How Blockchain Enhances Supply Chain Management: A Survey

Denisolt Shakhbulatov[2], Jorge Medina [3], Ziqian Dong[1], and Roberto Rojas-Cessa[3]
[1]Department of Electrical and Computer Engineering
[2]Department of Computer Science
College of Engineering and Computing Sciences
New York Institute of Technology, New York, NY 10023
[3]Networking Research Laboratory
Helen and John C. Hartmann Department of Electrical and Computer Engineering
New Jersey Institute of Technology, Newark, NJ 07102
Email: {dshakhbu, ziqian.dong}@nyit.edu, {jmc237, rojas}@njit.edu

Providing transparency and trust among participants and stakeholders and ensuring an efficient operation are current supply chain challenges. These challenges are difficult to resolve because the records of supply chains may be exposed to alterations by participants. Blockchain technology has been identified as a promising solution to resolve these challenges. In this paper, we introduce blockchain and survey recent blockchain frameworks that address some of the supply chain challenges. We describe the components and operation of these blockchain frameworks. We identify the objectives and motivation in each of the surveyed use cases and highlight the advantages and disadvantages of each adopted framework. We analyze how the reported blockchain frameworks address different supply chain challenges. We present a comparative summary of existing literature on blockchain for supply chain. We also summarize the properties of a blockchain framework for its successful adoption in future supply chains and discuss several remaining challenges and opportunities.

Index Terms—**Supply chain, provenance, blockchain, industries, distributed ledger, supply chain management, consensus algorithms, smart contracts, survey**

I. Introduction

SUPPLY chain is a set of sequential stages in the manufacturing, transportation, storing, or distribution of a product [?]. Each stage may be handled by one or many companies, suppliers, or stakeholders. Supply chain plays a critical role in the global economy [?]. The International Trade Administration reports that supply chain transactions account for over 76% of the world trade [?]. Large corporations outsource their assembly lines to low-cost regions to decrease production costs. The stages of the supply chain have been further divided and therefore, handled by an increasing number of affiliates. Supply chains have become more global, complex, and interdependent across stages [?].

Supply chain involves various participants and stakeholders and numerous processes in multiple stages. It is difficult to keep track of the processes, materials, and the ownership at different stages. Moreover, stages of a supply chain are often located at different places and sometimes across different countries. The supply chain complexity imposes administrative challenges for an efficient supply chain management.

Companies aim to address the increasing supply chain complexity by adopting different technologies such as barcodes, radio-frequency identification (RFID), and global positioning system (GPS) to directly collect information from the processes and stages of the supply chain. Data analytics is another technology that is increasingly used for stock management and demand prediction [?].

Although companies use data collection technologies as those described above, information on supply chain processes and changes of product ownership need to be resilient to accidental or intentional modifications. Moreover, supply chains must provide transparency so that stakeholders may have access to data on the status of the supply chain.

Today's supply chains need to be more reliable than ever. Disruptions in the supply chain can create significant losses for companies in both short and long terms and increase costs for end customers. Such companies need to create fast and agile solutions to meet dynamically changing demands [?]. Businesses and customers are raising new demands for information on a product, such as authenticity, origin, quality, and sustainability. These demands are associated with the supply chain of a product. However, recorded data in a supply chain can be altered by participants and, at the same time, its data may be inaccessible to customers.

To resolve most of the supply chain challenges, data must be kept immutable and accessible. Blockchain is a promising technology with the potential to satisfy many of the supply chain challenges. Blockchain is a distributed and immutable ledger that provides a trustable record that cannot be manipulated or tampered with [?], [?]. Its distributed architecture makes it immune to manipulation by a centralized authority. Blockchain was first introduced by Bitcoin in 2008 [?]. It has been considered a solution to address the supply chain challenges for different industries [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?]. Recent advancements in computing, sensing, and mobile

This project has received funding in the framework of the Joint Programming Initiative Urban Europe, with support from the European Union Horizon 2020 Research and Innovation Programme under grant agreement No. 730254. This material is based upon work partially supported by the National Science Foundation Grant Awards No. 1830718 and 1856032.

technologies have made it possible to apply blockchain in several industries, including healthcare [?], [?], [?], [?], [?], energy management [?], [?], [?], [?], [?], entertainment [?], [?], aircraft [?], vehicular network [?], and construction [?].

In this paper, we survey existing blockchain approaches applied to supply chains with a focus on different industries. These industries include food, wine, pharmaceutical, healthcare, and others. We highlight the objectives and challenges reported for each industry and identify the proposed blockchain frameworks that address these challenges. We also discuss challenges and opportunities for future blockchain frameworks and their applications in supply chain.

The remainder of the paper is organized as follows. Section ?? introduces supply chain and its features and describes the challenges that its management faces to achieve high efficiency and efficacy. Section ?? introduces blockchain frameworks that have been proposed for management of supply chains and others that can potentially be used for such a purpose. Section ?? analyzes blockchain framework adoptions that have been proposed to address various supply chain challenges in different industries. Section ?? discusses opportunities and challenges of the application of blockchain on supply chain management. Section ?? presents our conclusions.

II. Supply Chain

A. Supply Chain Management

A supply chain can be highly complex as it may comprise a large number of stages and all the involved parties need to keep track of the development of the product at each stage. Fig. ?? illustrates an example of the stages of a supply chain. The number of stages may increase in proportion to the complexity of the product. Moreover, a supply chain may be a set of several intertwined supply chains because some products may be parts for another.

As an example, suppliers provide raw materials to the processing units that manufacture parts of a complex product. The parts are then assembled into a complex product as the final product. These final products are then distributed by wholesalers or distributors. The involved parts could be distributed among various geographic locations where logistics are handled by importers and exporters across country lines. Further distribution of the products is handled by retailers who bring them to the end customers. The effectiveness of how materials, parts, and products are moved along the supply chain can affect the efficiency of the supply chain and, in turn, the cost of the product [?].

Some of the functions of supply chain management are inventory and warehouse management, supplier management, transportation, bookkeeping, and other operations [?]. Often, the handling of the product, as it passes through the supply chain, is a transaction made between participants. Transactions should be recorded accurately and reliably. Trust amongst the supply chain parties ensures smooth and seamless transactions. Moreover, for newly introduced trading partners, supporting technology that provides background information about the involved parties can speed up the process of building such partnerships.

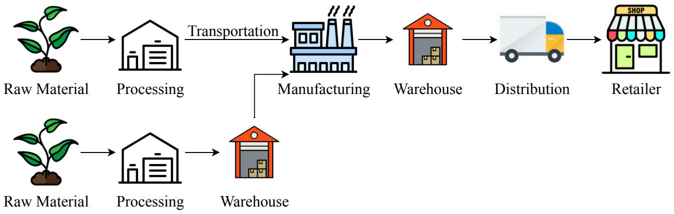


Fig. 1: An example of a supply chain.

B. Challenges in Supply Chain and its Management

The complexity of supply chain management has increased by not only directing the flow of goods but also the flow of information [?]. Although technology has digitized and automated various functions of supply chain management, some challenges remain for making the supply chain more efficient, reliable, and secure. In this section, we outline the challenges that supply chains need to address to ensure their efficiency and trust among their stakeholders.

1) Provenance

Provenance is a record of ownership over time [?]. Tracking and traceability are functions enabled by provenance. Tracking materials and the origin of a product is a complex operation. For example, a distributor may acquire produce from various farms and then distribute it to customers in the food industry. In the case of product recalls, it usually takes a long time to trace back the source of a contaminated product, and yet, sometimes the location is not precise. A system with tracing capability would overcome this issue.

Counterfeit detection is a popular application of provenance. Having a record of the product's provenance may help detect counterfeit products or verify a product's originality. Such a record is directly associated with the product's supply chain, but the record has to be both accessible to some stakeholders (e.g., consumers) and unalterable by supply-chain stakeholders.

A product passes through different stages of its supply chain and spends a different amount of time in each one. To oversee the operation of its supply chain, tracking is a necessary feature. For example, the shipment of a product is often carried out by a third-party logistics company and that makes real-time tracking by supply-chain participants challenging. In addition, having information on the status of the product and forecasting its progress can facilitate data-driven strategies that benefit the management of the supply chain and its stakeholders.

An analysis of the supply chain with real-time tracking can provide information about what occurs in the different stages. This information can be used to evaluate the performance and efficiency of suppliers and to identify and mitigate potential risks.

2) Performance Improvement

Performance of a supply chain can be defined by different key indicators, such as the time a product spends on each of its stages, the cost of manufacturing a product, and production yield [?]. Because the performance of the supply chain may directly affect the cost of the product, it must be managed and followed carefully.

