Assessing Blockchain for Security in Manufacturing Supply Chains

July 2019

Identify3D

Executive summary

In the decade since Satoshi Nakamoto published his famous bitcoin paper, applications for blockchain technology have exploded. These applications, from cryptocurrencies to medical record-keeping, span a myriad of businesses across commercial and government sectors.

Many of these innovative use cases tout security as a key advantage provided by blockchain. However, in many cases, the security attributes conferred by blockchain could be better achieved with other technologies. In fact, applying blockchain technology in the manufacturing sector may not be living up to expectations.

What's going on here? How is it that a technology offering decentralization, immutability, security, and transparency is failing in the manufacturing sector?

To help untangle this conundrum, this document:

> "90% of blockchain-based supply-chain projects are failing *"due to a combination of technology immaturity, lack of standards, overly ambitious scope, and a misunderstanding of how blockchain could, or should, actually help the supply chain."* Gartner

1. Explores how blockchain can indeed benefit the manufacturing and supply-chain industries;
2. Assesses the principle benefits blockchain offers (and where it falls short);
3. Proposes a blockchain complementary approach that can help manufacturers achieve specific business objectives.

Blockchain Basics

The core structure and components of blockchain technology provide an immutable record of data that can be verified and shared by a group of semi-trusted members. A blockchain is composed of a set of sequential data blocks, each with a secure hash digest that represents the fingerprint of the data and links the data of the current block with the data of all previous blocks. Once a new block of data is presented as a candidate for the blockchain, all members have the ability to check that the hash digest of the candidate block is valid, and that there are no changes to any previous data on the blockchain. This ensures the integrity of the entire set of data blocks.

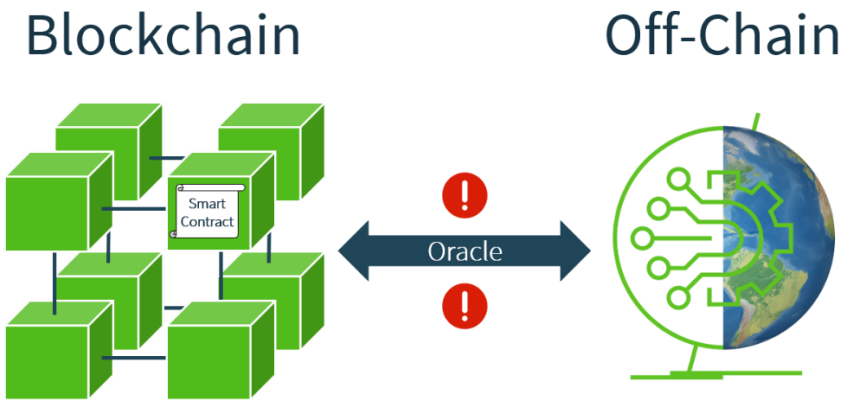
Although there are many database and data structure technologies with built-in integrity, the blockchain model enables a group of contributors to come to consensus on whether new data is accepted and can be stored in the blockchain. When the data is accepted, all members of the group are then assured of having complete and identical datasets.

Consensus models are complex, especially with cryptocurrency applications. However, most supply-chain technologies rely on a group of semi-trusted and vetted members acting upon a voting scheme for the group to come to consensus of the validity of a candidate block of data. This scheme avoids the pitfalls of proof-of-work consensus algorithms, such as the expensive mining operations used in bitcoin that underpin financial-based applications.

There are several private blockchain platforms that support supply-chain applications, including Hyperledger Fabric, Hyperledger Sawtooth, private Ethereum, and Multichain. Each of these technologies differ in implementation and how the data within a block is organized, but all are consistent with the foundational blockchain properties discussed in this paper.

Ledger records and **smart contracts** are the most common class of applications within a supply-chain blockchain ecosystem. To be precise, a ledger record on a blockchain is simply the recording of an event or transaction within a supply chain. A smart contract, on the other hand, is much more difficult to define with precision. Originally, smart contracts on blockchain were proposed as digital contracts implemented with logic rules as part of the block data.

