Research memo

Center on Sanctions & Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Leveraging Blockchain Technology to Protect the National Security Industrial Base from Supply Chain Attacks

Michael Hsieh, Ph.D., and Samantha Ravich, Ph.D.

July 11, 2017

Abstract

Cyber-enabled economic warfare is not limited to the use of digital networks for surveillance, theft, and sabotage. An emerging national security challenge related to the globalization of manufacturing supply chains is the phenomenon of attacks in which substandard, counterfeit, or maliciously-modified electronic components are introduced into the hardware on which the national security industrial base (the "NSIB") operates.[1] The focus of this work is not on physical countermeasures against infected electronics, but on harnessing blockchain technology to defeat the adversarial networks responsible for the attacks. The complexity of global economic institutions and processes produces an ocean of transactional data in which supply chain attackers can hide. Through blockchain technology, the structure of this data can be transformed to enable new kinds of forensics that can defeat these attacks at scale. This memo is a short-form discussion of the potential to transform legacy acquisitions systems via blockchain technology, along with an outline of pilot activities to initiate this transformation. The limitations of blockchain technology are also presented to ensure that expectations are properly aligned. A longer article that provides more depth and context for the issues raised herein will be published later.

Supply Chain Attacks as a Mode of Cyber-Enabled Economic Warfare

The increasing globalization of manufacturing supply chains will continue to drive broad-based, productivity-led economic growth around the world well into the 21st century.[2] But it also poses national security challenges

1. We use the more inclusive term National Security Industrial Base ("NSIB"), rather than the more common Defense Industrial Base ("DIB"), to describe not just the R&D, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, but also those items that go towards the broader fielding and sustainment of the entire U.S. fighting force and its support structure. The relevant supply chains under our definition include everything from the space-qualified supply chain and the nuclear forces supply chain to the civil critical infrastructure supply chains associated with vital national industries (e.g., aviation, communications, power, emergency response, healthcare, maritime, surface transportation, and water). "Member ISACs," *National Council of ISACs*, accessed July 5, 2017. (https://www.nationalisacs.org/member-isacs)

2. John Moavenzadeh, Sean Doherty, Ronald Philip, Thierry Geiger, Mark Gottfredson, Gerry Mattios, Bon Tjeenk Willink, Andres Correa, Bernard Hoekman, Selina Jackson, Michael Ferrantino, and Marinos Tsigas, "Enabling Trade: Valuing Growth Opportunities," *World Economic Forum in collaboration with Bain & Company and The World Bank*, 2013. (http://www3.weforum.org/docs/WEF_SCT_EnablingTrade_Report_2013.pdf)

of existential urgency as the technologically-complex electronic hardware that comprises our national security industrial base (NSIB) is increasingly produced or assembled in countries with documented histories of large-scale, technologically-sophisticated economic espionage against the United States.[3] The complexity and scale of the manufacturing supply chains that produce this hardware give our adversaries new options for economic warfare that directly threaten the physical security of a United States that is increasingly dependent on imported hardware of verifiably dangerous provenance.[4]

Economic warfare entails the use of non-kinetic actions against an adversary's vital economic targets to weaken it economically and thereby reduce its political and military power.[5] It implies an intense, coercive disturbance of the target's economy. *Cyber-enabled* economic warfare (CEEW) refers to a hostile strategy involving attack(s) against a nation using cyber technology with the intent to weaken its economy and thereby reduce its political and military power.[6] The focus of the present work is on what we consider to be CEEW waged at a strategic level – that is, attacking the entire NSIB of a nation-state by rendering the hardware on which it operates fundamentally unreliable. There are multiple levels of severity in such attacks. Among the more benign is the substitution of counterfeit components for legitimate ones;[7] ordinary economic incentives are sufficient to encourage unscrupulous suppliers to do this without any direction from a sovereign power. More pernicious are components that are modified with malicious functionality, often carefully obfuscated.[8] In such cases, strategic intent can be read more clearly, although there are at present no reliable data with which to assess the relative dominance of profit-driven counterfeiting versus strategically-motivated infiltration.

