

An abundance of works discusses the privacy-preserving approaches in blockchain technology, additionally to the security threats and privacy solutions utilizing blockchain techniques. However, there are not many studies that discuss the exact implications of this method in the field of the food supply chain. Furthermore, the implicative insinuation of cryptocurrencies and blockchain platforms is still at an early stage of development. Cryptocurrencies are becoming increasingly popular, and a shedload of them are perforating and revolutionizing fields such as the supply chain. What this study seeks to answer is

"How are privacy-preserving techniques present in the blockchain-based food supply chain?"

The rest of this paper is organized as follows: Section 2 presents the chosen methodology, as well as an overview of related work. This is followed by background knowledge and consequential concept definitions and context in Section 3. In Section 4,5 and 6, the core of this investigation's contribution can be found: an overview of privacy-preserving methods in blockchain in Section 4, linked with the applicability in the supply chain domain, a privacy-preserving proposal in Section 5, followed by an outline of the main supply chain blockchain project, such as Ethereum, Hyperledger and Vechain, as well as alternative cryptocurrency-proposals and industry use cases. Section 7 introduces the principal experimental results and a discussion component, together with the circumscriptions of this investigation. Afterwards, responsible research can be found in Section 8, while the conclusions and future directions are furnished in the last part.

2 Research Methodology and Related Works

2.1 Methodology

To better understand what ameliorations can be made to increment privacy methods in blockchain, we must first have a foundation of what the main privacy-preserving techniques of blockchain-predicated applications are. A systematic literature review has been conducted as suggested in [1]. The major benefits of doing this are that it provides a knowledge base on the topic and highlights aspects of precedent work to evade repetition. It withal acknowledges the work of other academics whilst pointing up inconsistencies such as examination gaps, past study disputes, or unanswered concerns. In the first stage of formulating, the central research question was chosen, along with additional questions that might be answered during the course of this thesis, namely *"What are the main privacy-preserving blockchain-based techniques utilized in the supply chain?"* and *"What are the most relevant cryptocurrencies in the field of the food supply chain and what are their utilization cases?"*

After that, various databases and search engines are utilized to amass scientific publications under certain parameters such as publication date, keywords or omitting and including elements. Since pertinent information is prioritized, more recent papers were selected, and for most searches, the publication date had to be more incipient than the year 2019. The most popular keywords were "blockchain", "supply-chain", "privacy". Supplemental bibliography was found by accessing the following databases: Google Scholar, IEEE Xplore Digital Library, Science Direct, Springer and ACM Digital Library. The snowballing phase availed in the utilization of references from one document or its citations to identify other documents. In the final stages of the process, the material was categorized into several formulated sub-questions, structured and "cleaned" in such a way that only the most pertinent information remained to answer the proposed sub-questions.

2.2 Related works

Interest in privacy-preserving approaches in blockchain can be observed in works such as [2],[6],[7],[8] that address security issues and privacy challenges and solutions. [6] is a Survey about privacy preservation in permissionless blockchain, and performs a comparison with existing examinations while providing an overview of blockchain technology and privacy threats and requisites in the blockchain. In [7], one can notice a deeper dive into the safety issues of blockchain and the possible types of attacks, as well as a breakdown of the privacy issues of the same innovation. The study in [8] divides privacy on identity and transaction and formulates some methodologies for these two types of privacy. It fixates on the technical part of procedures such as Mixing Services or Ring Signature. Last but not least, [2] tackles privacy challenges supplementally to solutions. Moreover, all the data is organized in tables, giving a clear overview of the disadvantages and advantages of all these approaches. Certain blockchain proposal scenarios are described, such as Smart Cities, E-governance and Cryptocurrencies.

Nevertheless, linking the existing privacy preservation methods with the appropriate scenarios of the food supply chain is something that has not been explored yet and needs some attention. Fields such as smart contracts, de-anonymization mechanisms, transaction and identity-based privacy initiatives, GDPR compliance, are explored among numerous others. The most important applications of blockchain platforms such as Ethereum and Hyperledger are subsequently examined, as well as more recent systems that introduce their cryptocurrencies to revolutionize the food sector of the supply chain. By analyzing multiple sources, a way to compare these platforms from the most pertinent angles is presented, in addition to solutions and future recommendations on how they can amend their capabilities.

3 Background Knowledge

3.1 Supply Chain, Blockchain and Smart Contracts

Being essential to humanity's current needs, the supply chain is the network of all operations, individuals, organizations, information, and resources involved in the conveyance of raw materials, components, and finished goods from origins to the final consumer[9]. Supply chain management (SCM) is the centralized management of the flow of goods and services. Gaining advantage in the marketplace, ameliorating product quality, keeping companies away from expensive lawsuits, as well as eschewing costly shortages or periods of inventory oversupply are the major benefits offered by a good SCM [10].

In 2008, when S. Nakamoto launched Bitcoin as the first peer-to-peer digital money framework, the idea of blockchain technology first emerged as a method for handling cryptocurrencies. Blockchain is established on a synchronized Distributed Ledger Technology (DLT) that makes use of decentralization and cryptographic hashing to make the history of any digital asset immutable and transparent [11]. Blockchain is based on the concept of decentralizing the system through the use of a shared distributed ledger and is thus "a database architecture that enables the maintenance and sharing of records in a distributed and decentralized manner while ensuring its integrity through the use of consensus-based validation protocols and cryptographic signatures" [1]. Prior to blockchain, trust in an environment was typically established through intermediaries. With blockchain, trust is shifted from a classical centralized approach to a plenary decentralized network of nodes [2].

Because it is a transactional process designed to manage subsequent events and activities in accordance with the terms of a contract or agreement instantly, the concept of smart contracts may be the most revolutionary blockchain advancement for supply chains. It allows for the creation of algorithms and systems that can be partly or entirely executed or applied when requirements are met, without the need for human intervention. Once a pre-set number of conditions chosen by the involved parties is triggered, a smart contract activates[12]. In terms of legal complexity, smart contracts on the blockchain ensure adherence to rules and regulations[1]. Some important additional concept definitions are the following:

- Consensus: A technique of verifying and validating a value or action taking place on a blockchain or distributed ledger without relying on a central authority[13].

- Proof-of-Work (PoW): To prevent anyone from manipulating the system, a decentralized consensus method forces network users to spend time-solving an arbitrary mathematical challenge[14].
- Proof-of-Stake (PoS): Reaching consensus by choosing validators based on their number of assets[15].
- Proof-of-Authority (PoA): Reputation-based consensus mechanism in which block validators stake their own reputation rather than coins[16].
- On-chain transactions need a complete blockchain update as well as a majority of participant consent. Off-chain transactions allow participants to reach a compromise outside of the blockchain, sometimes including a third party[17].

3.2 Privacy in Supply Chain

Privacy is a constitutional right essential to the autonomy and the preservation of human dignity, and it serves as the basis for many other humanitarian laws. It is the way "we seek to protect ourselves and society against arbitrary and unjustified use of power" [18]. The intrusion of our privacy is often utilized as a launching pad for the violation of our other privileges[19]. All major international and regional human rights mechanisms recognize the right to privacy, including the United Nations Declaration of Human Rights (UDHR) of 1948[18].

In this era of data exploitation, privacy has never been more significant. Our confidentiality is increasingly threatened due to the way information and technologies are used today[19]. As technology becomes more advanced and creative, more data is stored and shared, complicating identity protection and making securing sensitive information more difficult. As a result, privacy has quickly risen to the top of the list of safety concerns[20]. Perhaps the most serious problem with privacy is that it can be breached without the individual's knowledge[18]. Data privacy is about the use and control of personal information, whereas security is about protecting data from malicious threats and the profiteering of data theft. While security is vital for data protection, it is insufficient for resolving privacy concerns [20].

Among the most significant privacy regulations, the Privacy Shield Framework and the General Data Protection Regulation (GDPR) highlight the value of companies retaining vigilance over their digital supply chains to properly determine their third-party supplier compliance and privacy policies. Businesses must restrict the amount of data they exchange with external parties, and also ensure that distributors and suppliers protect and only utilize it for its intended purposes[21]. Both pronouncements establish regulatory foundations for data sharing while expecting companies to develop and implement protocols, let alone demonstrate that they have implemented and are following such policies. This has a strong effect on businesses that exchange consumer information with outside parties in their digital supply chains[21].

