Improving the Modern Food Supply Chain with Blockchain

Jessica Zastoupil
12/13/2021

Abstract

The modern foods supply chain is full of problems ranging from lack of transparency and trust, issues with food safety and delayed payments. In this paper, we will look at some of the problems within today's modern food supply chain. We will then look at how blockchain, coupled with smart contracts and other technology, can solve many of the modern food supply chain's most common problems. We will also discuss how the supply chain can ensure confidentiality of proprietary information by using zero-knowledge proofs.

1. Introduction

A supply chain is a system in which a raw product moves from source to destination, including any transformations it may make along the way. In a food supply chain, this could include farmers, producers, warehouses, factories, shipping agencies, retailers and any paperwork and logistics having to do with distributing the goods to the consumer [1].

Challenges that can happen at any stage of a food supply chain include lack of transparency, lost and destroyed goods, counterfeit goods, food contamination and adulteration, consumer trust and delays in payments. Blockchain can help solve many of these problems [1] [2].

Blockchain is a transparent, trusted system where anyone at any point in the supply chain can view what is happening and where. Blockchain's inherent qualities of traceability and transparency give consumers an open view to where their products came from, facilitating trust. This also allows ease of tracking by other members of the supply chain and regulatory agencies. In addition, smart contracts can be used on the blockchain to ensure timely payments at each step of the supply chain [2].

2.Value Proposition

Blockchain transparency and traceability gives users a clear insight into the full supply chain, allowing for easier tracking of goods along the chain. It allows consumers to do their own due diligence on a product to ensure that it meets their standards (organic, fair trade, etc). It also gives authorities the ability to quickly determine where a contaminated food came from or ended up. It can help determine at what point in the supply chain raw materials were lost or damaged by comparing weights at each phase. Lastly, smart contracts can be used on the blockchain to ensure timely payments in each step of the supply chain since they self-execute as soon as all conditions are met.

3. Blockchain

A blockchain is a decentralized, distributed ledger. Blockchains were developed to be fully transparent, where anyone can see anything and everything related to the transactions within the blocks. However, within a supply chain, companies may have proprietary information in transactions (such as prices, margins, capacity, and demand) that they do not want to share with the world at large. Luckily, we can still use a public blockchain for decentralization and transparency but help keep specifics private by using a transaction validation method such as zero-knowledge proof [3].

Anyone along the supply chain would be able to add data to the blockchain, ideally by use of technology such as scanners, QR codes, RFID tags, IoT, tamper proof seals with NFC technology, and even GPS [8]. This will help ensure that the supply chain is being tracked on the blockchain at every step and to minimize the possibility of bad actors interfering with the process by trying to manually enter incorrect information. An app would be built to give consumers access to view aspects of the blockchain such as the origins of the product and any certificates the farmer may have attached to their transaction (i.e., Free Trade, Organic, etc.) but they would not be able to use a blockchain explorer to view proprietary information within the transactions due to the use of zero-knowledge proofs at the transaction level. Smart contracts would be used to pay the farmer, truck driver, etc. immediately upon verification of delivery of the agreed upon amount of product [2].

User stories

- As a consumer, I want to view the origin of my coffee so I can verify it is free trade and organic.
- As a food safety regulator, I want to trace the food supply in case of a contamination incident so I can facilitate identification and recall.
- As a farmer, I want to see where my produce ended up so I can gather feedback by reading consumer reviews.
- As a factory foreman, I want to see where the product is enroute to the factory so that I can be sure to have enough workers to unload the truck when it arrives.

4. Proposed Ecosystem

As noted above, we will use a public blockchain so that the chain is truly decentralized. Validating transactions is done by each player involved in a transaction. If a farmer delivers one ton of fruit to a truck driver, the farmer and truck driver each validate the authenticity of the transaction using the zero-knowledge proof mechanism described later in this paper. They will each attach a fee (coins) to the transaction when they validate it which incentivizes block miners to participate in the mining of the blocks. Validated transactions are then mined by nodes using a Proof of Stake mechanism to assemble them into blocks. The miner who assembles the block will keep the coins attached to transactions as a reward. Anyone with the proper stake would be able to mine blocks.

Coins are kept in a wallet which contains key pairs consisting of a private and a public key. The public key is used to transfer coins for transactions while the private key is used by the wallet owner to secure the wallet.

5. Blocks

Blocks in a blockchain are like pages in a ledger book – they record verified transactions. Blocks are connected by a unique hash key that contains a hash of the previous block and the hash of transactions in the current block which produces a unique key for each block.

As noted earlier, within a supply chain, companies may have proprietary information in transactions that they do not want to share with the world at large. Because of this, we will use zero-knowledge proof (ZKP) as the mechanism to validate transactions prior to assembling them in a block. The benefits of ZKP include simplicity, increased privacy and security and shorter transactions [3]. ZKP allows for trust without having to share unnecessary information and will be used between validators on each side of a

transaction to verify they agree on the specifics of the transaction. In addition, because we can encrypt the transactions between nodes using ZKP, this means that only the two parties involved in the transaction will see the full data [4]. ZKP is also used by OriginTrail in their supply chain protocol [5] and by Zcash for their cryptocurrency [4].