3. U.S.-China Economic and Security Review Commission, "2016 Report to Congress of the U.S.-China Economic and Security Review Commission," November 16, 2016. (https://www.uscc.gov/Annual_Reports/2016-annual-report-congress). The Commission summarizes: "Chinese intelligence collection operations against the United States pose a large and increasing threat to U.S. national security. Reports of these operations have increased sharply over the past 15 years. China has targeted a wide range of U.S. national security organizations, including military forces, defense industrial entities, national security decision makers and government organizations, and critical infrastructure entities."

4. Senate Armed Services Committee, Press Release, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," May 21, 2012 (https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts). The Senate Armed Services Committee identified over 100 cases of suspected counterfeit parts in the defense supply chain. China was the "leading source country" for these parts, with 70 percent of the parts traced back to it. In acquisitions processes with "well-defined requirements, risk of unsuccessful contract performance is minimal, and price is a significant factor," the Department of Defense preferentially uses lowest price technically acceptable (LPTA) source selection. In such cases, exporting economies with structural cost advantages such as China's can be expected to have broad and persistent inlets into such supply chains.

5. This is based on the definition of economic warfare from George Shambaugh, "Economic warfare," *Encyclopedia Britannica*, accessed November 3, 2016. (https://www.britannica.com/topic/economic-warfare)

6. Samantha Ravich, "Cyber Enabled Economic Warfare: An Evolving Challenge (Vol. 2)," *The Hudson Institute*, November 2015, page 29. (https://s3.amazonaws.com/media.hudson.org/files/publications/20151117RavichCyberEnabledEconomicWarfareAnEvolvingChallengeVol2.pdf)

7. Discarded integrated circuits are commonly "blacktopped," by which original markings are sanded or otherwise moved, and new, fraudulent markings are added. At present, the detection of such components is generally labor- and capital-intensive – counterfeits are commonly detected by expert visual assessment, tactile inspection, or advanced microscopy. The Components Technology Institute Inc., as part of their Counterfeit Components Avoidance program, documents known and suspected examples of counterfeit integrated circuits, and the identification procedures commonly required for their identification. "Counterfeit Examples: Electronic Components," *Components Technology Institute Inc.*, accessed July 5, 2017. (http://www.cti-us.com/pdf/CCAP-101InspectExamplesA6.pdf)

8. Sergei Skorobogatov and Christopher Woods, "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip (Draft)," March 5, 2012. (https://www.scribd.com/document/95282643/Backdoors-Embedded-in-DoD-Microchips-From-China)

The cost of inaction is great. While we laud the recent focus on supply chain security problems of the defense industrial base (DIB),[9] we endorse a broader notion of the range of U.S. interests threatened by this phenomenon. Infected components are also potentially entering our national civil infrastructure *en masse* as well because civil enterprises share the same supply chain risks. In a conflict scenario, the collapse of the domestic economy would not only degrade national morale but disrupt the primary source of material support for U.S. forces.

The scope of potential penetration is difficult to bound with precision, but estimates published by the Semiconductor Industry Association in 2013 estimate that "as many as 15 percent of all spare and replacement parts purchased by the Pentagon are counterfeit."[10] At the hardware level, there are existing efforts to create better countermeasures against counterfeit components which have opaque chains of custody.[11] While these hardware-level solutions deal with bad components, there is a paucity of enterprise-level defenses to deal with bad actors in the supply chain. A 2017 Defense Science Board report describes the kind of gaps in our acquisitions system in which they so easily hide:

> In typically long DoD acquisition processes, approximately 70 percent of electronics in a weapons system are obsolete or no longer in production prior to system fielding. The Department's mechanisms for tracking inventory obsolescence and vulnerabilities in microelectronic parts are inadequate. Microelectronics components are likely to become obsolete repeatedly during the weapons system lifecycle. Efforts to track component obsolescence lack oversight at a Department-wide level. Reporting of counterfeit and "suspect-counterfeit" microelectronics is mandatory for some, but not all prime contracts and subcontracts. Such reporting requirements are inconsistent and no DoD system at present collects event information on cyber-physical attacks of electronic components as its primary function. To address these concerns, a shared vulnerability database and a parts application database of installed hardware could promulgate corrective actions across weapons systems.[12]

Apart from the economic damage done to victims of intellectual property theft in the case of counterfeits and recycled parts,[13] there is the wide-scale infection of our national infrastructure and defense arsenal with substandard

9. Senate Armed Services Committee, Press Release, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," May 21, 2012 (https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts). According to a 2012 Senate Armed Services Committee investigation, the U.S. Air Force indicates that just *one* single company (Hong Dark Electronic Trade of Shenzhen, China) supplied about 84,000 suspect counterfeit parts to the Department of Defense supply chain.