3.3 Blockchain and Food Supply Chain

The data in a blockchain is not controlled by a single entity. Without the use of an agent or a distributed consensus system, each party may independently check the records of its transaction partners. Users always have access to a robust audit trail of the operation, since existing blocks of the chain cannot be overwritten [23]. To provide a general summary, [22] claims that the distributed nature, decentralized consensus, trustless mechanism, cryptographic stability, and non-repudiation guarantee are the core properties of the blockchain.

There are two common ways to distinguish blockchain configurations, according to [1]:

- Based on **permission** (or who maintains the blockchain system) [24]: The blockchain is **permissionless** if anyone can publish a new block, as Nakamoto (2008) originally proposed. As no prior authorization is required, anyone can join the network, verify transactions, and execute them. In contrast, in a **permissioned** scenario, members must receive an invitation or permission to participate, and nodes and users are approved and controlled by a central authority.
- Established on **who can access** information: The blockchain was envisioned as **public**, with a public ledger that allows anyone to access all registered proceedings at any time, while users stay anonymous [25]. A single entity manages and monitors access to registered transactional data in a **private** blockchain.

Blockchain integrated with the supply chain has the ability to change the way network stakeholders interact, improve performance, and reduce negotiation costs. The principal factors of focus are cost, quality, risk reduction and flexibility [26], product traceability issues [27][28][29] and anti-counterfeits [30]. The benefits of blockchain include improved processes and operations across the supply chain, as well as secure, open, and productive transactions among system members. This would greatly improve stakeholder partnerships (cooperation and trust, for example) in supply chains. In addition, product traceability can be greatly increased, allowing consumers to track a product's entire route and upgrading the quality of logistics. All this contributes to a significant reduction in transaction costs, especially since an intermediary is no longer required [31][32].

While the internet has connected people all over the world, blockchain has the power to influence a whole range of industries, including supply chains, and could radically alter how we trust on a global level[1]. Trust relates to the accuracy of information supplied by trading partners or the protection and security of data handled by a central authority. Obtaining and preserving trustworthy data is crucial[23]. Because of its innovative features, blockchain can lower governance expenses and change the optimum governance system depending on certain circumstances[1].

3.3.1 Advantages and Disadvantages

Applied to the food supply chain, the most relevant advantages are: *low transaction costs*, as for buyer-supplier negotiations, blockchain reduces transaction costs by limiting opportunistic activity, environmental and behavioural instability[1]; *traceability*, since by reducing contract registration and the number of intermediaries, efficiency is increased due to the lack of reviewing efforts and fewer manual interventions[23]; *transparency*, that establishes improvement in the exchange of information between business partners and supply chain visibility[12]; as well as *hashing and digital tokens*, as the hashing method converts tangible and intangible assets into a securely encrypted token that can be recorded and exchanged on a blockchain using a private key. These digital tokens are manufactured to protect against counterfeit or theft. This organizational feature helps preserve secrecy since products and their related tokens are rarely exchanged amongst rivals within a given blockchain[12].

Despite the advantages of blockchain and smart contracts in transforming supply chain processes, there are still certain barriers to their universal acceptance. Compliance problems, a lack of guidelines and procedures, data exchange, relationships between organizations, commitment, and error aversion are among the obstacles[33]. Besides that, blockchain adoption differs by region, and in developing nations, the viewpoint of coworkers and family members on blockchain adoption matters even more than one would think, triggering real influence[32]. Nonetheless, the emphasis of this paper is on privacy, as blockchain allows all participants to exchange information on agreements to some extent.

3.3.2 Privacy Challenges

Besides the good parts it brings to the table, a certain number of privacy concerns arise for blockchain applications in various domains. [2] mentions the most important privacy challenges. Based on this, an overview table was created under the name Table A and can be found in the Appendix. This presents a short description of challenges, together with the proposed solutions in dealing with these concerns.

From another perspective, [7] states that three main categories can be derived for what concerns the legal privacy experts:

- Physical-Cyberspace Boundary: In a centralized administration, biometric identifiers can only be kept in one location. Storing these across all nodes makes it simpler to be hacked. Furthermore, there is a lack of a clear central authority to secure and alert people if their user credentials are breached.

- Information Storage and inference: With the assumption that data is encrypted, the fact that transactions occur reveals confidential details. While dangers can indeed be alleviated by functioning in closed networks, there still are advantages to open systems that necessitate the operation of at least some blockchains containing sensitive information in networks that aren't totally closed.

- Nature of blockchain: Due to blockchain's eternal record functionality, there is no control over where data is kept, what it is used for, or how it can be deleted. Furthermore, in the absence of specific ownership laws, public authorities and private individuals can have access to these details without the permission of the negotiation's participants.

3.3.3 Security and Privacy Attacks

Regarding blockchain safety, various threats exist. However, security, in general, is not in the scope of this research. As mentioned previously, security is a vital aspect for preserving data protection, but not enough for solving privacy concerns. Thus, the centre of attention is privacy-related attacks.

- De-anonymization and tracking: De-anonymization is possible, even though users typically utilize hash values of randomly chosen public keys as identifiers to mask their true identities[6]. Thanks to the public and transparency properties of blockchain, it is possible to perform a static review of the blockchain or actively listen for network knowledge to expose participants. Several attacks are performed for de-anonymizing the real identities of users, as per [8]. These attacks can mostly be linked to the Information Storage and inference challenge presented previously.

    1. Network Analysis: While broadcasting transactions, a node's IP address can leak due to the P2P network architecture.
    2. Address Clustering: It is possible to be discovered that certain addresses belong to the same individual.
    3. Transaction Fingerprinting: [34] suggest that random time-interval (RTI), the hour of the day (HOD), time of hour (TOH), time of day (TOD), coin flow (CF) and input/output balance (IOB) can be used to define certain facets of transaction behaviour and increase the likelihood of de-anonymizing a specific consumer.
    4. DoS (denial-of-service) Attacks: By compromising services of the host connecting to the Internet, the attacker attempts to make a machine or network resource inaccessible to its users.
    5. Sybil Attacks: By generating a vast number of pseudonymous identities, an attacker subverts the credibility structure of a P2P system. Such attacks have the potential to disable decentralized anonymity protocols[35].

- Transaction pattern exposure: In arrangements such as Bitcoin, all transfers are open and transparent, allowing participants to see the whole transaction. Any undertaking in the framework is traceable thanks to the blockchain's chain and Merkle tree structure, which allows an attacker to monitor the transaction and extract the necessary information[6]. Other dealings data streams to the public network might be utilized to derive statistical distributions, except for certain publicly identified information[8]. This type of attacks is therefore closely related to the nature of the blockchain category mentioned in the previous subsection.

    1. Transaction Graph Analysis: Concentrates on general features of transactions
    2. AS-level Deployment Analysis: Connecting to members recursively, asking and obtaining the collections of other peers' IP addresses.

4 Privacy Preservation Methods Overview

One of the most fundamental ways of dividing the privacy-preserving techniques is by looking at transaction privacy and smart contract privacy. The first one can be further divided into identity data related privacy methods and transaction privacy approaches. In this part of the section, a general overview of existing privacy-preserving approaches is conducted. Consequently, the linkage of all these mechanisms to possible supply chain applications and explanation on how they fit in the scheme is carried out.

4.1 Transaction related privacy preservation

Direct privacy leakage related to transaction transparency is a critical problem in the permissionless blockchain. An intruder can acquire the correlation between negotiation addresses and determine the user's true identity from additional information by evaluating the transaction graph. This is an example of indirect privacy leakage[6].

4.1.1 Methodology for identity data privacy preservation (Identity Data Anonymization)

In the context of the supply chain, the identity of a user can be preserved through the following methods. Whether it is about Mixing Services, Ring Signatures or Non-Interactive Zero-Knowledge Proofs (NIZK Proofs), they all have in common the goal of disallowing an attacker to track and discover the identity of a participant taking place in the supply chain.

- Mixing Services: Permitting multiple customers to create a single transaction containing multiple inputs and outputs reduces the chance of de-anonymization[6]. This approach looks at the message's timing similarity in the system, not any personally identifying information (PII)[2]. Depending on if a third party is required, mixing services may be classified as[6]: **Centralized mixing** relies on a trusted or semi-trusted third party called a mix server. Some examples of such services are Mixcoin, Blindcoin, CoinJoin or Tumblebit. In contrast, **decentralized mixing** services such as CoinParty, Xim, CoinShuffle or CoinShuffle++ benefit the users since no mixing fees are required. There exist several common drawbacks when using mixing services, such as the extra waiting period for mixing the transaction and the lack of content security.