Verified transactions then go to the mempool to wait for assembly into a block. Using Proof of Stake, a selected miner will grab the transactions in the mempool to assemble a block, as described in section 7. Because transactions are pre-validated, there is no need to validate each transaction, instead the only job of the miner is to assemble the block which makes the process very fast, and blocks can be generated as soon as one block is finished and more transactions are ready to be mined.

6. Hashing/ Signatures

Hashing is taking data of any size and mapping it to a fixed size using an algorithm. The same input will always produce the same hash, but a slightly different input will produce a wildly different hash output. In blockchains, hashes are used to ensure that the data within the block has not been altered in any way and also to connect blocks to each other. In essence, it is a digital signature verifying the validity of each block. This is important to ensure the integrity and immutability of the blocks – if any part of a transaction or block is changed, then the hash would be different, and any subsequent blocks would be invalid since their hashes are all based in part on that changed block.

SHA 256 is one of the most common hashing algorithms used for blockchain [6] and is the one we will use as well. The hash of each block is the hash of the previous block coupled with the hash of the transaction(s) within the current block. There is no need for a nonce since we are not using a Proof of Work consensus mechanism.

7. Consensus Mechanism

A consensus mechanism is how the nodes on blockchain agree on if a block of transactions is valid. Proof of Work (PoW) would be unnecessarily complex and wasteful in a supply chain situation, instead we will use Proof of Stake (PoS). PoS is faster than PoW and uses less energy to validate blocks since miners are not competing to mine the same transactions [7]. PoS requires miners own a certain number of coins and that every time they are selected to mine a block, they put up a portion of that stake as collateral against their work in mining the block [10]. PoS selects a miner randomly from the mining pool who then mines the block and sends it out as a candidate block to the network where it is validated by other nodes and added to the blockchain. The miner who creates the block receives a payment of the fees attached to the transactions within the block after the block has been confirmed by a certain number of other nodes.

8. Stakeholders and Motivation

Stakeholders would include the users of the blockchain (who also act as transaction validators) - farmers, transporters, wholesalers, factories, retailers - as well as any investors, miners, and the blockchain developers.

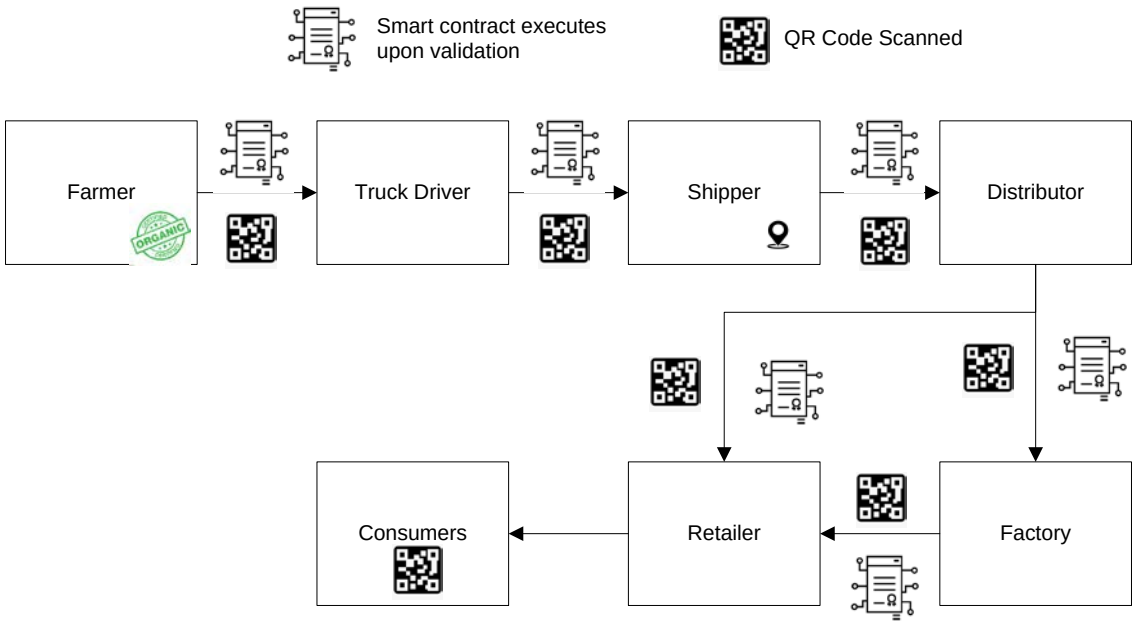
The motivation of both investors and miners is economic. Investors have an interest in seeing the blockchain do well so that their investment is profitable for them; they are compensated by the increasing value of their investment. Miners are compensated by the fees obtained from mining transactions.

Blockchain developers create the blockchain and any dApps and Smart Contracts associated with it. Their main motivation is to keep the chain working and to get paid for a good job. If the chain fails, they are out of a job.

