The challenge of authenticity: Blockchain in the supply chain

Received (in revised form): 4th November, 2018

Sam Kramer

SAM KRAMER

is a partner in Baker McKenzie's Chicago office in the Intellectual Property and Technology practice. He represents customers in managed services, IT procurement, complex licensing and supply chain agreements, and is a frequent speaker on outsourcing, cloud services and blockchain. Sam is co-chair of the company's North American FinTech Steering Committee and a member of the company's Global FinTech Steering Committee. Sam is recognised in Chambers Global, Chambers USA, the Legal 500 USA and Who's Who Legal. He is an adjunct faculty member in the Information Technology LLM programme at The John Marshall Law School, where he has taught cyberspace law.

Abstract

Today's complex and dispersed supply chains create significant challenges for supply chain managers. 'Organic', 'non-GMO', 'fair trade' and 'conflict free' are just some of the claims that require a transparency in the supply chain to maintain and verify. Product origin and authenticity are similarly at risk from a lack of transparency in supply chain data. Traditionally, supply chain managers use cumbersome and unreliable auditing to validate supply chain data to substantiate product information and provenance. But errors and fraud in supply chain information remain and threaten the brand reputation of affected products. Supply chain data is no stranger to technological enhancement. Enterprise resource planning systems have expanded the volume of real-time actionable data available. The reliability of that data is, however, still in question from its susceptibility to errors and falsification. Distributed ledger technology, best known as blockchain, offers the promise of greater transparency and reliability of supply chain data. Ultimately, that reduces the risks associated with product claims and provenance based on supply chain data. This paper examines the operation of blockchains and their resistance to falsification by looking at the mechanics of the bitcoin blockchain. The paper explores private blockchain alternatives to the bitcoin blockchain that can facilitate distributed data in a closed supply chain. The paper then describes several supply chain challenges where blockchain technology is being used to improve the reliability and integrity of the underlying supply chain data. Finally, the paper looks to the blockchain regulations that may have an impact on the adoption of blockchain in the supply chain. At the end of the day, substantiating supply chain product claims, minimising counterfeiting and enabling product recall all rely on the traceability and integrity of supply chain information, for which blockchain solutions are well suited.

Keywords

blockchain, supply chain, traceability, provenance

Sam Kramer
Baker & McKenzie LLP,
300 East Randolph Street,
Suite 5000,
Chicago, IL 60601,
USA

Tel: +1 312 861 7960;
E-mail: samuel.kramer@bakermckenzie.com

BITCOIN BLOCKCHAIN AND CONSENSUS

Any discussion of blockchain technology begins with bitcoin — the first, and best-known, blockchain. It is an unpermissioned blockchain, meaning that anyone who downloads a Bitcoin wallet can participate in buying and selling Bitcoins. Transactions on the bitcoin blockchain involve the transfer of records of Bitcoins from one account record to another. It is a distributor ledger that reconciles Bitcoins sent and Bitcoins received.

It is natural to wonder why a discussion of blockchain in the supply chain involves a cryptocurrency like Bitcoin. Assets in the real world are represented on a blockchain with a token or coin, and transfers of those tokens transfer the associated data (eg instructions, certificates, unique identifiers) along the blockchain. The mechanisms that cryptocurrencies use to prevent alterations of the ledger and double spending of coins are the same mechanisms used to maintain the integrity of supply chain data recorded to the blockchain.

The bitcoin blockchain was created to be a cashless peer-to-peer network for the exchange of value. In a transaction on the bitcoin blockchain, a Bitcoin holder wants to transfer some amount of Bitcoins to a recipient. To effect this transaction, the Bitcoin holder initiates a transaction that references some prior transaction on the blockchain in which the sender received Bitcoins. The transaction is initiated by the sender's private key (known only to the sender) and is a public instruction to identify one or more transactions in which the sender's public key (his digital wallet 'address') received Bitcoins, and to take those Bitcoins previously received and transfer them to the recipient's public key. Essentially, this is a change to the state of the ledger: the blockchain ledger has a public record of Bitcoins the sender previously received, and a new instruction has been given to update the ledger to reflect the transfer of an amount of unspent Bitcoins (the sender's 'balance') to the recipient.