  An overview table containing the specifications, as well as what privacy protection is achieved by each of these services is performed and can be found in the Appendix, under Table B. [6] was used for the privacy protection information, [2] for the year and main approach, while [8] for anonymity and the resistance between attacks such as Theft, Dos, Sybil.

- Ring Signature: This popular anonymity method can be utilized to conceal the identity of the signer. It does not, however, purposefully conceal the message to be signed, and the scale of the signature is equal to the number of recipients, implying higher storage and interaction with a greater number of participants[8]. The applicability of ring signatures with crypto-based techniques intersects projects such as CryptoNote, CoinJoin, ValueShuffle or Monero, whose overview is presented in Table C of Appendix.

- ZKP's: The zero-knowledge proof is a method for persuading a verifier that a given assertion is true without revealing any valuable facts[6]. Some of the most prolific making use of this technique are Zerocoin, Enhanced ZeroCoin (EZC), ZeroCash and BulletProofs. Similarly, an overview of these can be found in the same Table C of Appendix [2].

- NIZK Proofs: They have been presented as an approach for enabling complex privacy-preserving smart contracts, being essentially ZKPs that do not need interaction between the authenticator and the validator[2]. NIZK creates a comprehensive privacy protection framework for the blockchain. While Zerocoin offers high anonymity, it is unable to maintain transaction privacy, whereas Zerocash was created to achieve both anonymity and agreement privacy at the same time[8]. Mimblewimble surpasses Zerocash in terms of computational complexity, hence extra privacy aspects are being investigated.

- Complementary Approaches: Complementary practices to enhancing privacy properties of blockchain-based cryptocurrencies have also been discussed. Pedersen commitments allow users to commit a message, without actually revealing the content of it until a certain time in the future. Stealth addresses allow the transmitter to generate a unique, random address for each transfer on account of the receiver so that transactions to the same payee cannot be linked., while Mobius is a smart contract Ethereum-based mixing service. ValueShuffle [36] applies Stealth Addresses to the mixing method CoinShuffle++ to provide a more robust privacy-preserving solution[2].

4.1.2 Methodology for Transaction Data Privacy Preservation

- Mixing: In countless food supply chain applications, digital tokens (coins) are traded each time a transaction takes place. This procedure helps with the anonymization of traded coins.
- Differential Privacy: This approach focuses on data privacy by determining if an analysis technique discloses personal information or not. It entails adding a specific amount of random noise to queries such that any statistical analysis of the entire set comes near to the genuine findings, but inference over any single participant is impossible. Nonetheless, there seems to be a compromise between usefulness and privacy, since data cannot be totally anonymized while still being valuable for analysis[2].
- Homomorphic Hiding: The homomorphic cryptosystems, such as the Pedersen commitment scheme and Paillier cryptosystem, are useful procedures for safeguarding the details of a transaction whilst operating on private information to preserve blockchain privacy. It is ideally applicable for concealing and updating the quantity and other metadata of a negotiation promptly[8]. Nevertheless, this can also be utilized in the context of Identity Data Privacy Preservation for the exchange of coin addresses. This is applicable in the food supply chain, especially when the blockchain platform is formed on cryptocurrency trading.

4.2 Smart Contract related Privacy Preservation

Smart contracts face major privacy threats since the whole contract implementation stage is transparent to all parties involved and remains eternally recorded on the blockchain[6]. Consequently, numerous initiatives for privacy preservation have been proposed, and Hawk[37] is a very significant one. This is the first effort to guarantee both transactional privacy and programmability. Based on the Zerocash and smart contract systems, here participants transmit encrypted and committed data to the smart contract and depend on NIZK proofs to ensure contract execution and funds transfer accuracy. Although the outcome of a smart contract may be verified by the public, the complete sequence of transaction operations performed by the contract is kept private[8].

5 Privacy-Preserving Proposal

Policies like GDPR are a good commencement, yet they do not solve certain underlying infrastructure imperfections. There is no such thing as a magic formula when it comes to privacy. That's also the major problem with subsisting privacy-preserving techniques: albeit there exist partial clarifications for certain situations, none solves the privacy issue overall. Therefore, one of the best ways for amending this field is an assemblage of existing methods and futuristic proposals. Privacy concerns are still preventing information exchanges from reaching their full potential, thus in a society where data and privacy coexist, a contemporary data economy predicated on equity and trust has the potential to open up incipient possibilities[38].

A plethora of papers takes a look into amending the current privacy-preserving procedures. Data Storage Mechanism is one such example described in [39]. Due to the requirements of the supply chain for authenticity, this technique minimizes storage capacity by offering the blockchain a subsection storage model, called the parallel subsection model. This storage model can efficaciously control data access classifications and alleviate the supply chain business customers' privacy leakage issue. In a traditional blockchain, each authentication centre completely shares all data, however, the method of each node maintaining blockchain accounts waste in storage space. As a result, in the proposed architecture, each part of the blockchain is shared by certain authentication centres for the blockchain creating subsections. So, while each authentication centre does not fully store all of the blockchain's subsections, it may obtain all of the blockchain's data via the logic links between the subsections. Furthermore, rather than being serial, the supply chains of multiple manufacturing businesses are logically parallel in the supply network chain.

The proposal of this investigation combines certain elements such as the aforementioned **parallel subsection storage model** and **differential privacy** for introducing a small amount of noise to the data. This amplitude

of noise can be integrated into the subsection components. On top of that, the proposed method would contribute to the development of an administration that secures tracking and smart contract code while additionally distributing keys to the stakeholders of the tracking process, such as the end-users, farmers, distributors.

The model would ensure the anonymity of any transaction that the contract designs and executes, and it might be used to facilitate information exchange between partners in the supply chain who do not trust one another. This would open up sectors where strong privacy was required, such as keeping sensitive data about food in the supply chain or clinical records in the health industry on a centralized server[40]. A system similar to Hawk could be utilized to **generate the smart contract**. Hawk generates privacy-preserving smart contracts using a blockchain cryptography model. This sort of project has the potential to turn any N-party protocol into a zero-knowledge protocol that only trusts the blockchain for legitimacy and one specified party for privacy. However, in our instance, the idea would be to develop a privacy protocol that relies on zero parties[41].

Looking ahead, the outlined proposal respects a mixture of privacy by design, self-sovereign identification, and the "right to be forgotten." With the GDPR, privacy by design is now a legal obligation. **Privacy by design** entails including data protection from the start of system development, handling solely the absolutely essential information and restricting access to personal data to those who require it to carry out the processing[42]. **Self-sovereign identification** is a very plausible alternative for achieving privacy[42]. Allowing every individual authority over their personal data and identity is most certainly the way to go. In this instance, the individual is the only one who has the authority to reveal or provide access to classified information, and he or she also has control over the degree and length of external access[43]. Simply put, the GDPR's **"right to be forgotten"** provision requires that personal data processed on consumers be destroyed if they request it [44]. This is only possible under limited circumstances, but the fact that consumers have this level of control is a positive step forward in terms of privacy.

To recapitulate, the improvements this proposal brings are multiple. Due to the parallel subsection storage model, lack of waste in storage space is achieved, while effectively resolving the privacy leakage issue of the supply chain business subjects. As a result of introducing Differential Privacy, the conclusion of the statistical analysis is roughly similar regardless of whether somebody joins or not the database. Last but not least, probably the most crucial improvement is how privacy-preserving smart contracts would be generated. Hawk is a groundbreaking work, which made possible the idea of a zero-knowledge protocol that trusts one specified party for privacy. The removal of this entity would mean a great development, as we reduce the need for trust. There is a fine line between the lack of trust and the lack of need for trust. The latter is the one we are aiming for.

6 Supply Chain Blockchain Projects and Cryptocurrencies

Essentially, the majority of supply chain blockchain initiatives are built on either Ethereum or Hyperledger Fabric. Ethereum is famous for its capacity to execute smart contracts and facilitate financial transactions. Hyperledger Fabric, on the other hand, is a Linux-led private permissioned modular platform that aims to advance cross-industry blockchain growth. One big difference between the two relies on the consensus mechanism they use. The first one uses mining-based PoW to verify transactions, which means that all participants must agree on the order of all negotiations. It pays transaction fees and rewards miners with a built-in cryptocurrency called "ether". Hyperledger, on the other hand, allows for more fine-grained access control, with just the parties involved in an undertaking needing to agree[23].