3) *Quality Assurance and Quality Control*

Quality assurance and quality control are the compliance of a product, manufacture, or supply chain with a variety of quality attributes set out by the stakeholders, customers, or regulatory agencies [?]. These features may incorporate not only safety guarantees for consumer products but also compliance with established standards.

4) *Sustainability*

A study by McKinsey states: “The typical consumer company’s supply chain creates far greater social and environmental costs than its operations, and that accounts for more than 80% of greenhouse gas emissions and more than 90% of the impact on air, land, water, biodiversity, and geological resources" [?]. A sustainable supply chain must consider its impact on the environment and use environmentally-friendly materials and processes, so that it can reduce greenhouse gas emissions along its stages. A supply chain must account for its production of greenhouse gas emissions and other contaminants in a reliable and unbiased way. Such accountability would be beneficial for environmental impact evaluation by stakeholders and regulators [?].

Because of the broad variety of parties involved in a supply chain, tracking and quantifying its environmental impact is challenging. These tasks often incur additional costs. Although some large manufacturers may report their product carbon footprint [?], the numbers are often estimates. Therefore, there is a need for widely deployable standards on environmental impact for industries to follow.

5) *Transparency*

Transparency refers to the availability of and accessibility to information about the supply chain by trading partners, shareholders, consumers, and regulatory bodies [?]. Transparency makes data about the status of processes and materials in their supply chain accessible stakeholders.

Transparency in a supply chain has shown to have a positive impact on business reputation [?]. There has been an increasing demand for transparency of supply chain by both businesses and consumers. This feature requires that supply chain data remain immutable to ensure trust amongst the involved parties. Transparency can be partial to some stakeholders; some information about the supply chain may be accessed by only a group of designated parties. Because the cost incurred by the stages of the supply chain affects the final cost of the product, transparency enables accurate cost calculations and the exposure of irregular operations along the supply chain [?], [?].

6) *Data Privacy and Confidentiality*

Sensitive and proprietary information about a supply chain such as financial records needs to be accessible only to some stakeholders. An example of this information includes the cost of raw materials, benefits, surpluses, etc. Any information about transactions performed between different parties must be kept confidential but verifiable.

III. Blockchain Frameworks

A blockchain is a distributed immutable ledger that is used to record transactions performed between different users without resorting to a centralized and trustable party. Immutability is the driving feature of blockchain; it facilitates building trust among users by providing a permanent and verifiable record of transactions. A blockchain comprises a peer-to-peer network of participant nodes, a distributed ledger consisting of immutable blocks of data, transactions recorded in the blocks, smart contracts to execute the transactions, and a consensus algorithm that decides the proposer of the next block. Fig. **??** shows the components of a blockchain.

Participant nodes in a blockchain can be either a client, a light client application (light node), or a miner/validator (full node). A blockchain user communicates through the client node. A client node is a participant that generates transactions. A light node keeps track of the blockchain’s headers to verify the validity of a client’s transactions. A full node participates in the consensus process and proposes and validates blocks, records transactions by executing functions contained within a smart contract, and appends verified blocks to its local copy. Different blockchain frameworks may define the functions of miners and validators differently. Therefore, we call a node miner and validator in each blockchain framework according to their usage.

A block is sequentially linked to a previously recorded block using a hash pointer. The hash pointer contains the hashed information of the contents of the previous block and that guarantees the sequence of the blocks and the integrity of the data. The result is an immutable distributed ledger. Every block of data contains a group of verified transactions and a header with metadata including a proof of block authenticity and a hash pointer pointing to the previous block.

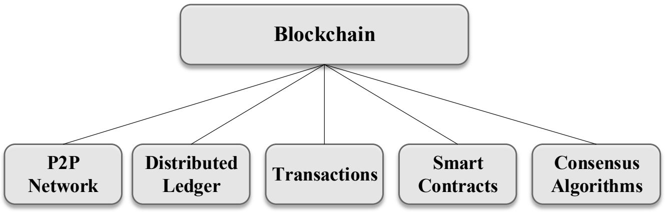


Fig. 2: Components of a blockchain.

A. *Classification of Blockchains*

Blockchain may achieve different levels of decentralization and be classified into permissionless (or public), permissioned (or private), and hybrid architectures. Table **??** shows differences between permissionless and permissioned blockchains. In a permissionless blockchain, access to the network and participation in the consensus algorithm is open to anybody who wishes to participate. Participants can use public keys that enable pseudo anonymous identities and replace them at any time, without requiring to reveal their real identities. Permissionless blockchains use a

TABLE I: Comparison of permissionless and permissioned blockchains.

Permissionless	Permissioned
• Open access to the network and consensus	• Restrictive access to the network and consensus
• Complex consensus algorithms	• Light consensus algorithms
• Low transaction throughput	• High transaction throughput
• Scalable consensus	• Consensus with limited scalability
• Incentive mechanisms	• No need of incentive mechanisms

consensus algorithm that defines strict rules to accept proposed blocks and an integrated incentive mechanism that rewards honest participation. However, decentralization is achieved at the expense of low transaction throughput, i.e., the number of recorded transactions per second (tps).

In a permissioned or private blockchain, access to the network, and participation in the consensus algorithm is restricted; participants of a permissioned blockchain are required to register before they can participate in the blockchain. Because the identities of the participants in a permissioned blockchain are known to the registered members, malicious behavior can be detected by byzantine fault tolerant (BFT) consensus algorithms. Distributed consensus algorithms are said to be crash fault tolerant (CFT) if they can tolerate a number of crashed nodes, i.e., nodes that stop working. Similarly, consensus algorithms are said to be BFT if they are both CFT and can tolerate a number of nodes acting maliciously while appearing to be working normally. Blockchain consensus algorithms can either be CFT or BFT. For a detailed description of distributed consensus algorithms, the readers are referred to [?]. However, BFT consensus algorithms may not scale well because their complexity and overhead increase as the number of validators grows.

Incentive mechanisms are not needed to reward honest participation in permissioned blockchains because validators are granted a level of trust. These blockchains provide data access to the participants in the distributed ledger. Such features allow a permissioned blockchain to use a light-weight consensus algorithm that can achieve high transaction throughput, but at the expense of diminished decentralization.

A hybrid blockchain combines the features of both permissioned and permissionless blockchains. It inherently includes the combination of data privacy and high throughput of permissioned blockchains and the high level of decentralization of permissionless blockchains. Such a blockchain has a private and a public ledger. It records sensitive data in a private ledger that are accessible to some designated stakeholders and non-sensitive data in a public ledger that are available to all participants.

B. Blockchain Consensus Algorithms

Blockchain consensus algorithms define the set of rules for miners or validators to agree on a common truth. As shown in Fig. **??**, blockchain consensus algorithms may include the following five components: block proposal, block validation, information propagation, block finalization, and incentive mechanism [?]. Yet, not all blockchain consensus algorithms implement all five components.

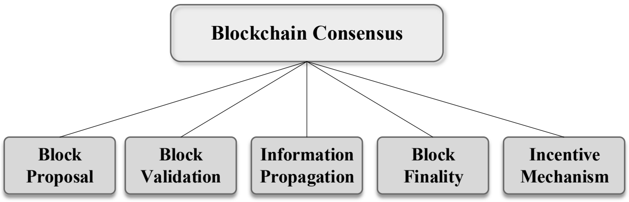


Fig. 3: Components of a consensus algorithm.

Block proposal is a process where miners or validators decide the next proposer of a block. For security reasons, a block proposal mechanism in permissionless blockchains requires a minimum inter-block proposal time. In addition, miners or validators are required to provide Proof of Work (PoW) or Proof of Stake (PoS), to earn the right to propose the next block.

Block validation is the process to verify that received blocks are syntactically correct. A block is valid when it includes the solution to a cryptographic puzzle and the verified digital signatures of the participants in the transactions recorded in the block.

In *information propagation*, full nodes broadcast blocks to the peer-to-peer network. They must follow the broadcast or dissemination protocols of a framework.

Block finality is the process to make the recording of a block irrevocable once it's committed to the distributed ledger. Once it is received and verified by participant nodes, a block is appended to the local copy of the distributed ledger that is maintained by full nodes. A consensus algorithm can be classified as either deterministic or non-deterministic according to how it proposes a block. A consensus algorithm is deterministic when it proposes only one block at a time. This proposal occurs after a leader is selected in every round. On the other hand, a consensus algorithm is non-deterministic when it proposes two or more blocks at a time. Because it is possible to have blockchain forks in the latter case, i.e., two different valid blocks that extend two different chains, a full node must decide which chain to extend and in this way, to remove forks. A full node can decide to extend the longest-chain or the chain that has received the majority of votes from a group of validators.

