The Potential Use of Blockchain Technology to Address Supply Chain Cyber Risks

Daniel C. Durham

University of Virginia

The Potential Use of Blockchain Technology to Address Supply Chain Cyber Risks

With as many as 80% of data breaches believed to have originated in the supply chain, the current concept of technology can no longer be relied upon to manage the vulnerabilities posed by suppliers in a fragmented and geographically diverse procurement system (Min, 2019; Shackleford, 2015). Further, increasingly sophisticated methods of perpetrating cybercrimes through the use of viruses, worms, and hackers, as well as an escalation of state-sponsored cyber-attacks have made the inherent challenges associated with preventing, detecting, and responding to data breaches all the more difficult (Swathy, 2018). As such, there is a critical need to establish more secure data storage processes for supply chain operations by considering the use of emerging technologies such as Blockchain. However, despite the potential for Blockchain technology to create greater efficiency for federal procurement activities, at this time existing Federal guidelines should continue to be used to manage cyber risks to supply chain operations.

Supply Chain Cyber Vulnerability

A report by the General Accounting Office (2018) has identified that the potential introduction of cyber threats into government information systems through the global supply chain process presents an unacceptable risk to federal agencies. While the adverse consequences associated with security lapses related to information systems is more commonly considered to be the compromise of personal information through the theft or hacking of electronic records, risks can also include allowing adversaries to take control of crucial government systems. A recent example of how the malicious infiltration of operating control systems can be spawned through weaknesses in the supply chain process involved the Russian government using trusted third-party suppliers to target network systems of the federal government as well as organizations in the energy, nuclear, water, and aviation sectors (U.S. Computer Emergency Readiness Team, 2018).

Need to Address Cyber Risks in Supply Chain Operations

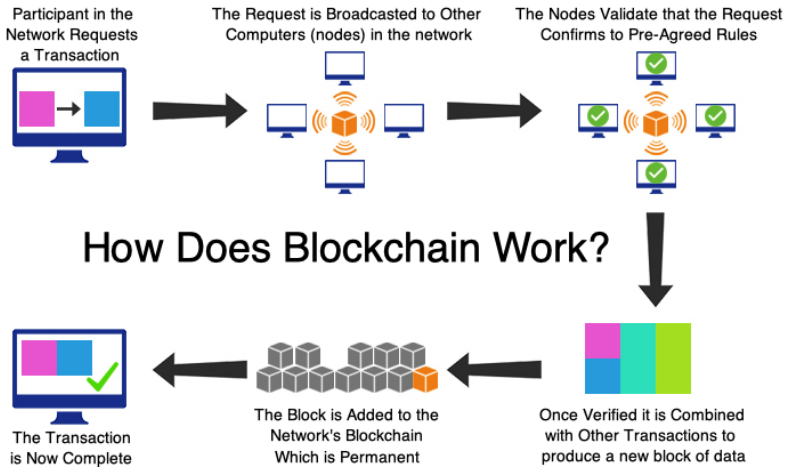
The National Counterintelligence and Security Center (2017) recently identified the need to secure supply chains from cyber-attack as one of the top priorities for maintaining the integrity of products used by the federal government. This consideration for cyber risks underscores the need for the development, implementation, and monitoring of supply chain activities to ensure the security and resilience of information systems (NIST, 2018). Nevertheless, the General Accounting Office (2018) identified that in 2012 four national security agencies had not fully developed or documented policies and procedures designed to address supply chain risks. While these agencies had taken actions to address supply chain protection measures by 2016, as of 2018 one of the agencies in question could not adequately demonstrate the manner that monitoring was conducted to assess the effectiveness of supply chain security measures (GAO, 2018). Notwithstanding the efforts of some agencies, the relative slowness and apparent difficulty in implementing standard commercial practices indicate the crucial need for innovative strategies and solutions for managing cyber risks in the supply chain system.

Leveraging Emerging Cybersecurity Technologies

Given the increasing digital connectivity and automation of business processes, it is imperative that next-generation technologies be considered for detecting a new generation of malware and cyber-attacks that are difficult to detect with present-day conventional tools. For this reason, the Food and Drug Administration (FDA) has initiated a five-year pilot program that incorporates the use of emerging Blockchain technologies to provide enhanced security for prescription tracking systems (Newman, 2019). However, while it is important to remain abreast of the latest technological developments, it is equally as important to combine the use of emerging technologies with fundamental cybersecurity controls (Rohmeyer & Bayuk, 2018).

The Use of Blockchain Technology for Supply Chain Operations

In little more than a decade since Blockchain technology was first introduced, it has shown the potential to transform the manner that data transactions and storage occur by providing a secure, distributed, and inexpensive database system that reduces the vulnerabilities of a cyber threat. So much so that in a recent survey of more than 3,200 C-Suit executives across North America and Asia, 68% identified that their organizations already have a defined Blockchain strategy to manage mass collaboration efforts and secure network data (Das, 2017).



In traditional networks, a central server is used to store all the data and is highly vulnerable to security attacks. In a Blockchain, data is distributed using cryptography and stored on a series of connected computers, rather than on a single central network server. Therefore, if one computer on the network is corrupted or attacked, other computers in the chain are used to maintain data integrity.

Figure 1. How does blockchain work (Lisk Academy, 2019).