6.1 Hyperledger Fabric

Hyperledger Fabric is designed as a modular framework with several features, such as division of channels structure or assignation of a unique ID once a member joins the system[45]. To engage and trade on the blockchain, all members must be verified. Chaincodes, which are smart contracts, are supported by Hyperledger Fabric[46]. In this blockchain platform, privacy is achieved by [47][48]:

- The Permissioned Nature: allows network participants to use robust authentication to prove their identity.
- Multi-Channel Design: Separating information into multiple channels preserves confidentiality of data.

- Private Data Collection (PDC): facilitates peers to endorse or commit confidential material without having to set up a new channel[49]. Because any peer can wipe its private database at any moment, the "right-to-be-forgotten" may be employed in private transactions.
- Asymmetric Cryptography and ZKP's: Maintain privacy by separating transaction data from on-chain records[49]. With the deployment of ZKPs, two privacy-preserving techniques are attained: *identity mixers*, which ensure that customers' transaction proposals are anonymously authenticated and *Zero-Knowledge Asset Transfer*, where clients can execute transactions without exposing any other details to peers about the asset exchange, except for evidence that each arrangement complies with asset management standards.

6.2 Ethereum

Ethereum, an open-source public blockchain, aspires to develop an application-building framework that enables anybody to create smart contracts and decentralized apps[50]. The disadvantages of this procedure include its high latency and the fact that, because it is permissionless, it is not ideal for secretive negotiations[45]. As a result, the employment of cryptographic algorithms and protocols for consumer and company privacy has become extremely important.

There are two privacy preservation approaches presented in [51] that are introduced before the blockchain transaction data is released publicly. The first is *chaotic map-based noise addition*, utilizing tent map functions to generate noise. Chaotic maps are functions that concentrate on dynamical systems that are sensitive to their beginning circumstances. The *differential privacy Gaussian noise enhancement* is the second form of noise addition, which is the statistical noise with a probability density function equivalent to the normal distribution.

Nonetheless, following the rapid development of cryptocurrencies in various fields, certain initiatives focused specifically on the supply chain arise. In the next few paragraphs we take a look at what are these, how are they relevant in the food sector, and how do they achieve privacy. The most notorious project of such is VeChain, and more attention is given to it, as it is shaping the path for the other supply chain cryptocurrencies.

6.3 VeChain

6.3.1 What is VeChain

VeChain is a decentralized system that utilizes blockchain to improve supply chain management and assists customers in verifying the legitimacy of items. This is accomplished through the use of near-field communication (NFC) chips, radio-frequency identification (RFID) technology and quick response (QR) codes, which are real-time accessible. It manages and creates value with two in-house currencies, VET and VTHO, built on its VeChainThor public blockchain. VET is a PoS token that is used for transactions and value transfer throughout the network, whereas VTHO is utilized as "gas" to fuel smart contract arrangements[52]. PoA is used as a consensus technique on the VeChainThor blockchain. No anonymous nodes are allowed, and revealing one's identity is a requirement for becoming an authority master node[52].

6.3.2 VeChain for the Food Supply Chain

Food safety concerns might be introduced into the aliment supply chain at any moment if proper monitoring is not in place. VeChain proposes clarifications such as the Consumer Confidence Index Platform, in which data acquired by the platform is validated by an independent third party, before being published to the VeChainThor Blockchain[53].

6.3.3 Privacy Preservation in VeChain

Because VeChain facilitates the formation of mutually advantageous partnerships between different organizations in the ecosystem, several of them may be concerned about privacy[54]. Their approach is to seek the data owner's approval before allowing it to be utilized by another entity. They're also experimenting with privacy

options such as multi-party computation (MPC), which aims to generate methods for entities to collectively calculate a function over their input variables while maintaining the privacy of those components. For full potential use of VeChain Thor, users are required to exchange VeChain based currency. Therefore, Mixing Services, Ring Signatures and ZKP's are all ideal candidates for preserving privacy in this initiative.

The GDPR requires compliance by any organization that sells products or services to EU citizens. To investigate compliance for VeChain's blockchain solutions, the development team proposed the following staged strategy, as demonstrated in [55]:

- Evaluate the current situation and assess whether or not it is applicable for areas that might gather or handle PII. The data stream was also mapped and recorded.
- Identify risks and gaps: Gap analysis was done against GDPR criteria over and above key cybersecurity standards such as ISO27001 and the China Cybersecurity Law.
- Improve and correct the compliance situation: define roles and responsibilities for security and privacy, improve VeChain proposal to adopt the principle of "privacy by design" and provide customers with the right to be forgotten, data deletion and portability

Apart from VeChain, some other significant blockchain platforms introduce digital currencies and have the main aim the supply chain digitalization and development. Among them, the most notable and promising ones are Waltonchain[56][57][58], Ambrosus[56][58][59][60], OriginTrail[56][61], Te-Food[62][63][64] and Devery[64][65]. Table 1 represents an overview of these initiatives and can be found below:

Table 1: Alternative Blockchain Platform Proposals

For Alternative Blockchain Platforms, the name of the platform, the principal infrastructure it is established on, the cryptocurrency/token it creates, as well as some unique characteristics and the method of privacy-preservation can be found in this table

Proposal	**Based on**	**Token**	**Characteristics**	**Privacy-Preservation**
Waltonchain	Go Ethereum consensus mechanism and smart contracts	WTC	Integrates physical and digital worlds by tracking goods and offering consumers extensive data about the process. Intends to achieve "consensus, co-governance,co-sharing and co-integration of IoT data". Focuses on proper management, smart agriculture, smart food traceability among others.	- RFID chip design with hash-and-signature-based data self-verification - Data storage and query index - Hybrid PoS and PoW consensus mechanisms
Ambrosus	Originally Ethereum \Now own platform	AMB	Combines high-tech sensors, blockchain and smart contracts to ensure food product quality, safety and provenance. Works on individualized tag technologies, food-grade tracers and biosensors.	- System of interconnected quality assurance sensors - Smart contracts
OriginTrail	Ethereum	TRAC	Ecosystem built on a token economy with no random charges for direct connections between users and network nodes. Aims for more transparency, collaborativeness, fairness and trustworthiness	Privacy-preservation inherited from Ethereum
Te-Food	Ethereum	TONE	Farm-to-table food traceability method that aims to democratize accessibility to food-related facts as common property, lower the extent and impact of epidemics and frauds, while assisting small farms in becoming more competitive.	- Cost effective 1D/2D and RFID identification tools - Smart contracts
Devery.io	Ethereum	EVE	Works on the Devery Protocol, a decentralized validation system for Ethereum that enables parties to create unique signatures for any items that are sold, issued or exchanged via the internet. Both suppliers and clients may verify the authenticity of a product, lowering the number of counterfeititems in the supply chain.	Privacy-preservation inherited from Ethereum

6.4 Use Cases in Food Supply Chain

Multiple sources, such as [3],[12],[66],[67],[68],[69],[70],[71],[72],[73],[74],[75],[76],[77] were analysed, to be able to create an overview of use cases in the food sector of the supply chain. This overview is presented in

Table 2, where the most important characteristics of each use case were the Initiator (or the Project Name), the technologies it relied on, a short description of the case, and its main focus.

7 Main Results and Discussion

In [78], the evolution of blockchain applied to supply chains is researched, by the analysis of 271 blockchain projects since the inception of the blockchain technology until June 2020. Some of the key takeaways are:

- Agriculture/Grocery (Food) leads in terms of sectors, accounting for 40% of the dataset over all years, owing to the importance of food safety and the capacity to track and trace food items.
- When it comes to the supply chain application areas, the majority (66 per cent) are concerned in the product tracing category.
- Ethereum, used by 23% of all initiatives, and Hyperledger, utilized by 21%, are the most popular blockchains.
- Blockchain acceptance has shifted from Ethereum (most common in 2015, 2016 and 2017) to Hyperledger (most popular in 2018, 2019 and 2020). The VeChain platform began to be included in 2018, with fewer than 5% applicability, then grew to more than 20% in just two years, in 2020.
- According to the kind of head organization, Ethereum is the most popular platform for startups, while Hyperledger is most favoured for consortia and public organizations. VeChain is utilized in roughly 10% of government efforts, the category in which it is most popular.