To participate in the bitcoin blockchain, one only needs to download a digital wallet and a copy of the then-current blockchain ledger. Every participant who wants to send or receive (buy or sell) a Bitcoin has an identical copy of the current state of the ledger. The transaction 'send X Bitcoin from A to B' is broadcast to all the nodes on the network, and each node relays that transaction to other nodes so that the message is quickly replicated and made available to all. If a node receives a transaction that is based upon an altered ledger entry, the transaction is ignored. Only transactions that are valid on their face — ones that point back to a prior transaction on the blockchain where the sender received the Bitcoins that have not already been spent and that he now intends to spend — are rebroadcast. If a malicious person (the sender or some other party) tried to falsify the ledger entries — to inflate his balance of Bitcoins, or to erase a prior transaction in which he spent Bitcoins — that altered ledger would not match the other copies held by every other node, so the altered version would be quickly identified and ignored. This distributed ledger means that there is no single repository of transactions to hack into to falsify the data.

Transactions that appear to be valid are rebroadcast to all nodes on the network, including those nodes that serve to validate transactions for permanent addition to the blockchain ledger. These nodes are known as 'miners', and they assemble presumptively valid transactions into batches, called 'blocks', to be appended permanently to the blockchain. Once part of the blockchain, the new block points back to the previous block, and the same with each block in the chain.

Each block of the blockchain is encrypted with a strong cypher, and any alteration of any element of any block in the chain alters the hash of the blocks.

Applying this technology to blockchain transactions makes the ledger immutable. No prior record in a previous block can be changed without alerting the network that the copy of the proposed blockchain has been altered.

Miners who take a batch of presumptively valid transactions proposed to be added to the consensus blockchain must demonstrate proof-of-work: that computer resources were used to solve a mathematically difficult puzzle. Solving this puzzle requires repeated hashing by trial and error, and its only purpose is to evidence that the miner proposing the block has expended resources.

Essentially, proof-of-work creates a tax on identities on the network. Because acceptance of a block is determined by a consensus of most nodes, were there no cost to proposing blocks, a malicious node could create a mass of alter egos and fool the network into thinking that one node represents a majority (this is also called a Sybil attack). If I were a malicious node, I could alter the blockchain record (eg to erase a prior transaction of Bitcoins spent) and then use all my alter egos that appear to represent a majority of nodes to convince the remaining nodes to follow the altered blockchain record. With a proof-of-work requirement for achieving consensus, the likelihood of adding the next block on the blockchain does not vary in proportion to the number of identities (nodes) on the network; rather, it varies in proportion to the amount of computer resources controlled on the network. So, if your computing power represents 10 per cent of the total network computing power (regardless of the number of nodes), you have a 10 per cent chance of solving the maths puzzle and adding the next block.

Miners race one another to be the first to solve the maths puzzle and propose the next block. The bitcoin software automatically adjusts the degree of difficulty of this puzzle so that a block is solved on average once every 10 minutes.

As miners race to propose new blocks, two blocks may be proposed at roughly the same time. Those blocks may not contain identical transactions, and may in fact contain incompatible transactions. Suppose, for example, that I had a balance of 5 Bitcoins that I wanted to transfer, and I initiated two transactions: one that transferred 5 Bitcoins to recipient A and one that transferred 5 Bitcoins to recipient B. These are both presumptively valid transactions; I have the 5 Bitcoins to transfer to either recipient A or recipient B, but I cannot transfer 5 Bitcoins to both. Two blocks proposed at roughly the same time with incompatible transactions create a fork in the blockchain. The fork will eventually be resolved by the network building on one side of the fork. The convention is to wait for six subsequent blocks to be built on the blockchain before the transaction is considered confirmed. And with 10 minutes between block creation, a transaction on the bitcoin blockchain is confirmed after one hour.

Blockchains operate on the consensus of the majority of its participants. In a system where no trust can be presumed, the bitcoin blockchain protects against a false projection of a majority by imposing a cost on those who would propose adding blocks to the blockchain (and rewarding the winner with newly minted Bitcoins). It also protects against double-spending with close-in-time transactions by requiring six subsequent blocks for transaction confirmation. These protections impose burdens on blockchain participants: the cost of mining hardware and the electricity needed to operate them, as well as the built-in delay of transaction confirmation.

PERMISSIONED BLOCKCHAINS AND CONSENSUS

Unpermissioned blockchains, such as the bitcoin blockchain, are useful in environments where no trust is presumed — no trusted central authority and no trust is required of any other participants. Proof-of-work is a consensus mechanism that does not require trust of any other network participant. A blockchain dedicated to an enterprise supply chain would be open only to participants known to the blockchain operator. While a supply chain participant may still act maliciously, the bad actor can be identified (and punished), making intentional wrongdoing less likely.

