DeLaRue

Supply Chain and BlockChain

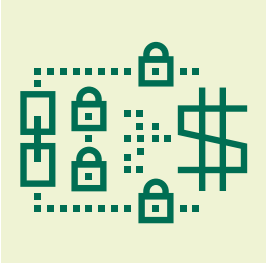
April 2018

Supply chain management and security is where blockchain technology shows great promise. Brand owners and manufacturers have new tools allowing them to bring authentic goods to market more efficiently and securely.

DeLaRue

Table of Contents

Introduction

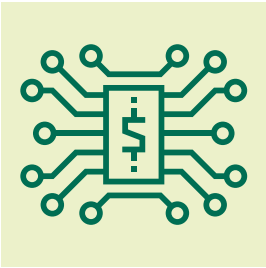


Blockchain has captivated the global economy like a tidal wave. At times it seems to be all consuming, and the suggested answer to every question. The purported benefits are endless and it promises to revolutionize nearly every industry. Proponents claim that it will provide transparency, security, efficiency, immutability, and many other virtues long pursued within finance, manufacturing, shipping, and retail.

Truthfully, in many cases, blockchain is a solution looking for a problem to solve. In fact, the concept, definition, and execution of blockchain is evolving even as it is implemented. The original versions of blockchain are proving to be cumbersome and ill-suited for most purposes. Consequently, revisions to existing blockchain technologies and new innovations are created and implemented as quickly as problems are discovered. New breeds of blockchain technology promise to solve specific problems for each market sector. The term 'blockchain' no longer describes a single concept popularized by Bitcoin and Ethereum.

Supply chain management and security is one sector in which newer modified versions of blockchain technology show great promise. Brand owners and manufacturers have new tools allowing them to bring authentic goods to market more efficiently and securely than ever before. Retailers and consumers are able to play an active role in product authentication and traceability. Here we discuss the creation and implementation of these newer technologies, specifically as they relate to brand protection and secure distribution of goods.

Origins and Evolution of Blockchain



There are currently countless white papers and articles describing the origins of blockchain with the creation of Bitcoin and the subsequent evolution of Ethereum. Other articles provide a detailed explanation of the mechanics of original blockchain technology. However, before discussing the implementation of certain technologies, a brief primer on older and newer technologies may prove useful.

Most are now familiar with the origins of Bitcoin as the first widespread implementation of distributed ledger technology that we now call blockchain. In summary, it is an open network of computers using their processing power to solve cryptographic problems. In so doing, they are validating transactions in hopes of earning a monetary reward. These transactions are immutably written to a public ledger, effectively eliminating the requirement for trust between counterparties. The community verifies the transactions, and fills the role of the intermediary that we've grown so accustomed to. The moniker "blockchain" describes the series of transactions written to the ledger in sequence like a chain of data blocks.

Although the idea was novel, soon after the rise of Bitcoin it was discovered that distributed ledger could be more than a simple means of cash transaction. Instead of a basic accounting ledger, blocks of code might contain contract terms or other descriptive script. This realization led to the birth and rapid popularity of Ethereum, a public ledger allowing the exchange of anything of value including information. The creation of "smart contracts" allowed for autonomously executing programs immune to censorship or interference. Again, the public network would validate transactions, eliminating the intermediary and creating the immutable ledger.

These early generations placed a strong emphasis on community validation. The primary intent was disintermediation; the creation of a network that eliminated the central authorities and any type of interference. The inherent requirement for such a network is openness, or what is referred to as a "permissionless" network. Anyone can participate
as a node in the network. Indeed, the technology relies on broad participation from many unrelated parties to prevent a coordinated attack on the integrity of the ledger. Unfortunately, it wasn't long before the drawbacks of these permissionless networks became apparent. Public networks lacked the kind of scalability offered by traditional databases. They were increasingly slow and required too much resource to maintain. Additionally, apart from select applications, complete disintermediation and public transparency are not necessarily a requirement. Indeed, many use cases demanded a much greater level of privacy than a public ledger could provide.

Soon after, new generation technologies appeared in the form of non-public "permissioned" blockchains. IBM Hyperledger Fabric quickly gained popularity and others such as Hashgraph were released to target specific markets. Participation would not be public, and would instead require permission to become a node in the network. These nodes would be granted a certain status and would not be financially compensated for their validation efforts. Consequently, there would be no need for associated cryptocurrencies that fluctuate wildly in value.