These results, amalgamated with the overviews created in Tables 1 and 2, show a great ascendance of the two major technologies mentioned afore: Ethereum and Hyperledger Fabric. Nevertheless, VeChain seems to have a vital word to say in the future. Projects such as Ambrosus, Te-Food, or OriginTrail are mostly constructed or inspired by the beforementioned two main infrastructures or are developed in the same manner, in the case of Hyperledger Sawtooth. The exordium of cryptocurrencies develops the field and makes people get involved more in the domain. We can visually examine that most of the initiatives are fixated on transparency, traceability and provenance, as this focus accounted for almost half of the initiatives presented in Table 2. However, countless others concentrate on aspects such as economic benefits, social impact, or the management of food integrity and safety. This variety is a very positive element, as all these aspects are interlinked to contribute to a more efficient and better functioning supply chain industry.

After reviewing several investigations, a wide range of blockchain technology applications were discovered in the field of the food supply chain. Cryptocurrency-based blockchain platforms are present, on top of a detailed overview on privacy-preserving techniques in blockchain and their pertinence in the application of the infrastructure on the supply chain. As a result, varied ways subsist to address the link between privacy and supply chain applications in the blockchain.

According to [79], the ZKPs, Pedersen commitment, and secure MPC deliver great anonymity and are the most significant technologies that have been researched and applied most to numerous digital currencies additionally to other application scenarios, such as Zerocoin, Zerocash, and Hawk. Nonetheless, existing blockchain privacy structures are far from flawless, and other issues need to be addressed and resolved. Among the most difficult aspects of privacy-preserving approaches is that to be computationally feasible, a privacy-preserving system should only change a tiny portion of the blockchain state in each transaction. As a result, statistical studies are able to uncover information; at the very least, they are capable of detecting trends[41]. Therefore, no universal method can solve the privacy issue in the supply chain. A proposal combining infrastructural aspects such as the parallel subsection storage model, Differential Privacy and the lack of trust in external parties for generating smart contracts was suggested. This procedure would also combine legal obligations such as privacy by design, self-sovereign identification and the "right to be forgotten". It is not yet clear whether this approach is more effective than existing techniques, but it is definitely worth investigating.

Nevertheless, certain limitations keep the research paper up to the current state. One of the best examples is the lack of detailed data about which privacy methods are utilized by the blockchain projects presented in Table

Table 2: Use Cases in Food Supply Chain

Most significant aspects of multiple Use Cases in Food Supply Chain are presented in the following table, such as the Initiatior (or the Project Name), the technologies it relies on, a description of the use case, and its primary focus

Led by / Project Name	Based on	Use Case Description	Focus	Comments
AgriBlockIoT	IoT devices	Tool for connecting IoT devices for creating and receiving digital data along the agri-food supply chain	Supervision and Management	
Albert Heijn / Refresco	PowerChain	Get the orange juice production chain open so that consumers may receive as much information as possible.	Transparency and Traceability	Scanning a QR code on an orange juice box allows you to track the item's whole journey from Brazil to the Netherlands.
Ambrosus Project	Ambrosus	Ensures complete openness and access to all information about baby food at all phases of manufacture.	Transparency and Traceability	Link food quality sensor devices that collect accurate statistics on the internal composition of food as well as the exterior environment in which it is consumed.
Blockchain for agri-food	OriginTrail protocol	Table grapes from South Africa are the subject of this PoC blockchain application.	Food Integrity	
FarmShare	IoT, FarmShare token	Combining token-based equity shares and automated administration, it generates new kinds of property ownership and self-sufficient local economies.	Small Farmers Support	
Food Data Market	OriginTrail protocol	New business models for the future of sustainable food supply chains are being supported.	Data Sharing for Sustainability	It is facilitated by a privacy-by-design strategy, which allows farmers and unions to reclaim ownership of their data, offer it a reasonable price, and sell it to supply chain allies that appreciate it.
Future Farm	IOTA Technology	Establish a nationwide marketplace for Round Bales and a new data infrastructure to enable farmers to manage their supply of Round Bales.	Higher Transparency and New Data Infrastructure	Through the DigitalTwin idea, the technology may represent actual assets such as a Round Bale.
Intel	Hyperledger Sawtooth	Sensory equipment is used to capture and store information regarding fish location.	Traceability of the Seafood supply chain	Sawtooth, another framework of Hyperledger, It may be utilized for both permissioned and permissionless blockchain systems, whereas Fabric is intended for permissioned networks.
Louis Dreyfus	Blockchain-driven agriculture commodity trade	Allows for speedier transactions, allowing farmers to get paid sooner while avoiding price pressure and retroactive payments	Economic Benefits	60.000 tons of American soybeans were sold to the Chinese government, resulting in an 80 percent reduction on overall logistics.
Maersk	HyperLedger Fabric	Mandarin oranges were monitored from California and pineapples from Columbia to Rotterdam, enabling end-to-end supply chain insight.	Digitalizing Global Trade	
Moyee Coffee	Stellar (payment network) / Bext360	In an initiative in Ethiopia, all participants were given access to data throughout the whole supply chain, and tokens increased in value as coffee beans moved through the supply chain.	Social Impact	
Paddock to plate	BeefLedger	A research effort aims to follow beef along the production-to-consumption cycle.	Food Integrity	
Provenance	Ethereum	From fishermen to wholesalers, tuna fish was traced throughout the supply chain.	Product Provenance and Traceability	A smartphone might be used to trace the entire chronology. To verify the provenance of a specific fish, digital tokens were utilized.
ShipChain	Ethereum	Increase the flow of information among logistics providers.	Lower Costs, Theft Reduction and Improvement of Transaction Times	Makes use of Track and Trace system, while utilizing smart contracts
Te-Food Project	Te-Food	Te-Food technology, built on Blockchain, is used to track chicken and eggs in 22 Vietnamese areas.	Transparency and Traceability	
The Other Bar	FairChain (Hyperledger Fabric)	Financial tokens are implemented by inserting a 0.25â¬ QR code on all the chocolate bars.	Financial Tokens	The token can be gifted to help plant a cocoa tree or retained to get a discount on the next order.
Trust Your Supplier	HyperLedger Fabric	Purchaser may access the profiles of their linked providers and the history of actions on a cross-industry network and a blockchain-secured system, which speeds onboarding and reduces risk.	Supply Data Management Inefficiencies	
Un World Food Programme	Devery.io	Monitoring the quality of meals served in Tunisia's more than 4000 schools.	Food Tracking	The Devery Protocol is interoperable with NFC and RFID chips, but also barcodes and QR codes.
Volcity Wine	Waltonchain	In New Zealand, red wine was traced through a system constructed on Waltonchain technology	Product Provenance and Traceability	
Walmart	HyperLedger Fabric	Tracking origin of food products	Product Provenance and Traceability	
World Food Programme (WFP)	Ethereum	More than 100.000 Syrian Civil War refugees from a camp in Jordan received food from entitlements recorded on a blockchain-based computing platform	Reduce Payment cost associated with Cash Transfer	Instead of cash, coupons, or e-cards, refugees use an eye scan to buy groceriesfrom local stores in the camp.
ZetoChain	IoT devices	Environmental monitoring at each point in the cold chain, detecting issues in real time and alerting for immediate response	Food Safety	Customers may scan Zeto tags on items to learn about the product's history. Smart contracts are used.

1. Since no information on the desired topic could be found in the Whitepapers of the proposals or generally anywhere on the Internet, contact with the platforms responsible was attended multiple times utilizing the contact details and email addresses from the official websites. However, no replication was received. Subsequently, efforts were additionally made to contact the developers of the initiatives, but again without prosperity. A final endeavour was made to communicate with the officials and the community around the proposals via Telegram groups, as this is where most discussions around the platforms take place, however with the same outcome.

8 Responsible Research

Literature of all kinds has been selected in the preparation of this study. It is vital not to be biased and only cull sources that fit the research questions and hypothesis. The good aspects of certain elements were discussed, let alone the disadvantages and potential dangers. One of the most vigorous points of this analysis is the immense number of studies accumulated in the Data Amassment phase. This gives a better overview and abbreviates the likelihood of the study going in a one-sided direction, as more unrelated perspectives are presented.