Permissioned blockchains can use consensus mechanisms to validate blockchain transactions that do not have the costs or delays associated with proof-of-work. Permissioned blockchains are curated: its participants are invited and their identities are known. Certain protections necessary for unpermissioned blockchains to resist malicious actors, such as proof-of-work to disincentivise Sybil attacks, are not needed in invitation-only blockchains. Proof-of-stake, practical byzantine fault tolerance and federated consensus are each consensus protocols that are alternatives to proof-of-work. These consensus mechanisms are lower cost, faster and capable of handling a greater throughput than proof-of-work systems designed and hardened to validate transactions in a network of unknown and untrusted participants.

One example of a consensus mechanism in a permissioned blockchain uses a round robin voting system to validate batched blockchain transactions through pre-selected but replaceable groups of validators. They vote on transactions, with only larger majorities of votes allowing the transaction batch to pass to the next round, until a super-majority affirmative vote results in the block of transactions being appended to the blockchain. This consensus mechanism relies on game theory to demonstrate that so long as no more than one-third of the nodes are acting maliciously, the resulting transaction can be trusted. This is possible in a finite 'members only' group such as a supply chain network, but would not be possible in a public and anonymous blockchain. As a result, a supply chain-based permissioned blockchain can take advantage of these cheaper, faster and more scalable consensus mechanisms instead of proof-of-work.

SUPPLY CHAINS AND TRANSPARENCY

Today's supply chains can involve thousands of suppliers and hundreds of thousands of raw materials and components, cross international borders and use multiple modes of transportation. Technology such as enterprise resource planning systems enabled the capture of detailed supply chain information, but its complexity led to integration issues, data entry errors and reconciliation problems. When a processed food producer makes a claim that its product is GMO-free, it is relying on the integrity and accuracy of data originating from numerous upstream suppliers, from growers, to warehouse operators, to shippers and packagers. Incorrect information introduced into the stream of data, supplied wittingly or unwittingly, can cause disruptions and delays, as well as financial and legal exposure.

Supply chain data networks can have multiple points of centralisation that require reconciliation and settlement. It can take days from the presentation of a bill of lading to reconcile it with the purchase order and pay suppliers. This network problem is magnified when data has been re-entered and transmitted across the supply chain with no visibility for remote supply chain participants to the original data stores and its transaction across the supply chain. The costs associated with processing of trade-related paperwork are estimated to be from 15 per cent to 50 per cent of the cost of the physical transport of the goods. Large supply chain partners are experimenting with smart contracts on the blockchain, which automatically release payments under letters of credit when the blockchain verifies the arrival of goods in port, lowering the reconciliation cost and speeding the payment process.

Costs from supply chain data inefficiencies are not only bureaucratic. Bad or fraudulent data can have a direct cost impact on producers, from recall costs to brand impact. In the food industry, the efficacy of addressing food safety issues is largely dependent upon the quality of the data. A salmonella outbreak in 2017 alone sickened 173 people, and the total impact of food-borne illness on the US economy is estimated to be in the tens of billions of dollars. It can take weeks to track down the source of contaminants, and longer to restore consumer confidence in a tainted brand.

Walmart, already a leader in supply chain traceability, conducted a tabletop exercise using its state-of-the-art food tracing systems to identify the origin of packaged mango slices. It took six days, 18 hours and 26 minutes to trace the package to the farm of origin. Using a blockchain-based system of supply chain records developed by IBM, the same exercise took 2.2 seconds. This dramatic reduction in time to answer could represent the difference between a targeted removal of specifically identified packages and a product-wide recall. Blockchain-based supply chain data traceability suggests that blockchains could dramatically reduce supply chain costs, from trade-related paperwork costs to product recall costs. Walmart has notified all its leafy green vegetable suppliers that they are required to implement its food traceability blockchain solution by September 2019.

Transparency in the food supply chain is a long sought-after feature to combat unsustainable harvesting, illegal fishing, food misidentification and exploitative labour practices. Blockchain company Viant uses QR tags to identify fish at the point of catch and upload the data to a blockchain, so that the fish can be traced as it moves from fishing boat to distributor to wholesaler to table. This transparency combats the fraudulent misidentification of fish that separate studies in Los Angeles and New York have found to be rampant. By uploading the transfers of fish through the supply chain, consumer purchasing the tagged fish can read the blockchain record associated with their fish purchases to identify the item from catch through each subsequent change of hands to their local market.

The coffee industry has suffered from unfair labour practices for many decades. Bext360's blockchain solution has enabled Moyee Coffee to identify the source of its coffee beans to the grower, ensuring that it purchases only fair trade coffee. The blockchain can also be configured to use smart contracts to automatically pay the farmer upon sale of the coffee beans. The diamond industry too has had forced labour in mining for gemstones that has resulted in international bans on blood diamonds. Everledger has created blockchain-based asset tagging of diamonds to track the provenance of loose diamonds. The blockchain data is also useful in meeting reporting requirements for conflict minerals under the Dodd-Frank Act.