These next-generation networks would emphasize privacy, security, and scalability. Most importantly, they still benefit from the critical efficiency and trust gains inherent in legacy blockchains. Multiple disparate partners could read from and write to a ledger without the worry of a single bad actor falsifying the record, and there is now a promise of development for a single global standard that will offer a plug-n-play solution across the entire value chain.

Critically, the newer ledger technology offers dramatic scalability that was conspicuously lacking in the earliest version of the technology. Bitcoin and Ethereum had originally offered processing speeds of 3 to 30 transactions per second. On a global scale, tracking billions of packages, this is woefully inadequate.

Conversely, newer versions of consensus ledgers mentioned above - Fabric and Hashgraph – offer per-second transaction speeds of 3,500 and 250,000 respectively. To offer a bit of perspective, two of the largest payment processing networks, Paypal and Visa, reach per-second speeds of 193 and 1,667 respectively, suggesting that the newer blockchains certainly offer the desired scalability.

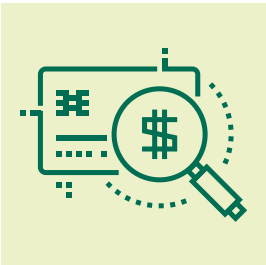
Blockchain for Supply Chain

Distributed ledger technologies are highly beneficial when there is a large network of disparate actors. As such, the technology is well positioned for use in supply chain management. Tracking goods, and components of goods, from the original blueprint to the end consumer might see the product or component pass through dozens of different checkpoints along the value chain. Often these checkpoints might be internal to a single organization but at different locations throughout the world. Many times the route will involve in excess of 30 different people and organizations external to the brand owner, such as contract manufacturers, licensees, shipping companies, customs officials, etc.

Such a fragmented process includes a significant amount of inefficiency and vulnerability to fraud. To combat this, there are several companies tailoring a blockchain solution to supply chain management. For example, it was recently announced that Maersk and IBM have embarked on a joint venture that seeks to use IBM Hyperledger Fabric to create a standardized blockchain for global logistics management. This type of effort will be key in blockchain adoption for supply chain. Gains in efficiency and cost reduction will be much more pronounced if the industry will widely adopt a single effective architecture.

Specifically, this type of network differs from the original blockchain technology in that it is designed as a consortium style permissioned network. A shipping company and brand owner would have the necessary control to approve various parties for access to the network in creation of a validation consortium, and then utilize the system to track the product through the various checkpoints en route to the final destination. Such a network realizes the benefits of scalability and speed offered by a traditional internal database, but offers the virtues of a blockchain; transaction immutability, significantly reduced paperwork, real-time monitoring, supply chain validation, and dramatic reduction in delays at various checkpoints.

Security Issues within the Supply Chain



For all the virtues of blockchain, there remain several problems within supply chain management that distributed ledger technology cannot sufficiently address on its own. This is because blockchain is inherently just a ledger system, very similar to the track and trace functionality that has been offered within the brand protection industry for many years. Certainly, in many cases blockchain provides a superior version of track and trace, but it is inherently limited in the same ways. A robust value chain isn't simply defined by a speedy transit at low cost. There are two significant underlying assumptions. First, the product and quantity received at the final destination is exactly what was expected. Second, the product entering the shipping channel was authorized in the first place. The following are several issues that must be addressed within the value chain to ensure product integrity.

- Counterfeit Production
- Diversion
- Tampering and Adulteration
- Overproduction
- Theft
- Returns and Warranty Fraud

Counterfeit Production

Counterfeit production introduces fake product to the market from unauthorized manufacturing. To combat this, individual product must be securely tagged in a manner that is impossible to circumvent or reproduce. Blockchain aids in counterfeit prevention by allowing real-time tracking of authentic goods. For example, a container of counterfeit shoes arriving at a port, absent the required digital certificate of authenticity and history contained on the blockchain ledger, would be seized by customs preventing it from ever reaching the final destination. The underlying assumption is that the code linked to the digital certificate has not been reproduced or falsified. Blockchain alone cannot address this issue but can integrate seamlessly with robust authentication tokens.

Overproduction

Overproduction introduces excess product through authorized manufacturers, thereby avoiding the payment of licensing fees and royalties to the brand owner. Blockchain provides a mechanism whereby the authorized manufacturers are unable to push excess product into distribution. The brand owner is able to effectively create a pull transaction which authorizes only a select quantity to enter the distribution channel. As each item is individually serialized, a secure digital certificate would disallow excess production.