Incentive mechanisms are used to prevent abnormal or malicious miner behavior by rewarding the miners who follow the rules. In a permissionless blockchain, miners are pseudo-anonymous. Therefore, miners could collude and propose invalid blocks and invalidate the main blockchain. Some consensus algorithms may implement an incentive mechanism to prevent such malicious miner behaviors.

Moreover, consensus algorithms may also establish penalties for miners that act maliciously.

C. Confidentiality

Clients use a public key as a pseudo-identity to participate in the network and a private key to digitally sign transactions. Transactions hold digital signatures that are used to ensure that the state of the ledger (i.e., the ownership and distribution of the assets) is only modified by legitimate clients, which are authenticated through their public and private keys. However, the contents, including sensitive data, of both transactions and operations performed by smart contracts are recorded in plain text in every local copy of the distributed ledger. Some blockchain frameworks address this data privacy problem using cryptographic algorithms and methods, e.g., zero knowledge proofs (ZKPs), to encrypt sensitive data of both transactions and operations in smart contracts before sending them to the blockchain. However, this feature comes at the expense of lowering the performance. In particular, permissioned blockchain frameworks are designed to provide data privacy guarantees by limiting access to some portion of the distributed ledger to the public. These guarantees can also be provided by segmenting the blockchain into small independent blockchains where each of them is used in a different section of an organization. Other blockchain frameworks aim to further enhance data privacy by delegating the execution of operations in smart contracts to only a pre-selected set of participants.

D. Smart Contracts

Smart contracts are self-executable computer programs that implement trading terms in a transaction that are verified by every full node. The execution of some smart contracts may cause the entire blockchain to halt when contracts have errors, such as non-deterministic functions, caused by coding mistakes or attacks. To address this problem, some blockchain frameworks bound the amount of running code by establishing service fees for every executed line of code. Therefore, only deterministic code is allowed.

E. Performance

Transaction throughput is a common and main performance indicator of a blockchain framework. The performance of a blockchain framework may be determined by the consensus algorithm, the size of the network, i.e., the number of participants, and the block size. Transaction throughput in permissionless blockchains, specifically on PoW-based ones, tends to be low because of the high computational cost of cryptographic puzzles that miners must solve to propose valid blocks. Solving cryptographic puzzles in PoW could be time-consuming and, therefore, limit transaction throughput.

Permissioned blockchains achieve higher transaction throughput than permissionless ones because the consensus algorithm of permissioned blockchains is generally deterministic. Some features, such as the block size, in a few permissioned blockchain frameworks can be customized. These frameworks may also follow modular designs. The performance of a blockchain framework may be also affected by the size of the block. For example, a large block may take longer time to be committed than a smaller one. Network delays may also undermine the efficiency of the consensus algorithm, particularly for consensus algorithms with built-in voting mechanisms because nodes broadcast their votes. Voting-based consensus mechanisms require a collection of votes from peers. A vote is a signature appended to a block.

F. Blockchain Frameworks

In this section, we review existing blockchain frameworks. Some are proposed for supply-chain management. We also add others that can be potentially adopted for the same goal. Table **??** presents a summary of existing blockchain frameworks.

1) Bitcoin

It is a permissionless blockchain framework that implements a decentralized digital currency system for the exchange of a cryptocurrency called bitcoin (BTC) [**?**]. Bitcoin has not been adopted by supply chain studies covered in this survey, but we introduce it here because it presents the concept of blockchain. Bitcoin uses the Nakamoto consensus algorithm (NCA) [**?**], which is essential to achieve decentralization and avoid double-spending in transactions. Double-spending occurs when a client transfers the ownership of an asset to two or more clients. NCA comprises a PoW algorithm for the proposal of new blocks, the longest chain policy as block finality mechanism, and the Gossip protocol for dissemination of blocks. PoW is a high-intensity computational algorithm where miners solve complex cryptographic puzzles until the required random number is found. PoW demands a high computational load from miners. From all miners solving the puzzle, the miner that solves it first is the only one rewarded. Therefore, miners with more computational power have higher opportunity to first solve the cryptographic puzzle, and to be rewarded. However, concentration of computational power is not desired as it undermines the decentralization principle of blockchain. Ownership transfer of a BTC is represented by a transaction with a set of inputs and outputs. If a client wants to transfer his/her BTCs to another participant, the client must define and sign a transaction that specifies as input the references of the transactions where the owned BTCs were obtained, and the identity of the new owner as the output. Thus, the global state of the distributed ledger in Bitcoin is simply an abstract representation of the sum of unspent transaction outputs (UTXOs) of every client. Another drawback of bitcoin, besides having to perform a computationally-demanding PoW, is that the size of blocks is hardcoded to 1 MB. In combination with the block generation time, this memory usage keeps the transaction throughput low. Moreover, the scripting capability of a transaction is limited to basic

TABLE II: Blockchain Frameworks.

Blockchain framework	**Type of blockchain**	**Consensus algorithm**	**Confidentiality**	**Type of Smart contract**	**Performance**	
					Throughput (tps)	**Block time (s)**
Bitcoin [?]	Permissionless	Nakamoto	None	Limited to P2SH and P2PKH	Less than ten	600
Zcash [?]	Permissionless	Nakamoto-based [?]	Shielded transactions with ZKPs	Limited to single and multisignature txts	Tens	150
Ethereum [?]	Permissionless	Nakamoto-based [?]	None	ETH smart contracts	Tens	10 to 20
HP3D [?], [?]	Hybrid	Nakamoto-based [?]	Partially via private ledgers	Not discussed	Not discussed	Not discussed
Gcoin [?]	Permissioned	Nakamoto-based [?]	Not discussed	Smart contracts and multisignature txts	Tens	15
TransICE [?], [?]	Permissioned	Nakamoto-based [?]	Encryption of sensitive data (ZKPs)	Hawk contracts	Not discussed	Not discussed
Multichain [?]	Permissioned	Nakamoto-based [?]	Stream-read restriction	Smart filters	Thousands	< 1
Hyperledger Sawtooth [?]	Permissioned or permissionless	PoET	Private UTXOs	ETH smart contracts via Seth	Thousands	< 1
Hyperledger fabric [?]	Permissioned	Various	Private transactions channels ZKPs	Chain-code in fabric	Thousands	< 1
Tendermint [?]	Permissioned or permissionless	Tendermint	Stream-read restriction	Via Tendermint ABCI	Thousands	< 1
Exonum [?]	Permissioned	Customized BFT	Not discussed	Services	Thousands	< 1
BigchainDB [?]	Permissioned	Tendermint	Not discussed	Not discussed	Thousands	< 1
Double chain [?]	Permissionless	PoS-based	Encryption of sensitive data	Intelligent contracts	Thousands	< 1
Carbon Footprint Chain [?]	Permissioned	RAFT like	Not discussed	Not discussed	Hundreds	< 1
Block-Supply Chain [?]	Permissioned	Tendermint-based	Not discussed	Not discussed	Thousands	< 1
QuarkChain [?]	Permissionless	Boson	Not discussed	ETH based Smart contracts	Thousands	Varies

operations like Pay-to-Pubkey-hash (P2PKH) and Pay-to-script-hash (P2SH).

2) Zcash

Zcash, while not reportedly adopted in the supply chain studies surveyed in this paper, it was the first open permissionless cryptocurrency that aims to fully protect the privacy of transactions. To achieve this goal, Zcash uses ZK-SNARKs as ZKPs for verification of ownership of tokens [?]. Zcash implements a consensus algorithm based on Bitcoin's NCA. However, Zcash uses a lighter version of PoW, which requires a large amount of memory for solving the cryptographic puzzle. The inter-block generation time of Zcash is 2.5 minutes and the block size is up to 2 MB. Zcash supports public and private transactions, where the latter hides critical data. The drawbacks of Zcash are poor scalability due to the significant usage of both memory and time by ZK-SNARKs.

3) Ethereum

Ethereum is a permissionless blockchain framework that implements a decentralized digital currency system for the exchange of the cryptocurrency known as Ether (ETH) [?]. Ethereum also adopts NCA and a light version of PoW. As a result, the inter-block (generation) time is reduced to about 15 seconds. Despite this shorter generation time, low transaction throughput remains in Ethereum.

Another modification to NCA in Ethereum is the integration of the Greediest Heaviest Observed Subtree (GHOST) protocol that operates in lieu of the longest chain rule as the block finality mechanism. The state of the distributed ledger is explicitly defined in Ethereum, as opposed to Bitcoin. Ethereum comprises many small objects called accounts, each of them holding a state, that interact with each other.