COMBATTING COUNTERFEIT IN THE SUPPLY CHAIN

In the previous section, we identified ways in which the lack of transparency in the supply chain can result in delays and costs that blockchain-based systems can reduce significantly. Faster access to more reliable supply chain data can not only reduce costs, but can also reduce malicious behaviour in the supply chain. It can provide a record of authenticity for goods as they move through the supply chain, reducing the risk of counterfeit goods reaching the consumer.

Blockchains are also capable of digitally mirroring assets in the real world. The blockchain can store the physical properties of the asset and transfers of the physical good can likewise be stored on the blockchain. These can range from simple certificates of ownership (eg by associating a serial number with the digital wallet of the owner) to mirroring each component of the product through its transformation in the supply chain.

Blockchains can also be used to create an immutable record of component transfers, ensuring an unimpeachable record of transfers from the component manufacturer through assembly to retail sale of the finished product. This is accomplished using a blockchain (bitcoin or other coin-based blockchains, such as Ethereum) by making very small payment transactions for each transfer of a component in the supply chain.

The manufacturer will create a digital wallet for each component part. The manufacturer buys the smallest fractional portion of the digital coin (the equivalent of a penny or smallest fraction of the digital currency) for each component. A batch of the components is sent to an assembler, along with a transfer of an equivalent number of 'digital pennies'. The assembler checks that the 'digital pennies' match the number and date stamp of the component supplier's delivered components. When the assembler delivers the assembled components to a distributor, the assembler transfers that portion of the 'digital pennies' received from the component supplier equal to the number of assembled components delivered to the distributor. The distributor then verifies that the 'digital pennies' received match the number and date of assembled components. And so on. In this way, the supply chain participants use the associated transfers of 'digital pennies' recorded in an immutable blockchain to verify the provenance of the components as they travel along the supply chain.

Introducing counterfeit components into this supply chain becomes an unprofitable enterprise. The fraudulent component supplier would have to have an equal number of authentic components with the same transfer dates. Once the component supplier sells the counterfeits, there is no way for the supplier to prove that the authentic components are indeed authentic.

The blockchain-secured supply chain described above provides an immutable record of the components as they traverse the supply chain. All components and sub-assemblies that have been assembled in the final product are subject to a traceable record. Any authorised servicing agent can determine whether the product is legitimate with all authentic components.

Once the final product has reached its end of life, the accumulated 'digital pennies' (ultimately paid by the retail consumer) can be refunded to the consumer upon recycling, allowing the manufacturer to regain control over the parts and to meet e-waste disposal obligations. This would not be available to consumers of counterfeit products, even those composed of authentic but harvested parts.

BLOCKCHAIN-ENABLING LEGISLATION

Blockchains offer a technological solution to failures in supply chain data integrity. Distributed ledgers offer a lower cost, faster and more reliable means to authenticate data across the supply chain, even to remote participants. The reliability of these immutable records can be demonstrated mathematically, but for them to have validity as a supply chain record, they must have legal recognition.

Several US states have addressed the status of records stored on the blockchain. Arizona amended its Electronic Transactions Act to recognise records or contracts secured to a blockchain as electronic records, and confirming the legal validity of smart contracts. Vermont amended its laws of evidence to allow the introduction of records secured on a blockchain as business records. And the State of Delaware amended its corporate law to recognise blockchain-based business records and to permit stock ownership to be recorded on the blockchain. These early legislative efforts to legitimise blockchain-based records in the legal system are another step in the direction of adoption of blockchain in business transactions. The legal recognition of information secured on a blockchain allows supply chain participants to rely on blockchain records to support payment authentication, authenticate provenance of goods and substantiate product-related claims.

CONCLUSION

Businesses are managing geographically dispersed suppliers and sub-suppliers in increasingly complex relationships. These attenuated relationships are increasingly difficult to manage and the supply information generated lacks transparency. These business realities strain the ability of an organisation to centrally manage its supply chain and the necessary commercial information that flows through it. Blockchain-based technologies offer potential solutions to some of these challenges by permitting supply chain data to be maintained and verified in a decentralised manner. The immutable nature of the blockchain allows all participants, from initial suppliers to end customers, to rely on the authenticity of the data residing on the blockchain. Adding transparency to distributed supply chains helps to reduce the risk of fraudulent and counterfeit goods, and traceability reduces the time between discovery of dangerous goods and their withdrawal from the market. Finally, the availability of blockchain-based supply chain data can enable companies to meet compliance obligations where data is frequently unavailable or unreliable.