All data has been accumulated from trustworthy sources, as the credibility of the sources cited is one of the main pillars of Responsible Research. All investigations this thesis has been constructed on have been properly cited. There was no single source of inspiration as this is an independent paper, thus no lone precedent study was acclimated and updated with current information. In terms of reproducibility, only publicly available sources from various databases, mentioned in earlier paragraphs, were utilized. Ergo, had this study been conducted in a similar manner and utilizing the same studies, kindred conclusions and results would have been reached. The research environment, as well as the methodology and all cited sources, were mentioned, hence offering transparency from the writer's side.

9 Conclusions and Future Work

The central objective of this investigation is the way privacy is maintained in the food supply chain and how is this achieved through the adoption of the latest blockchain platforms. For starters, a detailed overview of subsisting blockchain privacy procedures is introduced, coupled with current applications of the supply chain, with great examples in Zerocoin, Zerocash and sundry others. Then, the most important initiatives of supply chain crypto were presented, mainly based on the principal pillars of this domain, namely Hyperledger Fabric, Ethereum and the incipient and potentially game-changing network VeChain. Consequently, an overview presenting alternative blockchain platform proposals was engendered, displaying the developed tokens, the characteristics and the privacy-preservation these projects achieve. Another detailed overview exhibiting the most representative use cases in the industry of food supply chain was presented, followed by the main results, discussions and limitations.

It is clear that blockchain is an infrastructure with an astounding perspective that will revolutionize several fields, and the supply chain is one of them. It is true that blockchain introduces illimitable advantages. Nonetheless, we also need to consider the disadvantages and challenges that come with innovation, and privacy is one of the most pertinent aspects, considering the immense quantity of data shared nowadays. Smart contract privacy techniques, GDPR, as well as all the transaction and identity-related privacy methods are relevant and aim to solve privacy issues in this context. However, none of the approaches is perfect, and a further amendment is required in this area. In this direction, an incipient approach cumulating various existing tactics and legal obligations has been proposed.

In a nutshell, blockchain is an exhilarating innovation that has the potential to forever transmute the supply chain as we know it by making it more efficient and profitable. If future works focus on privacy and develop this field, innumerable other advantages arise, as trust grows, consequently making it possible to achieve its full capacity.

Appendix

Table **A**: Privacy Challenges in Blockchain

For the most common privacy challenges in Blockchain, the following table presents the name of the challenge, a short description of it, and a possible solution

Name	**Challenge**	**Solution**
Transaction Linkability	Different addresses of the same user may be linked in token-based blockchains	The number of input addresses in a transaction is reduced by using one-time addresses for each transaction. To collect the returns, the user should generate a new public address.
Private-Keys Management and Recovery	Each transaction in the blockchain is signed with a private key. Privacy leaks and identity fraud can occur if the private keys are hacked. Theft attacks on blockchain wallets (even encrypted ones) are possible [77].	Copy back-ups of the wallet file, paper wallets with QR codes, threshold cryptography, super-wallets, hosting private keys on third-party centralized services (comes with additional risks)
Malicious Smart Contracts	Private keys are used to sign each transaction in the blockchain. If they are compromised, privacy leaks and identity theft may happen. Blockchain wallets (even encrypted ones) are subject to theft attacks [77].	For maintaining a privacy-preserving approach, extra obfuscation methods for running smart contracts, such as Security Multi-Party Computation (SPMC), are required.
Non-Erasable Data & On-Chain Data Privacy	Personal data that has been hashed or encrypted is pseudonymous but not anonymous.	Since the GDPR would not apply to data that is not completely private, totally anonymization of data or storing personal data off-chain must be performed. [89] provides for continuous insertion to hashlinked documents while also allowing for record deletion. Lition is a decentralized blockchain that enables private data to be stored and deleted.
Crypto-Privacy Performance	To ensure complete anonymity in blockchain, cryptographic mechanisms such as ZKP [94] and ZKSNARKS [95] are needed, but most are inefficient because they require computational time to produce and verify proofs.	âNon-interactive zero-knowledge proofs of knowledge (NIZKPoKs) use shorter proofs than traditional ZKP to enhance performance or use symmetric-key primitivesâ
Privacy-Usability	Smart contracts are difficult to build for inexperienced developers because they aren't familiar enough with the underlying privacy-preserving mechanisms.	Create User-friendly Privacy management
Privacy Interoperability	Some blockchain implementations are fragmented, making it difficult to link them.	Some privacy-preserving building blocks, such as privacy-related data structures and strategies like Verifiable Claims[58] and Decentralized Identifiers[57], are being standardized by the W3C.

Table **B**: Mixing Services

The following table presents certain Mixing Service Proposals, the year they have been established, a description of their main approach, the privacy protection they achieve, along with the resistance to attacks (*where **D** stands fod DoS Attack, **S** for Sybil Attack and **T** for Theft, as well as the type of Anonymity it achieves and the degree of Centralization (centralized/decentralized)

Proposal	**Year**	**Main Approach**	**Privacy Protection**	**Resistance**	**Anoymity**	**Centralization**
Mixcoin	2013	It applies mix networks to Bitcoin in order to preserve indistinguishability properties in the face of active attackers.	External anonymity	Low for D High for S Accountable for T	Linkable at mixer	centralized
Blindcoin	2015	Extends Mixcoin and employs a blind signature scheme to keep every user's input/output address mapping away from the mixing server	External/internal anonymity	Low for D High for S Accountable for T	Unlikable	centralized
CoinJoin	2013	Extends Mixcoin and employs a blind signature scheme to keep every user's input/output address mapping away from the mixing server	External anonymity	Low for D Low for S High for T	Internal Unlinkable	centralized
Tumblebit	2017	To allow anonymous off-chain payments, the Tumbler, an untrusted intermediary, is used.	External/internal anonymity	High for D High for S Protected for T	Unlikable	centralized
CoinParty	2015	Secure Multi-party Computation (SMPC) and a threshold version of the ECDSA algorithm are used.	External/internal anonymity	High for D High for S Conditioned for T	Unlikable	decentralized
Xim (Sybil-Resistant Mixing)	2014	Focuses on solving sybil, Dos, and timing attacks and defines a two-party bitcoin-compatible mixing protocol.	External/internal anonymity	Middle for D Middle for S Low for T	Unlikable	decentralized
CoinShuffle	2014	To maintain privacy and robustness towards DoS attacks, it is built on the anonymous community contact protocol Dissent [237].	External/internal anonymity	Middle for D High for S High for T	Unlikable	decentralized

Table **C**: Ring Signatures and Zero-Knowledge Proofs Proposals

Table shows certain Ring Signatures and Zero-Knowledge Proof Proposals, by dividing the name of the proposal, a short description of it, as well as the privacy protection method it tackles

Proposal	**Description**	**Privacy Protection**
CryptoNote	To secure the sender's and receiver's anonymity, besides the transaction's data, it combines ring signature, one-time payment, and secret transaction.)	Hiding adresses of participants
Monero	Makes use of CryptoNote: for sender anonymity, it uses ring signatures, Ring Confidential Transactions [125] for number obfuscation, and Stealth Addresses [126] for receiver privacy.	Hiding transaction amount, addresses of participants
RingCT	It is a Monero-specific linkable ring signature system.	Hiding transaction amount, addresses of participants
Zerocoin	It is a Bitcoin-based cryptographic extension that leverages Zero-Knowledge Signature of Knowledge (ZKSoK) on message encryption to allow completely anonymous financial transactions.	Hiding adresses of participants
EZC	Built on Zerocoin, has the ability to disguise transaction amounts and address balances, something Zerocoin does not support. It has a smaller communication overhead.	Hiding transaction amount, addresses of participants
Zerocash	Decentralized anonymous payment mechanism which utilizes zero-knowledge Succinct Non-interactive ARguments of Knowledge (zkSNARKs) to deliver an anonymity-by-design alternative .	Hiding transaction amount, addresses of participants
BulletProofs	Presents a non-interactive ZKP-based protocol that uses brief proofs and does not demand a trusted configuration.	Hiding transaction amount, addresses of participants

References

[1] C.G. Schmidt and S.M. Wagner. "Blockchain and Supply Chain Relations: A Transaction Cost Theory Perspective." Journal of Purchasing and Supply Management, 25(4):100552, 2019.

[2] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges", IEEE Access, vol. 7, pp. 164908-164940, 2019.

[3] A. Kamilaris, A. Fonts, and F. X Prenafeta-Bold . "The Rise of Blockchain Technology in Agriculture and Food Supply Chains." Trends in Food Science and Technology, 91:640-652, 2019.

[4] AID Tech. "How Blockchain Technology is Enabling International Aid to be Delivered Transparently", 2017.