A major feature of Ethereum is the support of a complete scripting language that leverages the development of decentralized applications (DAPPs). Smart contracts are implemented through DAPPS. A smart contract runs on an Ethereum virtual machine (EVM) powered by a unit referred to as gas. This unit is the price charged for every step of execution in a contract. The EVM is a Quasi-Turing complete virtual machine intrinsically bounded by gas. The more code a transaction requires to run, the more gas it requires. The charging of gas helps to restrict the processing of malicious transactions which aim to run indefinitely [?].

4) HP3D

The hybrid peer-to-peer physical distribution (HP3D) blockchain framework is proposed for tracking shipments in a supply chain, and it covers the distribution of products from suppliers to customers [?], [?]. This framework comprises dynamic private ledgers for the recording of custody events that are visible to only the trading partners in a given shipment, and a public ledger.

HP3D records the activity of shipments using three types of events, namely *genesis*, *custody*, and *monitor*. A genesis event is the start of a shipment. This information is broadcast to a private ledger and a hash of it is broadcast to the public ledger. A custody event is the change of custody of a product (i.e., ownership). After a change of custody, the new custodian broadcasts the event to the private ledger and a hash of the event to the public ledger. In the private ledger, participants validate the signed custody events, which are subsequently recorded in the private ledger. External monitors generate monitor events and report them to the public ledger to keep track of the geolocation of trucks. Any participant in the public ledger can propose a block after solving a cryptographic puzzle, i.e., PoW. The proposed block is broadcast and validated against the participants' local databases.

5) Gcoin

Gcoin is a permisioned blockchain framework with an open government model, i.e., open data for transparency and accountability, that has been proposed for application in a drug supply chain [?]. Gcoin uses a double-spending prevention mechanism similar to that used in Bitcoin. This mechanism is aimed at countering the trading of counterfeit drugs. Gcoin records the entire history of a drug; from manufacture to sales. It combines the open government model and cooperation from decentralized autonomous organizations to foster greater transparency. In this framework, drug manufacturers mine new coins, large manufacturers, and government agencies validate the transactions. Also, third parties verify and hold the blockchain and pharmacies and consumers perform transactions to gain ownership of the coins, i.e., drugs. Gcoin also uses a multi-signature design, supports smarts contracts, and uses PoW with a block generation time of 15 seconds. This generation time leads to a transaction throughput that ranges between 17.5 and 26 transactions per second.

6) TransICE

TransICE is a permissioned blockchain framework for the logistics of integrated casinos and entertainment. TransICE is organized in three layers, the data or blockchain layer, the smart contract layer whose contracts are based on the Hawk model, and the interface layer for services and applications. The Hawk model is a decentralized smart-contract approach that provides transactional privacy guarantees using ZKPs [?]. A Hawk-based smart contract is split into private and public portions and both can be executed in Ethereum. Hawk's security guarantees include on-chain privacy and contractual security among users in the same contract. On-chain privacy is achieved because only encrypted data is sent to the blockchain while the required private computation is performed off-chain. The Hawk protocol is broken down into three essential stages: commit, compute, and finalize. First, users commit their data (offer) into the smart contract, then in the compute stage, the participants reveal their data to a trusted manager who collects all data and executes a private function in the smart contract. In the finalize stage, the result of a game is announced and the smart contract distributes the tokens to the winners who participated in the game as ruled by the smart contract.

7) Multichain

Multichain is a bitcoin-based permissioned blockchain framework that leverages data privacy and scalability by addressing computational-intensive mining, lack of privacy, and the open accessibility features of current public blockchain frameworks [?]. It integrates a transactional-based control mechanism for the management of users' privileges and permissions. This mechanism defines which activity is visible to each user, which transactions are considered valid, the block size, mining participation, mining rewards, and transaction fees. Similar to bitcoin, transactions in Multichain are input-output based but they differ in that they contain special metadata, such as communicating users' granted or revoked permissions.

Mining in Multichain avoids monopolization of the block proposing mechanism by a powerful single node through the use of a round-robin schedule where nodes take turns to propose a block. In its current version (2.0), Multichain provides smart filters, which are pieces of code embedded in the blockchain, containing rules to validate transactions and to restrict the data visibility for users according to their permissions. In Multichain, administrator nodes grant participants the right to participate in the consensus algorithm and to retrieve the contents of the distributed ledger. They restrict access to the distributed ledger, and that enhances data privacy and confidentiality. Multichain can also work as a compound blockchain node to communicate with other frameworks by simply setting the connection parameters in its configuration file.

8) Hyperledger Sawtooth

Hyperledger Sawtooth is a blockchain framework supported by Intel, which works as either a permissioned or a permissionless blockchain [**?**]. This framework implements ETH smart contracts via a tool called Seth and provides data privacy by means of private UTXOs. It uses Proof of Elapsed Time (PoET) as its consensus algorithm. PoET simulates the time used for PoW in a trusted execution environment (TEE) using software guard extensions (SGXs) enclaves [**?**]. A node with the shortest waiting time becomes the proposer.

9) Hyperledger Fabric

Hyperledger Fabric is a permissioned blockchain framework supported by IBM, which is primarily used for enterprise solutions [**?**]. Hyperledger Fabric follows a modular design that allows the integration of pluggable modules for its different infrastructure components (e.g., consensus algorithms). By default, it comes with built-in FTC algorithms namely, Kafka and Raft; and a centralized consensus algorithm namely Solo for development purposes. However, user-defined consensus algorithms can be plug-and-play when needed. Fabric supports chaincodes similar to ETH smart contracts.

A major difference between Hyperledger and other blockchains is that Hyperledger provides enhanced data privacy by incorporating private channels, ZKPs, and using endorsement policies. An endorsement policy defines the number of validators required to validate a transaction. An endorsement policy can be defined at the contract or at the data level. Hyperledger Fabric follows an Execute-Order-Commit model, in which transactions are initially executed on the set of validators defined in the endorsement policy. This approach improves scalability by reducing inter-block generation time, prevents non-determinism in contract code, and enables the private execution of transactions between a set of participants. Scalability of Hyperledger Fabric also depends on how fast the hardware of the involved peers executes the validation pipeline of transactions. Optimized transaction throughput from 3,000 to 20,000 tps has been reported [**?**].

10) Tendermint

Tendermint is a blockchain framework that runs the Tendermint consensus algorithm which is a BFT-based PoS consensus algorithm [**?**]. This algorithm works as a voting mechanism that runs in consensus cycles, each having multiple rounds. Every round consists of three steps, propose, prevote, and precommit. The function that selects a validator as the proposer of a new block is deterministic. A node is selected as a proposer with a weight proportional to the node's tokens; the higher the stake, the larger the probability that the validator is selected as the block proposer. A block is finalized and appended to the main chain after validators have received more than two thirds of the votes from the total set of validators. Tendermint is a flexible consensus algorithm that can be implemented in permissionless or permissioned blockchains. Tendermint can provide a high throughput because it has an unbounded block proposal time. However, the block proposal time depends on a node receiving the minimum number of votes to reach consensus. The number of participants, however, may affect the block proposal time.

11) Exonum

Exonum is a framework that provides the building blocks for the development of a permissioned blockchain [**?**]. Exonum uses a customized BFT consensus algorithm that is similar to Tendermint but it works in unbounded rounds, i.e., a round is the proposal of one block. Every round consists of three stages: propose, prevote, and precommit. In the propose stage, a selected leader proposes a list of transaction hashes and broadcasts it to the validators. Upon receiving the list, validators verify that the transactions in the list are consistent and broadcast a prevote for the received list. Then, validators collect two thirds of prevotes and process the transactions in the list. The validator that receives two thirds of the prevotes broadcasts the results to the other validators in a precommit message. If a validator receives two thirds of precommits, they commit the block to their local ledger. Exonum provides services, which are analogous to ETH smart contracts. It also has special features such as locks to keep the consensus algorithm off the influence of byzantine validators.

12) BigchainDB

BigchainDB is a permissioned blockchain framework that combines the decentralization, immutability, and owner-controlled assets properties of a blockchain with a high transaction throughput, low delay, and the indexing and query capabilities of a database. BigchainDB aims to resolve the single-point of failure scheme of master-replica database environments. Additionally, it uses Tendermint's consensus algorithm to synchronize the network peers, but it provides equal voting power to nodes. Therefore, BigchainDB inherits the low latency, fast finality, and BFT from Tendermint.

13) Double chain

Double chain is a permissionless blockchain framework designed for agricultural supply chains [**?**]. It aims to match and schedule decentralized agricultural commercial resources between suppliers and consumers using a transparent and credible management model. Participants in double chain are supply and demand nodes and they report their supply capacities and demands to a public centralized service platform that matches the participants. Double chain is based on two independent chains, the user information chain that records the hash of participants' public keys and the transaction chain that records the performed transactions between participants. The public service platform performs virtual integration of the reported decentralized agricultural resources. Intelligent contracts control the execution of a transaction and are generated after the public service platform implements an adaptive matching service to match the reported supplies and demands. To improve transaction throughput, Double chain uses a PoS-based consensus algorithm.