Diversion

Diverting authorized goods into an unauthorized distribution channel dilutes the integrity of the brand through tax avoidance and excess supply of goods into regions with higher profit margins. Real-time tracking of the pull transaction referenced above would notify the brand owner of products received outside of the intended region.

Theft

The physical act of an unauthorized actor stealing from an authorized distributer or transporter is difficult to prevent. However, a secure digital token with registered certificate can be deactivated prior to final distribution. Deactivation of the certificate essentially converts authentic product into counterfeit product that can no longer be sold through authorized channels. Indeed, blockchain ultimately allows the product to be fully certified only upon receipt at the final destination.

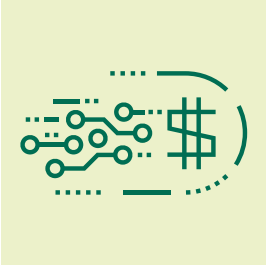
Tampering and Adulteration

Unauthorized access to the product provides opportunity for a bad actor to modify or replace the product or components with cheaper substitutes. Blockchain can do little to prevent tampering and must rely on integration with a secure tamper evident physical token. Such a token can be made to indicate whether there has been unauthorized access to the product, or even whether a critical component has been replaced.

Returns and Warranty Fraud

Fraudulent warranty or service claims can be prevented through proper registration of product and verification of the digital certificate when the claim is made. Again, it is critical that the digital code be protected from reproduction, which ultimately would require integration with a secure physical token or code.

The Ideal Solution



As explained above, there are many ways in which blockchain technology can assist in securing the supply chain. Ultimately, a robust manufacturing and distribution channel must offer timely efficient delivery of only authentic goods and materials. The ideal solution should address all value chain efficiency and security challenges.

One very big challenge in the industry has to do with the simplistic assumption that everyone in the value chain, from the brand owner to the consumer, desires product authenticity. As it turns out, this assumption many times proves incorrect in practice. Obviously, each actor has different incentives. A shipping company might value transactional efficiency very highly, and completely disregard product protection or authenticity. A retailer might be facing a tradeoff between the integrity of the brands they sell and maintaining sales revenue and margins. Even the consumer can be less concerned about product authenticity than about price, provided that a certain level of functionality is achieved.

Ultimately, the greatest beneficiary of a fully secure value chain is the brand owner. However, the motives and areas of greatest concern will be unique to each. Some might be primarily concerned with liability, some with consumer protection, and others with product integrity and public perception. A certain brand owner might desire that individual consumers join in the fight against unauthorized products, while others prefer a more behind-the-scenes approach. The ideal solution must be tailored to provide authentication and data collection only where desired.

Blockchain offers significant benefits in cost reduction and efficiency, but only marginal benefits with regard to brand protection and product authentication, without a secure physical code or token. Essentially, a blockchain-integrated value chain promises to fill a role that is currently already provided by brand protection companies through Trace & Trace services. However, private permissioned blockchain tracking offers a few differentiating advantages over existing proprietary database systems.

- **Immutability**
  - When properly configured, the transaction history is secured and cannot be altered maliciously, even by a central authority.
- **Distributed Ledger**
  - Community or consortium validation eliminates the single point of failure inherent in a private corporate database.
- **Decentralization**
  - Consortium ledgers are originally configured centrally, but are then self-governing. This removes the high level of trust required in a fully private database. Members of the consortium hold one another accountable for ledger integrity.

Supply Chain and BlockChain

Single Solution

Broad adoption of a standardized consortium style permissioned ledger, like IBM Hyperledger Fabric, integrates seamlessly into the full suite of tracking and data collection services currently offered by brand protection companies.

World leaders in product authentication and traceability, like DeLaRue, are uniquely positioned to provide the differentiated benefits of newer generation blockchain technology through incorporation of the network into our authentication solutions.

Ultimately, simple tracking of products through distribution channels falls short. Enabling robust digital authentication tokens with distributed ledger technology offers a single, tailored, cost effective solution to the brand owner that is impossible to circumvent and promises to address all desired value chain challenges, both in terms of product security and logistical efficiency.

De La Rue International Limited De La Rue House, Jays Close, Viables, Basingstoke, Hampshire, RG22 4BS

www.delarue.com