10. "Winning the Battle Against Counterfeit Semiconductor Products: A Report of the SIA Anti-Counterfeiting Task Force," *Semiconductor Industry Association*, August 2013. (https://www.semiconductors.org/clientuploads/Anti-Counterfeiting/SIA%20Anti-Counterfeiting%20Whitepaper.pdf)

11. As one example of existing efforts, the DARPA SHIELD program is focused specifically on hardware-level countermeasures against counterfeiting. Kerry Bernstein, "Supply Chain Hardware Integrity for Electronics Defense (SHIELD)," *Defense Advanced Research Projects Agency*, accessed July 5, 2017. (http://www.darpa.mil/program/supply-chain-hardware-integrity-for-electronics-defense)

12. U.S. Department of Defense, Defense Science Board Task Force, "Cyber Supply Chain," April 2017. (http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF)

13. "Winning the Battle Against Counterfeit Semiconductor Products: A Report of the SIA Anti-Counterfeiting Task Force," *Semiconductor Industry Association*, August 2013. (https://www.semiconductors.org/clientuploads/Anti-Counterfeiting/SIA%20Anti-Counterfeiting%20Whitepaper.pdf). The Semiconductor Industry Association estimates an annual revenue loss of $7.5 billion and the loss of nearly 11,000 U.S. jobs.

parts.[14] The most serious scenarios would entail an adversary that can remotely turn our systems against us during times of conflict.[15] However, even if the malign effects of supply chain infiltration fall short of the most extreme possibilities, the uncertainty alone in defense planning imposes a cost in its own right.

The Blockchain

Before proceeding, we define some commonly used terms in blockchain research and practice. The *blockchain* is a database whose security is assured by the mechanics of distributed consensus. When used generically, the blockchain refers to the general design concept on which such databases are built. The blockchain can also refer specifically to the data structure within a particular protocol. Usually, the generic or specific use of the term will be clear within its context.

The essence of how the blockchain works can be understood through an example. The first widely-adopted implementation of the blockchain is Bitcoin,[16] for which the database is simply a timestamped ledger of payments.[17] In the Bitcoin protocol, Alice transmits a payment to Bob by broadcasting her transaction to a distributed network of Bitcoin *miners* who race each other to check the validity of Alice's request. Specifically, the miners are checking that Alice does indeed have the requisite balance of bitcoin in her account by validating that she did not already spend her bitcoin elsewhere before attempting to pay Bob. The race between miners is transparently structured: The winner is the first to solve a mathematical problem that by its design requires a high volume of brute computational work.[18] The winning miner is compensated for his work with a fixed award of bitcoin added to his account.

14. U.S. Department of Defense, Defense Science Board Task Force, "High Performance Microchip Supply," February 2005. (http://www.acq.osd.mil/dsb/reports/2000s/ADA435563.pdf); U.S. Department of Commerce, Bureau of Industry and Security, "Defense Industrial Base Assessment: Counterfeit Electronics," January 2010. (https://www.bis.doc.gov/index.php/forms-documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file); U.S. Department of Defense, Defense Science Board Task Force, "Cyber Supply Chain," April 2017. (http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF). The Defense Science Board Task Force's report on the cyber supply chain states: "Exploitation via malicious insertion has … been confirmed in the commercial sector. Prominent recent examples include Volkswagen's insertion of a 'defeat device' to thwart emissions testing and insertion of embedded code into Juniper routers. Recently, FTDI, a semiconductor device company, used a Windows driver update to completely disable computers using functional clones of some component chips, demonstrating the full cycle of component insertion, subsequent activation, and effect."