14) Carbon Footprint Chain

Carbon Footprint Chain (CFC) is a cluster-based blockchain framework for recording the carbon footprint generated by the transportation of products between the stages of a food supply chain. This blockchain framework has as many clusters as the number of stages of a supply chain, each representing a food life-cycle stage (farm, processing, manufacturing, etc.). A cluster is a group of full nodes, or participants, in a stage. IoT devices integrated into trucks collect the mileage, carbon footprint, product, and other information needed to associate the transportation with the generated amount of carbon. As a truck arrives at a new stage, the IoT device publishes information to the closest node in that stage. The leader node of the cluster validates the block and broadcasts the block to every node. Each node then writes the block onto its local ledger. CFC implements a Raft-like consensus algorithm in each cluster, where a leader node in the cluster communicates with a random node of a previous cluster to validate the block. This process ensures that trucks in the supply chain record accurate generated carbon for each trip.

15) Block-Supply Chain

Block-supply chain is a blockchain framework designed to detect counterfeits throughout the product life cycle of a supply chain [?]. It integrates RFID and near field communication (NFC) technologies to detect modification, cloning and tag reapplication of products at different stages along the supply chain. Block-supply chain aims to address a centralized anti-counterfeit problem where a trusted server is responsible for the management and coordination of product authentication. Block-supply chain implements a Tendermint-based consensus algorithm but it customizes it to improve its performance at the cost of security. Block-supply chain's consensus algorithm reduces the number of required validators from $n-1$ to $log(n-1)$ and implements an equal-selection random algorithm to select validators every time a new block is proposed. It comprises two phases: Initialization and verification. In the initialization phase, the product manufacturer records the detailed information of a product on the product's NFC tag, generates an authenticated event, and broadcasts it as a genesis block. In the verification phase, the supply chain nodes execute a local and a global authentication algorithm to verify the authenticity of the product's information in the block and reach consensus.

16) QuarkChain

QuarkChain is a blockchain framework that aims to address the limited transaction throughput of permissionless blockchains [?]. QuarkChain is based on the concept of horizontal scalability or sharding, in which the global state of the blockchain is partitioned into multiple sub-states (i.e., sharded blockchains). Every shard runs in parallel and is independently processed; by increasing the number of shards, the transaction throughput is linearly increased. In QuarkChain, there are two types of transactions: balance transfer transactions that can be either in-shard or cross-shard and smart contract transactions, which are valid only if they are issued from within the same shards. QuarkChain runs two hierarchical layers namely the sharding blockchain layer, which consists of a list of sharded blockchains, each having their consensus and sharded-parameters, and the root chain layer. The latter layer is in charge to confirm the blocks in the sharded blockchains. A block in the root chain layer includes the block headers of the sharded-blockchain blocks. QuarkChain implements a two-layer sharding consensus algorithm, called Boson. An example is a collaborative mining/minting consensus algorithm, where the root chain layer runs PoW while the sharding blockchain layer runs PoS. It has been reported that QuarkChain can reach more than 55,000 transactions per seconds with 1,024 shards [?].

IV. Blockchain and Supply Chain Management

Supply chain management covers multiple stages of a product life cycle and often involves the participation of various stakeholders. The multiple stages and the variety of participants in the supply chain make it a highly interconnected network that is difficult to manage. Furthermore, supply chain management is challenged not only by the requirements on record-keeping but also by the requirements associated with a particular industry. In response, different blockchain frameworks and consensus algorithms have been proposed to address concerns in specific industries and products. Table **??** summarizes the blockchain frameworks for supply chain covered in this survey, categorized by industry, and outlines the objectives that motivated the adoption of blockchain.

A. Industries/Products

Because food supply chains are essential for society, they have attracted more interest in applying blockchain technology in this industry than any other ones. Some of the addressed challenges are transparency, provenance, performance improvement, quality assurance and control, and achieving sustainability [?], [?]. Food supply chains comprise many stages and they may not be finely monitored and tracked. As a result, end consumers are usually unable to trace their food products' origins.

Counterfeit drugs are a common challenge for the pharmaceutical industry. Recent studies in this industry show the effectiveness of blockchain in tracking and authenticating drugs [?], [?], [?], [?], [?]. The health industry has also explored the use of blockchain to secure digital records [?]. Some other challenges explored in the pharmaceutical industry include quality assurance and quality control [?], and performance improvement [?].

The entertainment and media industry faces transparency challenges in its supply chain because stakeholders need to be assured of the quality of service and compliance of regulations. The complexity of this industry is due to not only the size of operations but also to the vast number of regulations. The integrated casinos and entertainment (ICE) logistics involve management of other industries such as tourism, hotel, retail, etc. It is important for ICE logistics to ensure that each participant of the supply chain provides goods and services meeting the quality standards set by the industry or the customers' demand. Blockchain is a fit candidate to resolve this challenge because it ensures that all transactions within the network are transparent and easy to identify, track, and manage [?].

Automotive, wine, and wood products share the challenge on provenance. In these industries, provenance and originality are the main motivation of using a distributed ledger [?], [?], [?]. They are mostly interested in permissioned blockchain frameworks to keep the companies' proprietary information confidential.

Blockchain is also a very suitable solution to track ownership of digital assets, such as 3D models [?]. Intellectual property of digital assets is very challenging to track because these products are highly replicable. Association of these assets with blockchain needs further research.

Postage is an industry that considers blockchain for its supply chain to detect counterfeit stamps as the number of fraud cases continues to increase [?]. Adversaries may take advantage of the variation of currency and counterfeit old stamps. This work mentioned that the lack of expiration date of stamps increases the complexity of the challenge. The low-cost of stamps and their large numbers make stamp verification hardly cost effective and scalable.

Some studies provide blockchain solutions to address transparency, provenance, quality assurance and control, data privacy, confidentiality and sustainability in general supply chain without specifying the industry [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?]. These works aim to provide a general solution to all supply chains by leveraging the features of blockchain. However, other works focus on a specific industry and also on particular challenges.

B. Proposed Solutions to the Supply Chain Challenges

The following blockchain frameworks are the reported solutions to the supply chain challenges in the literature. They are categorized based on the specific supply chain challenge they address.

1) Provenance

This is one of the main sought features in the reported studies. Provenance has shown to mainly resolve three challenges: tracing the origins of a product, tracking a product, and identifying counterfeit products.

a) Tracing the origin of products: Knowing the provenance of a product may be crucial for quickly recalling defective or unsafe products. As an example of such a need, in 2015 the suppliers of restaurant chain Chipotle had spread of E. Coli and salmonella in their products that triggered a recall [?]. Accurate provenance information may have helped to have a more efficient response. Blockchain can assist companies to timely identify the lot and supplier from which the contaminated ingredient comes, speedup recalls, and mitigate risks for consumers. Blockchain is a suitable technology to keep track of provenance at different stages of a supply chain, as the product or material ownership changes are reflected in the distributed ledger.

Multiple studies in the food industry have proposed blockchain adoptions based on Inter-Planetary File System (IPFS) and Ethereum. IPFS is a distributed file sharing system [?] with fast data retrieval speeds, hence ensuring easy and fast accessibility to data for numerous stakeholders of the supply chain. Often in the adopted studies, the first block is created by farmers that collect the crops and transfer them to processors. A blockchain records a transaction each time the product moves through the stages of the supply chain. Transactions are executed through smart contracts that identify and validate them. The studies have also suggested utilizing IPFS for storing some of the information, like photos of crops. Having recorded the transactions of a product helps in identifying its origins because they indicate the ownership of the product at every stage [?], [?], [?], [?].

Standalone IoT devices and RFID tags have been vastly adopted to input data to the blockchain. In reported studies on food and wood industries, participants on every stage of the supply chain use RFID tags to label the products and store the corresponding information in blockchain [?], [?], [?], [?], [?], [?]. In the case of the wood industry, Figorilli et al. [?] suggest using RFID tags until the wood reaches the processing stage, where they are replaced by QR and barcodes. This approach reduces the high cost of RFID tags as they are used in logs (batches) and not on individual products.

Some studies have also introduced quality-control protocols in blockchain specific to supply chain [?], [?]. One of such studies proposed utilizing RFID tags and Hazard Analysis and Critical Control Points (HACCP) [?]. This study bases its adoption on BigchainDB. In this application, farmers label the collected crops with RFID tags that store descriptive information about the crop. The transfer of crops from farms to processing plants is recorded as a digital contract that is stored in the distributed ledger. Tien et al. employed IoT devices to maintain the correct storage temperature during the distribution stage. Rahmadika et al. [?] also used HACCP in their adoption of Ethereum. Other studies have used protocols like Electronic Product Code Information Services (EPCIS) or GS1 Standard as standards for storing provenance related information. These studies also utilize RFID tags to store information and smart contracts to validate the new blocks [?].