Within a supply chain, records of transactions may be recorded as ledger entries, but if these entries are used to trigger off-chain transactions and operations, then they may be referred to as smart contracts. To be meaningful, the smart contract needs to interact with the outside world. This is accomplished through so-called oracles that provide both input and output to the blockchain. However, as we will discuss later, creating trust in these oracles is a desire left unfulfilled with current technology.



Ledger recording and smart contract functions can help address specific business challenges. For instance, improving traceability in supply chains is perhaps the most discussed attribute of blockchains. Traceability is provided by stored ledgers of transactional data, which may include manufacturing data, raw material sources, supplier transactions, as well as financial payment details.

From a consumer perspective, traceability can provide provenance of goods sold, for example in the pharmaceutical supply or food industries. It can also support confidence of authenticity in luxury goods. For large manufacturers that rely on extensive supply chains, this type of knowledge provides greater reliability in supplies and provides visibility into the state of production at subcontractors. Smart contracts in supply chains have, for instance, the ability to automatically generate payments between suppliers or tariffs.

Additionally, the ownership of IP such as designs or manufacturing process descriptions can be tracked and managed, including the allowed usage of that IP by each member of the supply chain. Within digital manufacturing, smart contracts can work even deeper and control the details of how digital parts can be manufactured, including restrictions on fabrication material and the number of parts that can be

produced. In this case, to be meaningful, the above-mentioned oracle should cryptographically link the actual digital IP referenced in the blockchain as well any physical system that produces physical parts from the digital IP.

It is important to highlight the fact that currently a major barrier to traceability relates to the confidentiality of the data belonging to the individual companies who participate in a blockchain. For instance, supply sources or production volumes are strategic data that is often too valuable to share. So, beyond the overall shared benefits brought by the use of a blockchain, it is always important to consider the potential downside that some participants might see when asked to share certain data.

In contemporary manufacturing, the supply chain is often complex and composed of many independent members. With the intense competition for market share, members closely guard their operational data. If there is no data collection service that is trusted by all members of the supply chain, then blockchain can be a good solution by which each member can supply relevant ledger or smart contract data and determine which recipients are authorized to access the raw data.

An additional benefit is that long-term data retention is much more robust since all members of the network have a complete copy of all blockchain data. Therefore, if a member drops out of the consortium, the other members can continue without disruption. Furthermore, if there are strict audit requirements by independent audit agents, then implementing a blockchain with the audit agent as a member can be a powerful method to enable real-time monitoring and auditing of the supply chain.

Blockchain and Security

Although applications such as ledger records and smart contracts are potentially powerful improvements for supply chains, it is important to clearly define in advance the specific business objectives and use cases to be addressed. In fact, viable traditional alternatives, which are less complex and costly, should be considered before choosing blockchain.

For example:

- For the *ledger recording applications*, there are numerous methods for storing transactional data, including a centralized database management by a trusted third party or as a database owned by the manufacturer.

- For *smart contracts and commercialization control*, alternatives such as ERP/PLM and accounting systems may be appropriate. Large manufacturers and enterprise customers often have large investments in these systems and would need significant motivation to move to a blockchain system. Potentially, supply chains that contain shared IP would benefit from a shared authorization of commercial transactions to assure each owner's individual IP is managed properly, otherwise the benefits blockchain brings to commercialization and accounting are incremental at best.

Security Assessment

Security, defined as a combination of *confidentiality, authenticity* and *integrity* of data can also be achieved using standard methodologies.

- ***Confidentiality*** can be understood as simply protecting data from being accessed by unauthorized parties. In traditional systems, access control, along with data encryption, protect the privacy of data. Attacks to such access controls and cryptographic systems are well understood and robust defenses are available. However, with blockchain, access control is much more difficult due to the fact that each node in the blockchain network has access to the full dataset. Therefore, the same level of data protection must be implemented at each node. A single member with poor cybersecurity protections may leak confidential data. Even though technological options for data encryption within a blockchain network are emerging, cryptographic key distribution and protection at each node is extremely complex. Complexity in cryptographic systems always leads to vulnerabilities.
  Blockchain rating for confidentiality: D