15. The long tail of supply chains is exemplified by acquisitions such as the purchase of an Israeli company, Servotronix, by the Chinese Midea group. Yuval Azulai and Tali Tsipori, "China's Midea buys Israeli co Servotronix," *Globes* (Israel), February 12, 2017. (http://www.globes.co.il/en/article-chinas-midea-buys-israeli-co-servotronix-1001176475). Midea is the world's largest appliance company. Servotronix supplies devices such as meteorology systems to businesses such as AMSEC, LLC, which "provides a full spectrum of technical and professional services to the military and commercial maritime industry." AMSEC is part of Technical Solutions, a Division of Huntington Ingalls Industries. AMSEC LLC, accessed July 5, 2017. (http://www.amsec.com/). Midea also bought a 95-percent interest in German robot manufacturer KUKA. While the end products are still being sold to the U.S. military, KUKA had to sell its U.S. aerospace division, KUKA Systems Aerospace North America, to U.S. automation company Advanced Integration Technology Inc. prior to being acquired by Midea. Michael Alba, "KUKA Sells U.S. Division to Simplify Regulatory Approval of Chinese Takeover," *Engineering.com*, December 20, 2016. (http://www.engineering.com/AdvancedManufacturing/ArticleID/13967/KUKA-Sells-US-Division-to-Simplify-Regulatory-Approval-of-Chinese-Takeover.aspx)

16. In standard parlance, *Bitcoin* refers to the protocol, while *bitcoin* refers to denominations of currency within the protocol.

17. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin*, 2008. (https://bitcoin.org/bitcoin.pdf)

18. More precisely, the miner sends a combination of (a) the current block data and (b) a nonce into a SHA-256 hash. The transaction information in the block data is fixed, whereas the nonce value is a free variable. He increments the nonce until he finds the value that produces a certain number of leading zeroes in the hash digest. The zeroes themselves are of no particular significance; the purpose of this in the protocol design was to contrive a computational challenge that requires a large amount of CPU cycles, and whose successful solution can be easily and quickly checked.

Alice's transaction is validated by the miners along with a batch of other transactions submitted during a common interval of time; these transactions comprise a block. The blocks are "chained" together in the sense that every block contains a digest of the contents of the previous block.[19] This chaining of information in the state of one block with the state in the next block is central to the security model of the blockchain. If Alice seeks to attempt to cheat the network by modifying the state of a past block (e.g., by erasing a payment she made to Bob, or forging a payment from Bob made to her), she would need to solve a new puzzle[20] not only for that block, but every subsequent block because by design, the solution of the puzzle corresponding to any given block depends on the state of that block; her modification of the state of any past block would ripple through the states of all subsequent blocks and correspondingly create a new sequence of hard puzzles for her to solve.[21] It becomes rapidly more difficult over time for Alice to successfully modify any past transaction fast enough because the likelihood of her solving the necessary sequence of puzzles spawned by her dishonest transaction and shoehorning it into the blockchain decreases exponentially in the number of blocks subsequent to the one containing her dishonest transaction.[22] While the foregoing discussion focuses on the particulars of the Bitcoin protocol, the design principles described illustrate in a general manner the relationships between the data structure, security model, and consensus mechanism that typify most blockchain-based protocols presently in existence.

The "altcoin" development community seized upon the generality of the blockchain concept quickly. The open-source release of Bitcoin in 2009 was followed in 2015 with the release of Ethereum, which enabled the blockchain-based virtualization of Turing-complete machines, encompassing a general class of computational processes, of which a payments ledger like Bitcoin is only a special case.[23] The commonly-adopted term that describes this class is "smart contracts" – which describe a new model of constructing business contracts in which the definition, fulfillment, and validation of contingencies occur as the execution of code on a blockchain rather than as duties of a trusted third party. The prospect of projecting complex business processes onto code, and eliminating expensive middlemen, has already catalyzed over $1 billion in venture investments in blockchain technologies as of 2016.[24] This transformative potential of the blockchain may also revolutionize how we approach supply chain security for the NSIB.

19. The digest is a cryptographic hash of the previous block's contents.

20. The puzzle to be solved by Alice is the same as the miners', which is to increment the nonce appended to the block data until she finds the nonce that produces the correct number of zeroes when the nonce and block data are fed through the SHA-256 hash. However, since Alice has changed one of the transactions in the block, the puzzle changes, and Alice must solve this computationally expensive puzzle anew. She must do this not only for the block with her modified transaction, but for all subsequent blocks as well.