Besides following the product life-cycle model, some studies focus on the components or ingredients of a product. Westerkamp et al. [?] represented physical goods in the form of cryptographic tokens and the final products as a combination of tokens. Recipes are used to produce the final product. During the processing stages, the tokens are combined together in the same ratio as the ingredients in the recipes that are combined to make the product. The idea of such an implementation is to create an accurate digital representation of the end product. Smart contracts

TABLE III: Blockchain Frameworks and Supply Chain by Industry and Challenges.

Products	**Challenges**	**Framework**
Automotive	Provenance [?]	Ethereum
Digital Products	Provenance [?]	Ethereum
Entertainment & Media	Transparency [?]	TransICE
Food	Provenance [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], Performance Improvement [?], Quality Assurance and Quality Control [?], [?], Sustainability [?], Transparency [?]	Ethereum [?], [?], [?], [?], [?], [?], [?], [?], [?], Hyperledger [?], [?], [?], [?], [?], Double Chain [?], BigchainDB [?], Carbon Footprint Chain [?]
Pharmaceutical	Data Privacy and Confidentiality [?], Quality Assurance and Quality Control [?], Performance Improvement [?], Provenance [?], [?], [?], [?], [?]	Hyperledger [?], [?], Gcoin [?], QuarkChain [?]
Postage	Provenance [?]	Exonum
Wine	Provenance [?]	MultiChain
Wood	Provenance [?]	Ethereum
Other	Transparency [?], [?], [?], Provenance [?], [?], [?], [?], [?], [?], [?], Quality Assurance and Quality Control [?], Data Privacy, and Confidentiality [?], [?], [?], Sustainability [?]	Ethereum [?], [?], [?], Hyperledger [?], [?], HP3D [?], Block-Supply Chain [?]

may ensure that the correct amount of material is used for each ingredient. This study adopts Ethereum to implement the proposed blockchain framework.

b) Counterfeit Detection: Product ownership and counterfeit detection is a frequent application of provenance. According to a recent report by the Organisation for Economic Co-operation and Development, trading of counterfeit products makes up 3.3% of all global trade [?]. Because provenance is the history of the ownership of goods, the originality of a product and its ownership can be easily verified.

A study on the wine industry uses a blockchain framework based on the stages of the supply chain [?]. This approach is a common practice of provenance-based studies covered in this survey. Each stage of the supply chain is represented by grape growers, wine producers, and retailers. The authors propose using barcodes and RFID tags to collect information and MultiChain to record the information [?]. In this way, the authenticity of wine can be assured because blockchain can indicate the farms where the grapes were grown.

Counterfeits of digital products are more difficult to identify because they have no physical presence. Holland et al. [?] proposed an Ethereum-based network that works as a digital certificate of authenticity for 3D design intellectual property assets. They have integrated blockchain into OpenDXM GlobalX software [?], which is used by manufacturers for sharing data with maximum intellectual property protection. Each licensor and licensee has his/her own private keys. These keys are used for creating a digital certificate of authenticity when a licensor provides its digital assets to a licensee. This type of implementation decreases the risks of counterfeits because every purchase of the digital asset must be recorded in the blockchain and it becomes immutable.

The risk of counterfeit drugs has been increasing in the pharmaceutical industry. Researchers and pharmaceutical companies are interested in overcoming this challenge [?]. The drug supply chain is organized into four levels: suppliers, manufacturers, distributors, and pharmacies. Studies in pharmaceutical blockchain estimate that the risks of counterfeit drugs can occur on all of the listed stages [?].

Tseng et al. [?] proposed Gcoin to record transactions between pharmacies and consumers. The distributed ledger contains transactions with the relevant information on the drug, and the identities of seller and buyer. Only authorized personnel can perform transactions through smart contracts, thus minimizing the risk of acquiring counterfeit drugs by a customer.

Jamil et al. [?] proposed the adoption of a blockchain to facilitate sharing of medical records of patients among different departments of a hospital. Here, each department in a hospital is represented as a sub-network. In this way, the confidential information can be shared among specific departments directly without exposing it to the rest of the network.

Postage is another industry that has adopted blockchain to detect counterfeits. The adoption of blockchain here is motivated by a large number of victims of stamp fraud in Russia. Yanovich et al. [?] proposed a solution to prevent the usage of invalid stamps using Exonum. The architecture of the blockchain comprises transaction validators, token issuers, postal acceptance inspectors, clients, and auditors. The postal service of Russia is the transaction validator. They check compliance of transactions. Token issuers are companies authorized by the postal service to sell post stamps. Acceptance inspectors are company employees who are responsible for accepting mail. Clients are other entities participating in the postal stamps market. Auditors are parties assigned by a company to guarantee the correctness of the records. This approach ensures a transparent and trustworthy environment by removing a central authority and failure.

Peltoniemi et al. proposed a permissioned blockchain that can issue digital tokens to donors of blood to track plasma [?]. Each blood donation is recorded in the blockchain. To transform it into plasma, blood must go through many rounds of medical testing. This approach allows doctors to identify the origin of the plasma and minimize risks of using tainted plasma.

c) Tracking: Introducing real-time tracking can help a supply chain mitigate the inventory variations generated by an inefficient demand forecast. This feature can enable management to make agile business decisions for product development and inventory control under rapidly changing demands. Many blockchain adoptions employ IoT devices for real-time product tracking as it moves through different supply-chain stages.

The distribution stage of supply chains has been identified as one that can benefit from blockchain for recording events [?]. HP3D has been proposed to address this need. This solution leverages the central public ledger and multiple private sub-ledgers of HP3D.

2) Performance Improvement

One of the performance metrics of the supply chain is transaction throughput. Transaction information in a blockchain is sought by supply chain stakeholders as well as regulatory bodies. For example, Double chain is a proposed solution for creating a modular and scalable system [?]. The implementation separates entities into supply nodes and demand nodes. Each resource supply node looks up the appropriate demand node according to the latest information in the block.

Xie et al. [?] discussed the performance and scalability limitations of blockchains in pharmaceutical industry. They proposed sharding the blockchain into clusters to increase transaction throughput. This approach is implemented by a QuarkChain framework.

3) Quality Assurance and Quality Control

Chandra et al. [?] focused on having a system that verifies that food remains Halal after passing through each processing stage. Due to a large number of rules that define a product as Halal, ensuring that the product is properly processed is difficult. The authors proposed the use of IoT devices, QR codes, and RFID tags to collect product information at each processing stage and record this information into the distributed ledger for verification.

The vast number of health concerns on food processing motivates the adoption of blockchain to record the processing quality and thus the quality of the food products. Tse et al. [?] proposed a blockchain for governments and regulatory bodies to exercise quality control. The authors divide the supply chain into suppliers, manufacturers, sellers, customers, and regulators. Before it moves to the next stage, a product is authenticated by the regulatory body. This authentication process eliminates the possibility of unidentifiable materials entering the production.

Quality assurance is crucial in the pharmaceutical industry. Hulea et al. [?] explored the use of Hyperledger Sawtooth to ensure that cold storage standards for drug storage are met during the distribution of drugs. The authors proposed using IoT devices with temperature sensors to track the temperature of the cold storage during transportation and record it in the distributed ledger.

4) Sustainability

Provenance also plays a major role in analyzing the sustainability of a supply chain. Denisolt et al. [?] proposed CFC to record the carbon footprint of stages of a product supply chain with an emphasis on transportation. There is an increasing demand for such information by regulatory bodies to evaluate supply chain sustainability. However, there is also a need for associating the amount of carbon a supply chain can generate such that the manufacture of a product or service is sustainable. Regulatory bodies can use this approach to ensure carbon footprint compliance. CFC enables an accurate accounting of carbon footprint release.

5) Transparency

Liao et al. [?] aimed at providing transparency in the entertainment industry by using TransICE. This blockchain framework allows for a transparent record keeping of all transactions occurring in the logistics of this supply chain. TransICE is an application that runs on Ethereum with smart contracts for the management of ICE to validate the adherence to the set policies.

The challenge of transparency is also found in the food industry [?]. The concern for transparency comes from customers bidding on food products. Blockchain can ensure fair bidding in the supply chain. Koirala et al. [?] proposed a Reverse Auction Bidding (RAB) network, where a customer solicits bids from a producer until the customer is satisfied. This work uses smart contracts that maintain the transparency of transactions and automate the application in Ethereum.

6) Data Privacy and Confidentiality

Data privacy and confidentiality are concerns raised in many studies of supply chain, but most of the proposed works do not address them. Some studies address concerns on attacks on data privacy and how to use blockchain to solve that problem [?], [?].