Benefits of Blockchain. By distributing data across a network, Blockchain technology eliminates the risk associated with centralized storage. Existing supply chain operations have transformed into a dynamic global system comprised of multiple manufacturers all attempting to communicate and coordinate work together. Blockchain technology had the potential for allowing the use of computer applications that once only worked through a centralized storage repository to now operate in a decentralized manner. This structure provides Blockchain technology with the capability of being the most secure forms of storing and sharing online information presently available by reducing the dependence on third-parties for data verification (Casado & Prieto, 2018; Min, 2019; Mahoney & Helper, 2017; Underwood, 2016).

Risks Associated with Blockchain. Despite the decentralized structure of Blockchain networks that provide resilience against network-wide attacks, instances of hacking have occurred (Blossey, Eisenhardt & Hahn, 2019). However, identified security weaknesses have not been within the Blockchain, but rather a result of human error or an external vulnerability resulting in service disruptions or the theft of sensitive data (Conoscenti & Vetro, 2016; Lansiti & Lakhani, 2017; Sheldon, 2019). Nevertheless, while data residing in a Blockchain may be considered tamper-proof, the future is uncertain in consideration that the actions of cybercriminals are becoming increasingly sophisticated in their attempts to attack data networks. Further, given that it takes time for any new technology to be incorporated into business operations, it will be many years before the reliability of Blockchain is proven to be resilient from hacking and the technology becomes widely adopted as a component of cybersecurity.

Conclusion

Despite the potential for Blockchain technology to redefine network security, at this time existing Federal security guidelines should continue to be used for managing supply chain operations. While Blockchain technology has significantly challenged conventional thinking and approaches for securing the storage and transmission of network data, there are significant challenges associated with establishing a distributed networked storage system necessary to secure global supply chain operations. Further, Blockchain technology is not immune to hacking and does not fully resolve all cybersecurity issues associated with human failures or the infrastructure used for implementation. Accordingly, broad-scale adoption of innovative technologies such as Blockchain for federal government global supply chain operations should be a gradual process that is undertaken after full-scale testing activities have been initiated and an in-depth study of the benefits, vulnerabilities, and sustainability have been completed.

References

Blossey, G., Eisenhardt, J. and Hahn, G. (2019). *Blockchain Technology in Supply Chain Management*. Proceedings of the 52nd Hawaii International Conference on System Sciences. https://scholarspace.manoa.hawaii.edu/bitstream/10125/60124/0684.pdf

Casado, R. and Prieto, J. (2018). How blockchain improves the supply chain. *Procedia Computer Science*, 134, pp.393-398. https://www.sciencedirect.com/science/article/pii/S187705091831158X

Conoscenti, M., and Vetro, A. (2016). Blockchain for the Internet of Things. *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. https://ieeexplore.ieee.org/abstract/document/7945805

Das, S. (2017). *Blockchain Global Analysis*. Cognizant Research Center, pp.3-19. https://www.cognizant.com/Resources/cognizant-blockchain-global-analysis.pdf

General Accountability Office (2018). *GAO-18-667T: Supply Chain Risks Affecting Federal Agencies*. Washington, DC. https://www.gao.gov/products/GAO-18-667T

Lansiti, M. and Lakhani, K. (2017). The Truth About Blockchain. *Harvard Business Review*. https://enterprisersproject.com/sites/default/files/the_truth_about_blockchain.pdf.

Lisk Academy. (2019). *How Does Blockchain Work? | Lisk Academy*. https://lisk.io/academy/blockchain-basics/how-does-blockchain-work

Mahoney, T. and Helper, S. (2017). *Next-Generation Supply Chains | MForesight: Alliance for Manufacturing Foresight*. http://mforesight.org/projects-events/supply-chains/

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, 62(1), pp.35-45. https://www.sciencedirect.com/science/article/pii/S187705091831158X

National Counterintelligence and Security Center (2017). *Strategic Plan 2018-2022*. Washington, DC. https://www.odni.gov/files/NCSC/documents/Regulations/2018-2022-NCSC-Strategic-Plan.pdf

NIST – National Institute of Standards and Technology (2018). *Cyber Supply Chain Risk Management*. Washington, DC. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf

Newman, P. (2019). *FDA considering blockchain*. Business Insider. https://www.businessinsider.com/fda-considers-blockchain-tracking-prescription-medications-2019-2

Rohmeyer, P. and Bayuk, J. (2018). How Do I Manage This? *Financial Cybersecurity Risk Management*, pp.125-156. https://link.springer.com/chapter/10.1007/978-1-4842-4194-3_6#citeas

Shackleford, D. (2015). *Combatting Cyber Risks in the Supply Chain* (pp. 1-16). SANS Institute. https://www.sans.org/webcasts/combatting-cyber-risks-supply-chain-100657

Sheldon, M. (2019). General Considerations on Private and Permissioned Blockchain Audit. *Issues in Auditing*, pp.1-11. http://www.aaajournals.org/doi/pdf/10.2308/ciia-52356

Swathy Akshaya. (2018). Risk Assessment of Cloud Computing. *Advances in Systems and Computing*, pp.37-59. https://link.springer.com/chapter/10.1007/978-981-13-1882-5_4

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, 59(11), pp.15-17. https://cacm.acm.org/magazines/2016/11/209132-blockchain-beyond-bitcoin/abstract

United States Computer Emergency Readiness Team. (2018). *TA18-074A Alert: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*. Washington, DC. https://www.us-cert.gov/ncas/alerts/TA18-074A