21. The key contents in each block are a set of transactions to be timestamped. After the transactions are bundled into a block, a hash of the block is transmitted to the network; the "chaining" is performed by including the timestamps of the prior block into this hash. More detailed discussion of the security properties of the protocol can be found in Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin*, 2008. (https://bitcoin.org/bitcoin.pdf)

22. The Bitcoin protocol is protected by a voting-type system against attackers who generate a fraudulent chain and nominate it to the network in hopes that it will be accepted. By design, the protocol selects the longest chain validated by the network as the "majority decision" whenever there is a multiplicity of chains under consideration. Effectively, voting power on the network is accorded by CPU power, and any successful attacker must generally muster more CPU power than all the honest miners. The website Blocktrail (https://www.blocktrail.com/BTC) provides a real-time breakdown of the mining pools that contribute the largest percentages of the CPU power on the network. As of May 2017, the hash rate for the entire Bitcoin network has exceeded 5.0 exahashes (10^{18} hashes) per second, the most powerful hashing network ever.

23. Formally, any computational process that is reducible to the operation of a single-tape Turing machine is Turing-complete. As a practical matter, this encompasses most any kind of computation performed on modern computing machinery.

24. Garrick Hileman, "State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin," *CoinDesk*, May 11, 2016. (http://www.coindesk.com/state-of-blockchain-q1-2016/)

Bringing the Blockchain Solution to the NSIB Supply Problem

The essence of the blockchain solution to supply chain security is the unification of all the transactional activities that constitute a supply chain into a single dataspace so that the transactional fog in which adversaries presently hide can be minimized. At present, adversaries can easily hide because the volume, heterogeneity, and sparseness of records associated with supply chain events makes timely investigations impracticably difficult. By projecting supply chain events onto a common dataspace, auditors and investigators will have a homogeneous, detailed, and real-time graph not only of suspicious transactions and relationships, but also a large baseline corpus of "normal" relationships and transactions as well. With such graphs, the full power of anomaly detection methods from machine learning (ML) and artificial intelligence (AI) can be brought to bear on the scale of the problem. This may speed the time-to-detection of infiltrations, and even deter some attempts outright, as the probability of non-detection perceived by would-be attackers is diminished.

As a general example, we consider a contract awarded to a prime contractor for the production of a complex electronic system for the NSIB. The prime contractor will have subcontractors, and subcontractors to subcontractors. Upon approval to start work, the prime and subcontractors will be assigned accounts on a common blockchain through which payments will be effected. Every value-adding activity by the prime or by a sub will be required to be annotated as events on the blockchain – such events could be the fabrication, testing, or delivery of a component. Payment will only be rendered from a prime to a subcontractor, or a subcontractor to another subcontractor, when the value-adding activity is annotated in a timely and accurate manner on the blockchain (this has the effect not only of ensuring accurate recordkeeping, but also encouraging timely payment to subcontractors). In this manner, the transactional provenance for even a single component can be fully mapped out via the payment chains of the tens or hundreds of subcontractors involved in its manufacture. As transactional graphs are constructed for all components that comprise a device, and all devices that comprise systems, a uniform transactional database is constructed for the entire NSIB, resolvable to any level of precision required for an auditor or investigator.

The simplest problem of excluding known bad actors is almost immediately solved with a blockchain-based dynamical graph of transactions. As an example from a services-based supply chain problem, the Special Investigator General of the Afghanistan Reconstruction (SIGAR) found in its audit of the construction of the Parwan Province justice center that a known bomb-making cell had infiltrated the supply chain of contractors and had actually gained two days of access to the construction site.[25] Such explicitly blacklisted entities, even if only tenuously connected with a performer in an active contract, would be flagged in real time with a blockchain-based contracting system. The simplest cases aside, more sophisticated adversaries are likely to use front organizations to mix and tumble their transactions or to generate other kinds of transactional noise to obfuscate their activities. The blockchain also offers a more oblique technological path to defeating this kind of adversary through ML and AI methods. The adversary is now faced with an immeasurably risky problem of (a) faking his behavioral data such that (b) its deviations from the normal baseline of behavior falls within