Xu et al. [?] propose a hybrid blockchain model and a two-step block construction method to protect data privacy in a public ledger. This work addresses the concerns on security by encrypting the records that are stored in the distributed ledger with the public keys of the participants who are authorized to access the record.

V. Discussion

In this section, we discuss opportunities and challenges in adopting a blockchain framework for supply chain management and outline the features of the blockchain framework that address some of the supply chain challenges. We also discuss topics for future research.

A. Opportunities and Challenges of Blockchain in Supply Chain Management

1) Immutability

Immutability supports transparency, traceability, inventory verification and originality which motivate blockchain adoption in supply chain. For example, immutability can help preserve the records for inventory verification, traceability, and provenance. However, immutability may be achieved at the cost of transaction throughput. Methods that support immutability without affecting transaction throughput need to be developed.

2) Tracking Accuracy

To achieve high tracking accuracy, a blockchain needs to record a large number of transactions. The challenge lies in the amount of storage required to host the distributed ledger. As the number of transactions increases, the size of the distributed ledger also increases. Taking into account that many of the blockchain adoptions employ IoT devices for publishing tracking data, a blockchain is required to process a large number of transactions and a consensus algorithm to keep up with the demand.

3) Provenance

Provenance requires recording of the ownership of a product through the supply chain. The blockchain must allow retrieving chronological records of a product from its origin to the final stage. A secondary data structure, such as a hash map table, may be needed to operate with the blockchain data.

4) New Supply Chain Management Models

Supply chain reliability is an important issue under a catastrophic/disastrous event that can disrupt one or more stages of the supply chain. Novel blockchain and supply chain models need to be developed to address this issue. The immutability property of a blockchain allows the use of reliable data from supply chain. Such data can be used for developing new models for supply chain management. Recently, works that use artificial intelligence to analyze data from blockchain to improve the supply chain efficiency have been proposed [?].

5) Throughput

Supply chains may need to report a large number of transactions. The number of transactions may be massive for some products. In fact, McKinsey reported: “In a 90-day period, a single auto manufacturer would typically issue approximately 10 billion call-offs just to its tier-one suppliers" [?]. The trade-off between security and performance has to be balanced in a blockchain.

Another challenge is the incorporation of IoT devices into supply chain as they may increase the amount of data generated, and that requires a commensurate transaction throughput. Existing blockchains can support a limited number of transactions, which may raise potential concerns for scalability.

6) Cost and Complexity

With the integration of big data, blockchains may collect vast data about the supply chain and the customers [?]. Although blockchain supports supply chain management by resolving some of the existing concerns, like provenance and quality assurance, it also introduces additional costs for implementation and maintenance. Blockchain requires infrastructure for computing, communications, data collection, and integration into the existing supply-chain management. The characteristics of the adopted blockchain and the requirements of the supply chain dictate the amount of infrastructure needed.

As an example, RFID tags that track products can be expensive to implement. Therefore, cost and risk analysis must be considered for a sustainable implementation. This challenge opens opportunities in cost optimization. Also in an implementation that requires automated quality assurance and quality control, the sensors collecting relevant information must be placed at every stage. Therefore, the number of needed sensors may be large. This challenge opens opportunities for the integration of data collected by multiple IoT devices.

7) Security

Although blockchain can resolve many challenges of a supply chain, it may also introduce some security concerns. The success of a blockchain lies on decentralization. However, a high concentration of computational, staking and voting power on a few nodes may threaten decentralization. Mining and validation diversity is essential to retain such a feature.

The immutability feature of a blockchain distributed ledger relies on the security of its consensus algorithms. Consensus algorithms are considered secure when the majority of miners and validators are honest. However, consensus algorithms based on PoW and PoS are compromised when adversaries take over more than 50% of the computation and staking power. Adversaries with such power capabilities could propose malicious blocks to fork and invalidate the main blockchain ledger. Additionally, blockchain BFT consensus algorithms are exposed to similar security threats when adversaries compromise the majority of voting power, which is required to elect the block proposer in every round [?]. Moreover, CFT algorithms, such as RAFT, are prone to security attacks because validators neglect security checks on block proposals. The leader can write an arbitrary block to the blockchain.

Users use a public and private key pair to access blockchain. The public key serves as a digital identity while the private key is used to prove ownership of digital assets. The private key must be stored in a secure location at the user's computing system. However, there are no mechanisms that allow users to either retrieve or change their keys. Thus, an adversary may compromise users' information stored in the ledger with a stolen key [**?**].

IoT devices are becoming widely adopted to acquire data of supply-chain processes. However, their limited computing and storage capacity make them vulnerable to security attacks [**?**]. The network connectivity of IoT devices also exposes them to attacks that aim to control the information they broadcast and, in turn, that corrupts the blockchain. Those resource limitations also make them easy targets of Denial-of-Service (DoS) attacks, which may entirely disable the devices. While research on protecting IoT devices from DoS attacks has recently attracted interest [**?**], protection schemes on how to protect the information these devices input to a blockchain need to be considered in the near future.

B. Features of a Blockchain Framework for Supply Chain Management

Blockchain provides a suitable communication platform with built-in security guarantees for the implementation of robust and cost-effective decentralized supply chain management applications. Here, we discuss the key features of a blockchain framework for its application on supply chain management.

1) Confidentiality and data privacy guarantees

Some Blockchain frameworks allow the encryption of sensitive data in transactions before it is appended to the blockchain ledger, using cryptographic functions like hashing, encryption, and methods like ZKP. A blockchain framework may also restrict the access and visibility of the contents of the blockchain to only authorized users. Moreover, to provide selective data visibility, a blockchain must enable some authorized participants to access private data and all participants to access public data.

2) Light-weight consensus algorithms

Blockchain frameworks must support light-weight consensus algorithms to achieve high transaction throughput. Supply chains may need to support a large volume of transactions that are input by heterogeneous IoT devices [**?**]. To cope with large amounts of input data from the IoT devices, new light-weight consensus algorithms are needed. Additionally, a blockchain framework must provide services to enable the enrollment and authentication of IoT devices prior to their reporting of any transaction data.

3) Deterministic smart contracts

Deterministic smart contracts need to be developed to maintain a single common ledger state. Smart contracts implement a set of functions that define the business logic of the supply-chain management application. However, the use of non-deterministic functions in smart contracts can create inconsistent ledger states that may cause an entire application to halt.

4) Fast information retrieval

Tracking the development of a product as it passes across the different stages of its supply chain requires support for the retrieval of data from the blockchain adopted by the supply chain. Such data is used in logistic decisions or product monitoring [**?**]. Although it is a secure and immutable data structure for record-keeping, a blockchain is inefficient in query processing because of the absence of indexing in its data structure. Current blockchain frameworks overcome this challenge by combining database features to handle large volumes of data and enable faster data retrieval. In those blockchain frameworks, every peer has a database that hosts the complete historical records. The databases are synchronized broadcasting blockchain data.

5) Flexible verification algorithms

Blockchain frameworks must be flexible to allow the definition of verification algorithms to integrate different supply-chain applications. Peers use verification algorithms to accept or reject received blocks and transactions to update the blockchain ledger.

A supply chain application may require the verification of transactions using product-specific features and a flexible-verification algorithm. Therefore, the life cycle of transactions for different products with its verification algorithm must be clearly defined, before validators append a valid record into the blockchain ledger.

C. Literature on Blockchain Applications to Supply Chain

Throughout the set of surveyed literature, we identified a large number of works, where some are exploratory and others leave the blockchain implementation out of scope. Therefore, we organized these works into three categories: a) Application; which propose a blockchain implementation, b) Theory; which is mostly an exploratory work, and c) Case study or literature review. Table **??** shows the organization of the literature according to supply chain industry, challenges, and blockchain framework. The challenges of each work are split into specific and general challenges. Specific challenges are those that the paper addresses in particular, and general challenges are the ones outlined in Section **??**. As the table shows, there is an increasing interest in solving many of the supply-chain challenges by adopting blockchain technology. Real-life applications of blockchain on supply chain remain to be reported because they may allow us to identify the actual potential this technology has to offer and to resolve actual supply-chain challenges. Many of these works listed in this table have been described in this survey.

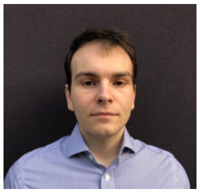
VI. Conclusions

In this survey, we introduced supply chain and described its operation, features, and existing challenges to make it more effective and efficient. We also introduced blockchain, which is a technology that can improve the management of

TABLE IV: Studies of Blockchain and Supply Chain by Industry and Challenges.