The users of the blockchain in essence all have similar motivation – to make their lives easier and to make the process more transparent overall and to make payments easier. In their role as validators, their motivation is to ensure that the data is correct so that they get paid properly.

9. Flow Diagram

A small, organic fruit farmer in South America digitizes his organic certificate and uploads it to the blockchain along with the information regarding his latest harvest. This harvest is put into crates tagged with a QR code that points to the blockchain. The farmer sells the fruit to a distributor in the US who hires a truck driver to pick up the fruit and bring it to a ship they have contracted to deliver the fruit. A GPS device tracks the shipment to locate exactly where the product is enroute. A smart contract is set up to pay the farmer immediately upon verification that the truck driver has picked up the agreed upon amount of fruit. Another smart contact is set up to pay the truck driver upon delivery and confirmation that the load was delivered to the ship and another smart contract is set up to pay the ship captain immediately upon delivery of the fruit at the distributor's docks. All of these are triggered by scanning the QR code at various locations, which is written to the block chain. The distributor sells the fruit to a factory or a grocery store, again all of it written to the block chain. Once the consumer buys that fresh fruit from the store or the fruit juice made in the factory, they can scan the QR code on the package and see exactly where that item came from and the fact that the farmer indeed is a certified organic farmer.



10. System Considerations

We protect against bad actors by using ZKP to validate transactions and PoS to mine blocks, which allows for consensus even if nodes do not trust one another.

We do not anticipate any scaling issues. Unlike a cryptocurrency, we will never have need to mine millions of transactions per second but even if we did, proof of stake is an extremely fast, scalable protocol [9] and block size limits can be adjusted to accommodate more transaction if necessary. There is no need for arbitrary throttling as with Bitcoin.

There will be a need for outside databases to connect to the blockchain so that companies connected to each leg of the supply chain can use the data for their own internal processes. In addition, there will be a need to federal health and safety authorities to have access to the data in the blockchain to trace any public health threats.

11. Conclusion

Modern food supply chains have many issues which blockchain has the potential to improve with its inherent transparency, immutability, and smart contract integration. Our food supply chain system is a public blockchain that uses zero-knowledge proof as a transaction validation system and proof of stake for block mining. Products are tracked with QR codes, scanners and GPS and smart contracts are deployed for timely payments. Altogether, this leads to insight into the full supply chain, allowing for easier tracking of goods along the chain as well as giving consumers the ability to do their own due diligence and for authorities to trace contaminated food quickly and easily.

While we propose beginning with simple integrated technology as noted above, future enhancements could include more integration with other technology such as RFID tags, IoT, tamper proof seals with NFC technology that would help ensure better tracking and control of possible adulteration and food contamination.

References

[1] https://www.blumeglobal.com/learning/supply-chain-explained/
[2] https://primerevenue.com/resources/blog/solving-the-late-supplier-payment-problem/
[3] https://101blockchains.com/zero-knowledge-proof-blockchain/
[4] https://www.coindesk.com/markets/2016/09/11/the-trend-towards-blockchain-privacy-zero-knowledge-proofs/
[5] https://origintrail.io/storage/documents/OriginTrail-White-Paper.pdf
[6] https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm
[7] https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake
[8] Video: Blockchain In Food Industry (Part 2) | DOCUMENTARY | Cryptocurrency | Bitcoin | NFC | RFID | QR
[9] https://medium.com/@poolofstake/proof-of-stake-and-scalability-2ecaa8fd5d7c
[10] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Additional references:

https://www.forbes.com/sites/yasamankazemi/2019/06/27/how-the-modern-supply-chain-is-evolving/
https://foodindustryexecutive.com/2020/08/demand-for-transparency-continues-to-increase/
https://www.blumeglobal.com/learning/smart-contracts-blockchain/
https://www.mckinsey.com/business-functions/operations/our-insights/blockchain-technology-for-supply-chainsa-must-or-a-maybe
https://www.hyperledger.org/learn/publications/walmart-case-study
https://corporate.walmart.com/newsroom/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens
https://www.provenance.org/whitepaper
https://www.mdpi.com/2305-6290/5/3/46/pdf
https://agrichain.com/
https://blockheadtechnologies.com/zero-knowledge-proofs-a-powerful-addition-to-blockchain/
https://101blockchains.com/zero-knowledge-proof-blockchain/
https://z.cash/technology/zksnarks/
https://cryptoandfire.com/zero-knowledge-proof-zkp-in-blockchain/

Video: Blockchain In Food Industry (Part 1) | DOCUMENTARY | Crypto Currencies | Bitcoins | Supply Chain
Video: Blockchain for Food Traceability in Supply Chains
Video: How the blockchain will radically transform the economy | Bettina Warburg
Video: Alternative Consensus Mechanisms
Video: Blockchain 101 Ep 57 - What is Zero knowledge Proof?
Video: Zero Knowledge Proof - ZKP
Video: What are zk-SNARKS | Mina Protocol
Video: zk-SNARKs Explained - Basic Principles (Privacy, Blockchain & Crypto)