25. Special Inspector General for Afghanistan Reconstruction John F. Sopko letter to Secretary of Defense Chuck T. Hagel, November 8, 2013. (https://www.sigar.mil/pdf/investigations/SIGAR-Alert-Contractor-Base-Access.pdf). The letter indicates that the Defense Department's Bagram Regional Contracting Center awarded CLC Construction Company (CLC) a contract in June 2011 to build a courthouse at the Parwan Justice Center complex. CLC subcontracted Zurmat Material Testing Laboratory (ZMTL), a subsidiary of the Zurmat Group, to conduct construction safety tests. Specifically, on April 27, 2012, the Department of Commerce added the Zurmat Group and ZMTL to its Entity List because of their involvement in 'networks that provide components used to make improvised explosive devices (IEDs) used against U.S. and coalition troops in Afghanistan.'"

an error bound that may (c) be modulated by auditors and investigators in ways beyond his ability to know. In the long run, we hypothesize that the probability of successfully faking one's behavioral data to evade detection will generally decrease as the data itself will become inherently more difficult to hide in. The difficulty is driven by the additive value of data – over time, there can only be a monotonic increase in (a) the number of validated cases of fraud or infiltration to be added to the collection of ground truth instances and (b) the absolute size of the dataset on which ML- or AI-based detection can learn. Asymptotically, there will be more instances of normal and anomalous behavior with which to improve the precision and latency of detection.

There are significant limitations to a blockchain-based approach to supply chain security, and we do not propose it as a fully comprehensive solution by itself. The fundamental problems not addressed directly by the blockchain are twofold. First, the blockchain solution is optimized toward finding bad transactions rather than bad actors. Second, the blockchain only provides an economical and secure dataspace for measurements; for the analysis on such a dataspace to be useful, there must still be a critical density and volume of high-quality measurements of events in the supply chain. While the blockchain will provide an economical, secure, and uniform dataspace to record such events, the forensics enabled by the blockchain are ideally suited to identifying malice in *enterprise-level* behavioral patterns and relationships. However, an individual bad actor within an enterprise will likely have a variety of ways to evade detection if he has knowledge of gaps in the security procedures in and around his organization, such as the range of realspace events not annotated on the blockchain. Therefore, a blockchain solution will not entirely substitute for sound personnel vetting procedures and personnel activity monitoring. In addition, for even enterprise-level analytics to be effective, the physical spaces and electronic processes which constitute supply chains must be instrumented with a density and distribution of sensors commensurate to the subtlety of the phenomena sought. The development and deployment of such sensors at scale is a nontrivial problem in its own right. We anticipate that any broadly-effective solution to the supply chain security problem will require a combination of approaches of which the blockchain will be one of many parts.

Policy Recommendations

While the NSIB policymaking community wrestles with the potentially existential threats embedded in supply chain threats, the private sector is already embracing the blockchain for its own supply chain security problems.[26] We are in full accord with the policy recommendations of the April 2017 Defense Science Board report; however, implementation of them at scale in a cost-effective manner will require the unique capabilities of the blockchain.

Small-scale experiments can be done, particularly in technology-savvy communities – e.g., cybersecurity specialists and cryptographers. We can develop a novel set of requirements for prime contractors who are able and willing to accept the blockchain-based payment system. To support this, we will need to train a contracting officer and contracting officer technical representatives to define and validate contractual contingencies on such a system. At a more fundamental level, we need to update the privacy requirements for contractor information – existing Defense

26. Multiple efforts that are relevant to the present discussion include applications of the blockchain to protect against counterfeiting on the pharmaceutical supply chain (BlockVerify), track high-value items (EverLedger), and build trust between consumers and producers by introducing transparency in the building process for products (Provenance). Ben Dickson, "Blockchain has the potential to revolutionize the supply chain," *Tech Crunch*, November 24, 2016. (https://techcrunch.com/2016/11/24/blockchain-has-the-potential-to-revolutionize-the-supply-chain/)

Federal Acquisitions Regulations (DFAR) requirements impose standards for protecting contractor information,[27] and the pseudynomous[28] quality of behavioral data embedded on a blockchain raises a host of technical risks[29] that will likely have to be managed at the policy level as well as at the technical level.