[5] L. Tom, "Blockchain technology trialled to tackle slavery in the fishing industry", the Guardian, 2016. [Online]. Available: https://www.theguardian.com/sustainable-business/2016/sep/07/blockchain-fish-slavery-free-seafood-sustainable-technology. [Accessed: 25- May- 2021].

[6] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu. "Privacy Preservation in Permissionless Blockchain: A survey." Digital Communications and Networks, 2020.

[7] N. Gupta. "A Deep Dive Into Security and Privacy Issues of Blockchain Technologies." In Handbook of Research on Blockchain Technology, pages 95-112. Elsevier, 2020.

[8] Q. Feng, D. He, S. Zeadally, M.K. Khan, and N. Kumar. "A Survey on Privacy Protection in Blockchain System." Journal of Network and Computer Applications, 126:45-58,2019

[9] W. Kenton, "How Supply Chains Work", Investopedia, May 2021. [Online]. Available: https://www.investopedia.com/terms/s/supplychain.asp. [Accessed: 27- May- 2021].

[10] J. Fernando, "Supply Chain Management (SCM): What You Need to Know", Investopedia, May 2021. [Online]. Available: https://www.investopedia.com/terms/s/scm.asp. [Accessed: 27- May- 2021].

[11] "What Is Blockchain Technology? How Does It Work? | Built In", Builtin.com, 2021. [Online]. Available: https://builtin.com/blockchain. [Accessed: 28- May- 2021].

[12] K. Francisco and D. Swanson. "The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency." Logistics, 2(1), 2018

[13] S. Seibold and G. Samman. "Consensus: Immutable agreement for the internet of value." KPM,2016.

[14] M. Decrypt / Jeff Benson, "What is Proof of Stake? | How it Differs From Proof of Work - Decrypt", Decrypt, May 2021. [Online]. Available: https://decrypt.co/resources/proof-of-work-vs-proof-of-stake. [Accessed: 28- May- 2021].

[15] "What is Proof of Stake? Get the definition here.", Cryptocurrency Dictionary, 2021. [Online]. Available: https://decryptionary.com/dictionary/proof-of-stake/. [Accessed: 28- May- 2021].

[16] "Proof of Authority Explained | Binance Academy", Binance Academy, Dec 2020. [Online]. Available: https://academy.binance.com/en/articles/proof-of-authority-explained. [Accessed: 30- May- 2021].

[17] "The Difference Between On-Chain and Off-Chain Transactions", Medium, Sep 2019. [Online]. Available: https://vertexmarket.medium.com/the-difference-between-on-chain-and-off-chain-transactions-6b5121da9d4c. [Accessed: 01- Jun-
2021].

[18] "What Is Privacy?", Privacy International, 2021. [Online]. Available: https://privacyinternational.org/explainer/56/what-privacy. [Accessed: 01- Jun- 2021].

[19] "Privacy Matters | Privacy International", Privacyinternational.org, 2021. [Online]. Available: https://privacyinternational.org/learning-resources/privacy-matters: :text=Privacy%20is%20foundational%20to%20who,and%20to%20live%20in%20dignity. [Accessed: 02- Jun- 2021].

[20] "What is Privacy", Iapp.org, 2021. [Online]. Available: https://iapp.org/about/what-is-privacy/: :text=What%20does%20privacy%20mean%3Famp;text=Broadly%20speaking%2C%20privacy%20is. [Accessed: 03- Jun- 2021].

[21] D. Simberkoff, "Digital Supply Chain: Privacy and Security Considerations", CMSWire.com, Jul 2018. [Online]. Available: https://www.cmswire.com/information-management/digital-supply-chain-privacy-and-security-considerations/. [Accessed: 03- Jun-
2021].

[22] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka. "Security Services Using Blockchains: A state of the art survey." IEEE Communications Surveys Tutorials, 21(1):858-880, 2019.

[23] Y. Wang, J.H. Han, and P. Beynon-Davies. "Understanding Blockchain Technology for Future Supply Chains: A Systematic Literature Review and Research Agenda." Supply Chain Management: An International Journal, 24, 12 2018.

[24] D. Yaga, P. Mell, N. Roby, and K. Scarfone. "Blockchain Technology Overview." arXiv preprint arXiv:1906.11078, 2019.

[25] C. Cachin et al. "Architecture of the Hyperledger Blockchain Fabric". In Workshop on distributed cryptocurrencies and consensus ledgers, volume 310. Chicago, IL, 2016.

[26] N. Kshetri. "Blockchain's Roles in Meeting Key Supply Chain Management Objectives." International Journal of Information Management, 39:80-89, 2018.

[27] K. Biswas, V. Muthukkumarasamy, and W. L. Tan. "Blockchain Based Wine Supply Chain Traceability System." In Future Technologies Conference (FTC) 2017, pages 56-62. The Science and Information Organization, 2017.

[28] R. Chen. "A Traceability Chain Algorithm for Artificial Neural Networks Using T-S Fuzzy Cognitive Maps in Blockchain." Future Generation Computer Systems, 80:198-210, 2018.

[29] Q. Lu and X. Xu. "Adaptable Blockchain-Based Systems: A Case Study for Product Traceability." Ieee Software, 34(6):21-27, 2017.

[30] K. Toyoda, P.T. Mathiopoulos, I. Sasase, and T. Ohtsuki. "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain." IEEE access,5:17465-17477, 2017.

[31] H, Kim and M. Laskowski. "A Perspective on Blockchain Smart Contracts: Reducing Uncertainty and Complexity in Value Exchange." In 2017 26th International Conference on Computer Communication and Networks (ICCCN), pages 1-6. IEEE, 2017

[32] M.M. Queiroz and S.F. Wamba. "Blockchain Adoption Challenges in Supply Chain: An Empirical Investigation of the Main Drivers in India and the USA." International Journal of Information Management, 46:70-82, 2019.

[33] S. E. Chang, Y. Chen, and M. Lu. "Supply Chain Re-Engineering Using Blockchain Technology: A case of Smart Contract Based Tracking Process." Technological Forecasting and Social Change, 144:1-11, 2019.

[34] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating User Privacy in Bitcoin," Financial Cryptography and Data Security Lecture Notes in Computer Science, pp. 34-51, 2013.

[35] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-Resistant Mixing for Bitcoin", Proceedings of the 13th Workshop on Privacy in the Electronic Society, 2014.

[36] T. Ruffing and P. Moreno-Sanchez."Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in Bitcoin." In International Conference on Financial Cryptography and Data Security, pages 133-154. Springer, 2017.

[37] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts." In 2016 IEEE symposium on security and privacy (SP), pages 839-858. IEEE, 2016.

[38] A. Xiao, "Unlocking the Future of Blockchain Innovation with Privacy-Preserving Technologies - Help Net Security", Help Net Security, Aug 2019. [Online]. Available: https://www.helpnetsecurity.com/2019/08/22/blockchain-privacy/. [Accessed: 05- Jun- 2021].

[39] Y. Fu and J. Zhu. "Big Production Enterprise Supply Chain Endogenous Risk Management Based on Blockchain." IEEE Access, 7:15310-15319, 2019.

[40] R. O'Leary, D. Cawrey, M. J.Casey, D. Morris, I. Allison and M. Shen, "4 Projects Seeking to Solve Ethereum's Privacy Paradox - CoinDesk", CoinDesk, Jun 2018. [Online]. Available: https://www.coindesk.com/four-projects-seek-solve-ethereums-privacy-paradox. [Accessed: 05- Jun- 2021].

[41] Ethereum Foundation, "Privacy on the Blockchain", Blog.ethereum.org, 2021. [Online]. Available: https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/. [Accessed: 07- Jun- 2021].

[42] A. Munro, "The Future of Privacy is on the Blockchain, For Better or Worse | finder.com.au", finder.com.au, Apr 2018. [Online]. Available: https://www.finder.com.au/the-future-of-privacy-is-on-the-blockchain-for-better-or-worse. [Accessed: 07- Jun- 2021].

[43] S. Smith, "Blockchain, Self-Sovereign Identity, And The Future Of Data Privacy", Forbes, Sep 2020. [Online]. Available: https://www.forbes.com/sites/seansteinsmith/2020/09/09/blockchain-self-sovereign-identity-and-the-future-of-data-privacy/?sh=307abe0dea7d. [Accessed: 07- Jun- 2021].

