# Software Engineering Institute

**Blogs**

## Could Blockchain Improve the Cybersecurity of Supply Chains?

**NOVEMBER 4, 2019 • SEI BLOG**

*By Eliezer Kanal (/author/eliezer-kanal)*

Best Practices in Network Security (https://insights.sei.cmu.edu/sei_blog/best-practices-in-network-security/)

cybersecurity (https://insights.sei.cmu.edu/sei_blog/cybersecurity/)

A September 2018 report to the President, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States (https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SuPPLY-CHAIN-RESILIENCY.PDF) , raised concerns about cybersecurity in light of the reliance on complex supply chains in defense applications.

> *Gaps in the cybersecurity sector lead to pervasive and persistent vulnerabilities to the industrial base, [...] unauthorized access to any facet of manufacturing information could create rippling effects and cause innumerable negative economic and national security situations.*
>
> *[...]*
>
> *Cybersecurity risks impact all facets of manufacturing supply chain operations, from product and process data flowing within and across factories, to supply chain operations and logistics, to the reliability of tools and equipment used within manufacturing enterprises. Multiple approaches exist to manage cybersecurity risks within the industrial base, but not all approaches are appropriate or even adequate to meet the national security need to protect covered defense information and controlled unclassified information. Three key issues--lack of uniform security implementation; inconsistent implementation of adequate security by defense suppliers; and reliance on self-attestation--expose manufacturing to cybersecurity risks.*
>
> *(p. 88)*

Blockchain (https://insights.sei.cmu.edu/sei_blog/2017/07/what-is-bitcoin-what-is-blockchain.html) is an emerging technology that, in theory, could reduce the cybersecurity risks intrinsic to supply chains: it creates an auditable, immutable, unchangeable history of transactions that can be tied to a verifiable identity. In this blog post, I discuss both the promise and the challenges of applying blockchain to improve the cybersecurity of supply chains.

At its most basic, a blockchain (https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/) is simply a distributed ledger that tracks transactions among parties. What makes it appealing for a wide variety of applications are its fundamental properties, which apply to every transaction:

- All parties agree that the transaction occurred.
- All parties agree on the identities of the individuals participating in the transaction.
- All parties agree on the time of the transaction.
- The details of the transaction are easy to review and not subject to dispute.
- Evidence of the transaction persists, unchangeable, over time.

This combination of properties results in a system that, by design, timestamps and records all transactions in a secure and permanent manner, and is easily auditable in the future. In addition, due to its distributed nature, the system is highly resilient to downtime. These properties explain much of the interest in the technology.

Because blockchains are still not being used much in practice, we are just beginning to underst they could do. People are attempting to use blockchain technology for many different purpose platforms, customizing it for specific use cases and discovering where it does and does not wor

- technologies for sending money, including Bitcoin (https://bitcoin.org/en/) , Ripple (https://www.rippl and many others (https://www.cointracker.io/)
- platforms for legal contracts such as Quorum (https://www.goquorum.com/)

- platforms for the development of standard business appllications, such as Ethereum (https://www.ethereum.org/) and Hyperledger (https://www.hyperledger.org/)
- applications built for storing health records (https://www.medpagetoday.com/practicemanagement/informationtechnology/74695)
- applications for supply chain management such as Everledger (https://www.everledger.io/)

**The Promise of Blockchain for Supply Chains**

A recent article in Information Age (https://www.information-age.com/blockchain-in-supply-chain-management-123484861/) identified lack of end-to-end visibility as one of the key challenges of supply chains:

> *With numerous moving parts and different partners and suppliers involved, supply chains get out of hand easily. For the vast majority of enterprises, interactions in their supply chains are going unmonitored and the silos between the different stops along the fulfillment process* [are] *directly causing business inefficiency.*

Blockchain creates an auditable, immutable, unchangeable history of transactions. Every transaction is tied to a verifiable identity. Combining the property of identity-based transactions with an immutable log of history creates a system that, theoretically, provides unprecedented levels of transparency and assurance regarding supply-chain risk management.

This characteristic of blockchain is well suited to supply chains and security settings. Every time anyone adds anything onto a supply chain, it is important to know with certainty where it came from. The ability to tie every entry to a specific identity represents the promise of blockchain for supply chains. Automating the establishment of trust among parties and the management of risk in supply-chain interactions also has the potential to reduce costs.

**Cybersecurity Supply-Chain Risk**

The risk posed to a software supply chain is slightly different from that typically present in those associated with physical goods. Given the relative ease by which software can be modified, risk mitigation tends to focus on two aspects: (1) minimizing opportunities for unauthorized changes, and (2) measuring the extent to which such opportunities are, indeed, present. Moreover, modern software makes extensive use of both open-source and proprietary libraries to extend functionality. While these tools can significantly increase functionality and decrease development time, they present a risk in that the provenance of the libraries is often not guaranteed, particularly at multiple levels down the supply chain. The Software Engineering Institute has an extensive library of techniques (https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485408) for managing software risk and maximizing software assurance and has developed a suite of tools to help achieve these ends, including the CERT Resilience-Management Model (CERT-RMM) (https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=514489), the External Dependencies Management (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-EDM.pdf) (EDA) methodology, and the Security Engineering Risk Analysis (https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=427321) (SERA) framework.

Blockchain could complement these techniques and others by helping provide a more secure provenance for all elements of the software supply chain. Software has the benefit of being easy to digitally tag using modern cryptographic techniques (https://en.wikipedia.org/wiki/Digital_signature), which can provide a digital signature for any code. Indeed, many modern software-development tools--including most of the most popular code-management tools--regularly create such digital signatures to keep track of versions of software. Even more so, these signatures are designed to identify real-world identities easily. Using the blockchain to help distribute these digitally signed pieces of code could significantly reduce many aspects of modern software supply-chain risk.