Legislative and regulatory action should be taken in partnership with industry. There is a common understanding of the urgency of supply chain security, but the globalization of electronics production will continue to be a necessary phenomenon to sustain the global semiconductor industry's ability to create consumer value, drive economic growth, and innovate into the 21st century.[30] The unique equities of industry and those of the national security community can be harmonized with a combination of technologies and incentives. We may envision a secure acquisitions model in which good faith participation in any new model of supply chain transactional record-keeping can be rewarded with safe harbor indemnifications; but the transparency introduced by the blockchain may also justify a higher duty of care to their ultimate end-users in the NSIB.

Conclusion

Our dependence on foreign supply chains is a reality that policymakers will have to contend with in an increasingly open global economy. The blockchain solution will not by itself provide a complete solution, but it will raise the cost and risk of supply chain attacks. Broadly, blockchain-based solutions are just one of a broad range of tools needed to secure the supply chains for the NSIB, providing tools for enterprise-level forensics to detect malicious activity. A full transformation of NSIB acquisitions processes to accommodate the blockchain may require long-term, whole-of-government and whole-of-industry efforts, but can be experimentally implemented in the short run on small scales. In such experiments, we can begin to develop the data required to address broader questions of the return-on-investment (ROI) of blockchain approaches

27. Defense Federal Acquisitions Regulation, U.S. Department of Defense, §252.204-7000, October 21, 2016. (http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7000). There are broad standing restrictions against contractors releasing any information relating to a contract with specific approvals, specifically from the Contracting Officer (CO). There is an exception for information "already in the public domain before the date of release," which may be interpreted as an opening for the kind of real-time transactional information uploaded to a publicly visible blockchain to be *a priori* exempted from CO pre-approval for release. However, according to regulatory guidance from the General Services Administration, "federal government contractors who operate systems of records containing personal information" are bound in the same way as government entities to the requirements of the Privacy Act of 1974. In general, contractors who operate systems of records containing personally identifiable information (e.g., information pertaining to counterparties up and down the supply chain) are barred, under civil and criminal penalty, from releasing such information about parties in their records without prior written consent from the parties at hand. Further clarification on the possibly conflicting interpretations of the existing regulations for federal acquisitions will be required to ensure compliance for any pilot activity. U.S. General Services Administration, "Privacy and Contact Requirements," accessed July 5, 2017. (https://www.gsa.gov/portal/content/104249)

28. On the Bitcoin protocol, transactions are pseudonymous, rather than anonymous, in the sense that each counterparty is identified by his Bitcoin address rather than his legal name.

29. Yves-Alexandre Montjoye, Laura Radaelli, Vivek Kumar Singh, and Alex "Sandy" Pentland, "Unique in the shopping mall: On the reidentifiability of credit card metadata," *Science*, January 30, 2015. (http://science.sciencemag.org/content/347/6221/536). Even if contractor information were encoded with pseudonyms, hash values, or other privacy-protecting anonymizers, it is well-known that behavioral data, economic and otherwise, has a fingerprint-like quality in being able to uniquely identify individuals. As one of many examples, an MIT study revealed that by examining three months of credit card records for 1.1 million people in a small developed country, there was a 90 percent reidenfication probability for an individual given four randomly selected spatiotemporal points drawn from the individual's corpus of transactions.

30. "Beyond Borders: The Global Semiconductor Value Chain: How an Interconnected Industry Promotes Innovation and Growth," *Semiconductor Industry Association*, May 2016. (https://www.semiconductors.org/clientuploads/Trade%20and%20IP/SIA%20-%20Beyond%20Borders%20Report%20-%20FINAL%20May%206.pdf)

versus approaches based on traditional forensics and analysis. The development of metrics and measurements for such ROI assessments are objectives in their own right in any such experimentation, as the adoption of blockchain technology can be expected to be improvisational and iterative.

Securing the NSIB supply chain is a systems engineering challenge of unprecedented dimensions. Essentially, the problem at hand is to police a corpus of commercial activity which, if only counting the Department of Defense, would comprise the 20th largest economy in the world.[31] While the blockchain, as a new technology, entails extraordinary risks, it also bears extraordinary promise as a tool uniquely suited to such problems of singular scale and complexity.

31. World Development Indicators database, "Gross domestic product 2016," April 17, 2017. (http://databank.worldbank.org/data/download/GDP.pdf)