[44] "Gartner Future of Privacy Predictions: Blockchain "Privacy Poisoning"", Tech Monitor, Feb 2019. [Online]. Available: https://techmonitor.ai/policy/future-of-privacy-2019. [Accessed: 07- Jun- 2021].

[45] S. Pooja and M. R. Mundada. "Blockchain in Agriculture and Food Supply Management."

[46] M. Zand, "An Introduction to Hyperledger Fabric", Opensource.com, Sep 2019. [Online]. Available: https://opensource.com/article/19/9/introduction-hyperledger-fabric: :text=The%20Hyperledger%20Fabric%20blockchain%20can,in%20the%20food%20supply%20chain. [Accessed: 07- Jun- 2021].

[47] "Private and Confidential Transactions with Hyperledger Fabric", IBM Developer, 2021. [Online]. Available: https://developer.ibm.com/technologies/blockchain/tutorials/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowledge-proof. [Accessed: 10- Jun- 2021].

[48] S. Brotsis, N. Kolokotronis, K. Limniotis, G. Bendiab, and S. Shiaeles, "On the Security and Privacy of Hyperledger Fabric: Challenges and Open Issues," 2020 IEEE World Congress on Services (SERVICES), 2020.

[49] C. Ma, X. Kong, Q. Lan, and Z. Zhou. "The Privacy Protection Mechanism of Hyperledger Fabric and its Application in Supply Chain Finance." Cybersecurity, 2(1):1-9, 2019.

[50] "Ethereum Whitepaper | ethereum.org", ethereum.org, 2021. [Online]. Available: https://ethereum.org/en/whitepaper/. [Accessed: 10- Jun- 2021].

[51] E. S. Kumar. "Preserving Privacy in Ethereum Blockchain." Annals of Data Science, pages 1-19, 2020.

[52] "VeChain price today, VET live Marketcap, Chart, and Info | CoinMarketCap", CoinMarketCap, 2021. [Online]. Available: https://coinmarketcap.com/currencies/vechain/. [Accessed: 10- Jun- 2021].

[53] "What is VeChain - The World's Leading Blockchain Application Platform Driven by Enterprise Adoption", Vechain.com, 2021. [Online]. Available: https://www.vechain.com/. [Accessed: 11- Jun- 2021].

[54] "VeChain Whitepaper | VeChain Builders", Vechain.org, 2021. [Online]. Available: https://www.vechain.org/whitepaper/. [Accessed: 11- Jun- 2021].

[55] "How VeChain is Tackling GDPR Compliance", Medium, Jul 2018. [Online]. Available: https://vechainofficial.medium.com/how-vechain-is-is-tackling-gdpr-compliance-5431e3d13e0c. [Accessed: 12- Jun- 2021].

[56] "Top 10 Supply Chain Blockchain Projects, Rated and Reviewed - Bitcoin Market Journal", Bitcoin Market Journal, Jun 2019. [Online]. Available: https://www.bitcoinmarketjournal.com/supply-chain-blockchain-projects/. [Accessed: 12- Jun- 2021].

[57] "Supply Chain Cryptocurrencies on Blockchain - Quantaloop", Quantaloop.io, 2021. [Online]. Available: https://quantaloop.io/supply-chain-cryptocurrencies-on-blockchain-wtc-ven-trac-qnt/. [Accessed: 12- Jun- 2021].

[58] H. Agrawal, "These Are The Top Supply Chain Management Based Cryptocurrency Projects", coinsutra.com, 2020. [Online]. Available: https://coinsutra.com/supply-chain-management-cryptocurrency-blockchain-projects/. [Accessed: 13- Jun- 2021].

[59] "Ambrosus Whitepaper", The Whitepaper Database, Aug 2020. [Online]. Available: https://www.allcryptowhitepapers.com/ambrosus-whitepaper/. [Accessed: 13- Jun- 2021].

[60] "Supply Chain Management Alt Coins Are Set to Explode", NewsBTC, Oct 2020. [Online]. Available: https://www.newsbtc.com/news/company/supply-chain-management-alt-coins-are-set-to-explode/. [Accessed: 13- Jun- 2021].

[61] B. Rakic, T. Levak, Z. Drev, S. Savic, and A. Veljkovic. "First Purpose Built Protocol for Supply Chains Based on Blockchain." [Online], 2017.

[62] "TE-FOOD Whitepaper", The Whitepaper Database, Feb 2021. [Online]. Available: https://www.allcryptowhitepapers.com/te-food-whitepaper/. [Accessed: 15- Jun- 2021].

[63] H. Malviya, "Top 5 Cryptocurrency Projects in Supply chain", Blockchain, Sep 2018. [Online]. Available: https://itsblockchain.com/top-5-cryptocurrency-projects-in-supply-chain/. [Accessed: 15- Jun- 2021].

[64] B. Lester, "Best Supply Chain Blockchain Projects, Rated and Reviewed for 2019", Remedi, 2019. [Online]. Available: https://www.remedi.com/blog/best-supply-chain-blockchain-projects-rated-and-reviewed-for-2019. [Accessed: 15- Jun- 2021].

[65] "Devery Whitepaper", The Whitepaper Database, Aug 2020. [Online]. Available: https://www.allcryptowhitepapers.com/devery-whitepaper/. [Accessed: 15- Jun- 2021].

[66] "Introducing Food Data Market", Medium, Mar 2020. [Online]. Available: https://medium.com/origintrail/introducing-food-data-market-3ef055e1899c. [Accessed: 15- Jun- 2021].

[67] "Ambrosus Protects Baby Food Quality via Blockchain Smart Contracts", Medium, Aug 2017. [Online]. Available: https://medium.com/@ambrosus/ambrosus-protects-baby-food-quality-via-blockchain-smart-contracts-8cc51c5dd7bf. [Accessed: 16- Jun- 2021].

[68] A. Lashuk, "Blockchain use cases in food industry | OpenLedger Insights", Openledger.info, Jan 2020. [Online]. Available: https://openledger.info/insights/blockchain-food-industry/. [Accessed: 16- Jun- 2021].

[69] "Farm Share: Nonprofit Organization: United States", Farm Share, 2021. [Online]. Available: https://www.farmshare.org/. [Accessed: 17- Jun- 2021].

[70] "Beefledger - Blockchain Solution for the Australian Beef Supply Chain", Beefledger.io, Mar 2021. [Online]. Available: https://beefledger.io/. [Accessed: 17- Jun- 2021].

[71] "Hyperledger-Powered Supply Chain Solutions in Action - Hyperledger", Hyperledger, Oct 2020. [Online]. Available: https://www.hyperledger.org/blog/2020/10/28/hyperledger-powered-supply-chain-solutions-in-action. [Accessed: 17- Jun- 2021].

[72] A Peter. "In China, You Can Track Your Chicken On - You Guessed It - The Blockchain." Fast Company, 82, 2017.

[73] L. Ge, C. Brewster, J. Spek, A. Smeenk, J. Top, F. van Diepen, B. Klaase, C. Graumans, and M. de Ruyter de Wildt. "Blockchain for Agriculture and Food: Findings from the Pilot Study." Number 2017-112. Wageningen Economic Research, 2017.

[74] D. Mao, F. Wang, Z. Hao, and H. Li. "Credit Evaluation System Based on Blockchain for Multiple Stakeholders in the Food Supply Chain." International journal of environmental research and public health, 15(8):1627, 2018.

[75] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda. "Blockchain-Based Traceability in Agri-Food Supply Chain Management: A Practical Implementation". In 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), pages 1-4. IEEE, 2018.

[76] Y. Kayikci, N. Subramanian, M. Dora, and M. S. Bhatia. "Food Supply Chain in the Era of Industry 4.0: Blockchain Technology Implementation Opportunities and Impediments from the Perspective of People, Process, Performance, and Technology." Production Planning Control, pages 1-21, 2020.

[77] "Walmart Case Study - Hyperledger", Hyperledger, 2019. [Online]. Available: https://www.hyperledger.org/learn/publications/walmart-case-study. [Accessed: 18- Jun- 2021].

[78] N. Vadgama and P. Tasca. "An Analysis of Blockchain Adoption in Supply Chains between 2010 and 2020." Frontiers in Blockchain, 4:8, 2021.

[79] D. Wang, J. Zhao, and Y. Wang. "A Survey on Privacy Protection of Blockchain: The Technology and Application." IEEE Access, 8:108766-108781, 2020.