Type	Industry	Specific Objective	Challenge	Framework
Application	Automotive	Provenance	Provenance	Ethereum [?]
	Digital Goods	Ensure ownership of 3D assets		Ethereum [?]
	Food	Provenance		Ethereum [?]
				Ethereum [?]
		Transparency	Transparency	Ethereum [?]
		Ensure food products are Halal	Quality Assurance and Quality Control	Hyperledger Fabric [?]
		Food Provenance	Provenance	BigchainDB [?]
				Ethereum & Hyperledger [?]
				HyperLedger Fabric [?]
				Ethereum [?]
				Ethereum [?]
				Hyperledger [?]
				Ethereum [?]
				Hyperledger Fabric [?]
				Ethereum [?]
		Improve supply chain reliability		Ethereum [?]
		Counterfeit and use of excessive preservatives in wine		MultiChain [?]
		Provenance of soy bean products		Ethereum [?]
	General	Storing carbon footprint of the Supply Chain	Sustainability	CFC [?]
		Low performance of single chain structure	Performance Improvement	Double chain [?]
		Lack of trust in Enterprise Resource Planning systems	Transparency	Hyperledger Fabric [?]
		Counterfeit products	Provenance	Block-Supply Chain [?]
		Collaboration among multiple supply chain systems		Hyperledger [?]
		Detection of forgeries		Ethereum [?]
		Ensure product ownership post supply chain		Ethereum [?]
		Exploring potential use cases	Immutability	Ethereum [?]
		Absence of real-time tracking of goods	Provenance	HP3D [?]
		Exploring privacy concerns in sharing data	Privacy	Custom [?]
		Lack of trust and transparency	Transparency	Ethereum [?]
	Healthcare	Reducing the risk of drug counterfeit	Provenance	Hyperledger Fabric [?]
		Ensuring quality of drugs		Hyperledger Sawtooth [?]
	Entertainment & Media	Issues in lack of transparency	Transparency	TransICE [?]
	Pharmaceutical	Performance Improvement	Performance Improvement	QuarkChain [?]
		Reducing the risk of counterfeit drugs	Provenance	Gcoin [?]
	Postage	Reducing the risk of counterfeit postage stamps		Exonus [?]
	Wood	Wood Provenance		Ethereum [?]
Theory	Automotive	Exploring potential use cases	Immutability	[?]
	Digital goods	Survey of Blockchain and IoT implementations		[?]
		Investigation of requirements for integration of blockchain in Supply Chain		[?]
	Food	Food safety	Provenance	[?]
				[?]
		Exploring future challenges on use of Blockchain for Provenance		[?]
		Exploring potential use cases	Immutability	[?]
		Exploring requirements for adoption of Blockchain		[?]
	General	Exploring potential use cases		[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
				[?]
		Assuring Quality of goods	Quality Assurance and Quality Control	[?]
		Enhancing resilience of Supply Chain	Security	[?]
		Security concerns of blockchain implementation in Supply Chain		[?]
		Exploring potential use cases in Supply Chain sustainability	Sustainability	[?]
		Systematic tracking of goods	Provenance	[?]
		Analysis of blockchain innovation in logistics	Immutability	[?]
		Reducing the risk of counterfeit goods	Provenance	[?]
		Trust issues in Supply Chain	Transparency	[?]
	Healthcare	Security of digital records	Immutability	[?]
		Exploring potential use cases		[?]
			Provenance	[?]
	Manufacturing		Immutability	[?]
				[?]
	Pharmaceutical			[?]
		Tracking the origin of plasma	Provenance	[?]
		Identifying and tracking counterfeit drugs		[?]
		Encreasing the efficiency of order processing	Transparency	[?]
	Sustainability	Exploring potential use cases	Immutability	[?]
Case Study / Literature Review	Digital goods	Review of frameworks for digital Supply Chain	Literature review	[?]
		Exploring potential use cases		[?]
	Food	Literature review of blockchain adaptations		[?]
		Exploring potential use cases	Case Study	[?]
	General	Analysis of effectiveness of blockchain		[?]
		Analysis of the state of the art blockchain in Supply Chain	Literature review	[?]
				[?]
		Review of blockchain adoptions for ensuring transparency		[?]
		Analysis of effectiveness of blockchain		[?]
				[?]
		Exploring potential use cases		[?]
		Literature review of blockchain adaptations		[?]
				[?]
		Traceabilty of IKEA Supply Chain	Case Study	[?]
	Sustainability	Study of blockchain applications to reduce waste		[?]

supply chains. We surveyed existing blockchain frameworks that have been proposed to address the supply chain challenges. We identified different industries for which blockchain has been proposed and highlighted the addressed challenges. We also compared the existing solutions and listed the remaining challenges of supply chains where blockchain may still find their use. We presented a snapshot of the current state of blockchain in supply chains in the literature. We finalize our discussion with directions for future research.



Denisolt Shakhbulatov received his B.S. in Computer Science with a concentration in Big Data Management & Analytics from New York Institute of Technology (New York Tech) in May 2019. He currently works as a machine learning engineer. His research interests are blockchain, data mining, natural language processing, and machine learning. He received awards for multiple blockchain competitions hosted by NEO & Microsoft and City of Zion.

Jorge Medina received the B.Sc. in electrical industrial engineering from La Universidad Nacional Autonóma de Honduras, and his M.Sc. degree in telecommunication systems from The Blekinge Institute of Technology, Karlskrona, Sweden. He is currently pursuing the Ph.D. degree with the Networking Research Laboratory, Helen and John C. Hartmann Department of Electrical and Computer Engineering from the New Jersey Institute of Technology (NJIT), Newark, NJ, USA. His research interests are computer networking, computer optimization, blockchain and machine learning.

Ziqian (Cecilia) Dong received her B.S. degree in Electrical Engineering from Beijing University of Aeronautics and Astronautics, Beijing, China, M.S. in Electrical Engineering and Ph.D. in Electrical Engineering from New Jersey Institute of Technology (NJIT), Newark, NJ. She is an Associate Professor in the Department of Electrical and Computer Engineering at New York Institute of Technology (New York Tech). She was awarded the Hashimoto Prize for the best Ph.D. dissertation in Electrical Engineering, NJIT. Her research interests include architecture design and analysis of practical buffered crossbar packet switches, network security and forensics, wireless sensor networks, assistive medical devices, and data analytics and innovative sensing technology to improve sustainability and resilience of both natural and built environment. She is a senior member of IEEE. She served as the general co-chair of the Food, Energy, and Water Nexus Conference 2019, the Networking Networking N2Women Workshop 2019, and the 37th IEEE Sarnoff Symposium 2016. She has served in technical program committee of IEEE HPSR, IEEE Sarnoff, IEEE ICC, GlobeCom, GreenCom and ChinaCom, and as a reviewer for IEEE journals, conferences and NSF panels. She is the recipient of 2006 and 2007 Hashimoto Fellowship for outstanding scholarship and the New Jersey Inventors Hall of Fame Graduate Student Award. She received the New York Institute of Technology Presidential Award in Student Engagement in Research and Scholarship in 2015, Innovate Long Island's Fifth Annual Innovator of the Year Award in 2020, and the American Society of Engineering Education (ASEE) Engineering Research Council 2020 Curtis W. McGraw Research Award.

Roberto Rojas-Cessa (S’97–M’01–SM’11) received the B.S. degree from Universidad Veracruzana, Mexico, a M.S. degree from Research and Advanced Studies Center, Mexico, and M.S. and Ph.D. degrees in computer and electrical engineering, respectively from Polytechnic University (currently, the New York University Tandon School of Engineering, Polytechnic Institute), Brooklyn, NY, USA. He is currently a Professor with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology (NJIT). He has authored the books “Advanced Internet Protocols, Services, and Applications,” (Wiley, 2012) and “Interconnections for Computer Communications and Packet Networks” (CRC Press, 2017). His research interest includes the wide area of networking, cyber-physical systems, energy, intelligent systems and learning, and emergency communications and systems. He serves in different capacities for IEEE conferences and specialized journals as reviewer and editor, and as a Panelist for U.S. National Science Foundation and U.S. Department of Energy. He was the General Chair of IEEE Sarnoff Symposium 2011 and IEEE International Conference on High Performance Switching and Routing 2020. In addition, he has been a Technical Program Committee Chair of the two flagship conferences of the Communications Society: International Conference on Communications (ICC) and Global Communications (Globecom). He is a recipient of the Excellence in Teaching Award from the Newark College of Engineering at NJIT and the New Jersey Inventors Hall of Fame—Innovators Award in 2013. He was an Invited Fellow of the Japanese Society for the Advancement of Science in 2009. He was the recipient of the Excellence Progress in Research by the Dept. of Electrical and Computer Engineering (2005).