- ***Authenticity*** certifies that the data accurately characterizes what it purports to represent. Blockchain does provide a robust, shared record of data and this aspect should not be confused with authenticity. Although blockchain provides an immutable record of all transactions accepted, there is no guarantee that the data generated outside of the blockchain is authentic. With ledger recording applications, for the data to be meaningful, it should represent genuine transactions, operations and processes actually taking place within the supply-chain workflow. Blockchain only verifies that the stored data conforms to a predefined rule agreed to by the participants. So, there is a gap between the blockchain input and where/how the data actually originated, allowing for modification and forgery.
  For example, let's consider a major spare parts supplier that relies on an external manufacturer. If there is no method to verify the parts scrapped by the manufacturer, the manufacturer can deflate its report of parts produced and then sell the remaining "scrapped" parts to counterfeit suppliers. Until this final gap is secured, both blockchain (through an oracle as described above) and traditional technologies will fall short of providing a complete secure record of all events occurring within the workflow of a supply chain.
  Blockchain rating for authenticity: C

- ***Integrity*** refers to the assurance that data has not changed since the data was stored within a system. This is built into all major enterprise-grade centralized database solutions. Although these systems may be vulnerable to cybersecurity attacks, data integrity failure is otherwise extremely rare. On the blockchain side, data integrity is perhaps its strongest attribute. A hash-linked chain of data blocks provides a very strong defense against data modification. However, blockchain still has the same type of cybersecurity vulnerabilities as centralized solutions. For instance, an attack on a single node can modify the node's local blockchain data without knowledge of that node's owner. Attacks on a majority of nodes can lead to catastrophic data integrity failure for the entire blockchain.
  Blockchain rating for integrity: A

Conclusion

As the effects of digital transformation permeate all functions of an enterprise, the modern manufacturing function is driven by digital data that must be secured. The transition from the classic engineer–manufacture–distribute model to the Industry 4.0 model of engineer–distribute–manufacture means that manufacturing and IT teams are looking to address critical needs of digital IP information flowing across engineering, distribution, manufacturing, and logistics/tracking.

To fully justify the cost and complexity of implementing a blockchain solution to address those needs, the benefits must be analyzed in the context of existing technologies.

> *"Organizations remain cautious about early adoption and not rush into making blockchain work in their supply chain until there is a clear distinction between hype and the core capability of blockchain."* Gartner

Implementing blockchain on the premise that it will make all data secure is not only fundamentally misleading, but it may be a recipe for disaster, given the cost and the gap that would still exist in securing the full data flow of such an application.

From a security point of view, to determine whether your application is a good match for blockchain technology within a supply chain, consider how to address the following three fundamental questions:

1. **Do all members of the consortium want to freely share data?**

   If data confidentiality is a concern, then you should consider additional technologies to complement the standard blockchain solution. These can be privacy solutions built into Hyperledger Fabric/Sawtooth, or industry-specific solutions that sit on top of the blockchain to provide data encryption and access controls.

2. **What is the authenticity plan to extend the data represented by the blockchain? I.e. how do you authenticate the data that you either bring into or link to a blockchain?**

   A thorough understanding of the risks associated with unverified data is needed in order to determine what data, moving into or out of the blockchain, needs to be authenticated. Once the requirements are understood, then a robust oracle solution can be chosen that provides the desired level of authentication. For instance, if a manufacturing policy required to produce a part is stored on the blockchain, then the oracle must enforce the policy during the manufacturing process to ensure the quality standards are met.

3. **Is there a third-party audit or certification party that requires access to important data within a supply chain?**

   There are two important considerations to assess in order to enable auditing capabilities. The first is to determine the exact data that is required by the auditor and then ensure there is a robust oracle solution that extends the reach of the blockchain to protect the integrity of this data at its source. The second consideration is to ensure that only the auditing participant has access to data that must be kept confidential from other members. In order to do so, traceability

and authentication mechanisms targeting specific data throughout the digital supply chain need to be in place.

How Identify3D complements and extends blockchain

Either as a blockchain extension or standalone, the Identify3D technology suite helps protect confidentiality and integrity of data in digital manufacturing by providing intellectual property protection, manufacturing repeatability, and traceability — from initial design to finished product. By enabling manufacturing and IT to converge on a proven solution that provides tight control of the digital supply chain, the true potential of distributed manufacturing can be realized.

To learn more, or to schedule a demo and understand how Identify3D can enable you to realize the advantages of digital manufacturing, contact us today at info@identify3d.com.