**Limitations and Caveats**

Despite the theoretical compatibility of blockchain's features with the very challenges that confound the management of supply chains, adoption of blockchain solutions to date has been slow. There are significant hurdles that must be overcome before blockchain solutions for supply chains can be said to have entered the mainstream.

Factors the currently limit the widespread adoption of blockchain include the following:

**No Compelling Market Demand or Success Stories**

In no way can the market be said to be demanding blockchain solutions. According to a 2019 Deloitte report on enterprise blockchain adoption (https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html), 53% of the 1386 interviewed executives stated that blockchain had become a critical priority, but only 23 per cent have actually begun using it. "Though a majority of respondents call blockchain a top-five priority," the report states, "only 23 percent have already initiated a blockchain deployment--down from 34 percent. Attitudes about blockchain r
percent still see blockchain as overhyped, up from 39 percent last year."

One of biggest warning signs about blockchain is that there are no successful examples of bloc
for supply chains that we can study and analyze. Some companies use blockchain and have ma
chains, but usage alone is not evidence of success. There is a noticeable dearth of public assert
documented cybersecurity improvements that might motivate others to adopt the technology.

the use of blockchain technology by the U.S. Department of Health and Human Services (https://fcw.com/blogs/lectern/2017/10/comment-kelman-gsa-blockchain.aspx) for IT products and services in the General Service Administration (https://www.gsa.gov/) have to date not provided persuasive evidence that the use of blockchain in this case represented any kind of a significant or essential improvement over more conventional solutions that were available.

Alternatively, well-understood solutions to full-scale supply-chain management do exist. While not doing so perfectly, today's modern computing infrastructure already handles supply chains after a fashion. There are many solutions, such as the creation of large-scale databases, and many of them appear on the surface to have the problems associated with management of supply chains solved. To that extent, while blockchain technology appears promising, many are concerned that blockchain is still a solution in search of a problem.

**Untested Nature of Blockchain Technology**

Current blockchain technology is still relatively young. There are some issues we are aware of, such as that it doesn't scale very well, and that it is hard to work around policy issues. Collaboration on a blockchain allows anyone who participates to add anything they want to add to the chain; because a blockchain is immutable, anything that anyone adds will be there forever, even if it is later redacted. This feature alone could represent a legal nightmare: the legal aspects of blockchain are untested. For example, GDPRs (General Data Protection Regulations) (https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection), widely used in Europe for data privacy, have a legislative requirement called the right to be forgotten (https://gdpr-info.eu/issues/right-to-be-forgotten/). This right is clearly at odds with the very nature of blockchain. The fact that blockchain is legally untested may diminish the appetite for companies to adopt it.

**Scale of the Required Transition, Adoption Challenges, and Management of Change**

Technology adoption or transition is hard (https://insights.sei.cmu.edu/sei_blog/2017/11/five-models-of-technology-transition-to-bridge-the-gap-between-digital-natives-and-digital-immigrant.html). The size of an undertaking to manage supply chains by means of blockchain technology is huge and would require adding a large amount of information to a blockchain, with buy-in and adoption required of all participants, who would need to commit to using this new technology. Questions about the general scalability of blockchain--how well it could work to integrate multiple organizations and data sets--also remain unresolved.

The difficulty of managing such large-scale change is exacerbated by the lack of an off-the-shelf, complete, packaged solution--a whole product (https://en.wikipedia.org/wiki/Whole_product), in the parlance of author Geoffrey Moore (https://en.wikipedia.org/wiki/Geoffrey_Moore), who popularized the term. Blockchains currently available for adoption are only complex hybrids of conventional blockchain technologies that would not be easy for organizations to transition to from their current states.

Costs associated with the technology itself for things such as electricity usage and network connectivity are not nearly as prohibitive as the sheer managerial overheard of adopting an entirely new technology. This challenge is particularly true in the case of blockchain, where the technology is immature, standards do not exist, and there is widespread misunderstanding of how blockchain could, or should, actually help to secure the supply chain.

**What Is the SEI Doing With Blockchain?**

Despite all the aforementioned risks, blockchain research remains active and vibrant. As with many young technologies, researchers are not nearly as concerned as practitioners about the lack of immediate applications. Some of the recent innovations show promise in solving known problems, as well as in opening up new areas of research. One such area includes the interledger protocol (ILP) (https://interledger.org/rfcs/0003-interledger-protocol/), a protocol to enable communication between different blockchain technologies. Other areas include enabling robust offline data storage, enabling the removal of malicious or illegal information from a blockchain, and software architecture design patterns for blockchain-based applications.

At the SEI, we have also been investigating the use of blockchain technology within the DoD. Our current focus has been on ensuring that the blockchain application-development process doesn't expose applications and users to unnecessary risk. Unfortunately, as with any new technology, early adopters have helped expose a number of significant design flaws with existing blockchain implementations. Our team has partnered with Carnegie Mellon University (CMU) to develop a secure-by-design (https://en.wikipedia.org/wiki/Secure_by_design) language that can be used for blockchain application development. By creating a language that specifically makes certain types of bugs impossible to create, we aim to significantly reduce the risk inherent in the adoption of blockchain technology. By contributing to the maturation of blockchain technology, we hope that our work can help blockchain to achieve its promise for securing supply chains that are critical to our infrastructure and national defense.

**Additional Resources**

Read the SEI blog post, What Is Bitcoin? What Is Blockchain? (https://insights.sei.cmu.edu/sei_blog/2017/blockchain.html) by Eliezer Kanal.

Read other blog posts by Eliezer Kanal (http://insights.sei.cmu.edu/author/eliezer-kanal/).