AU/ACSC/2019

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

THE EMERGING IMPACTS OF BLOCKCHAIN TECHNOLOGY ON DOD ASSET CYBER SECURITY

By

Mr. Daryl Woodfield, DAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Dr. Gregory F. Intoccia and Dr. Richard Smith

Maxwell Air Force Base, Alabama

March 2019

DISCLAIMER

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the U.S. Government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the U.S. Government.

TABLE OF CONTENTS

FIGURES

PREFACE

As a Logistics Management Specialist for the Army and Air Force, I have heard the same question every day, “Where is my stuff and when will it arrive?” One day I was asked that question about several multi-million dollar, nuclear certified, pieces of equipment that were due to arrive in Texas, but found they were halfway around the world at a Republic of Korea Air Force base. Although the Department of Defense (DOD) supply chain has been criticized for its inefficiency and lack of accountability, I did not realize how serious the consequences could be due to these weaknesses. I have seen multiple components arrive damaged, incomplete, and even include sub-par pieces bought on the black market. The DOD supply chain did not catch any of these unacceptable components, which led me to ask, “How easily could an adversary undermine our operations through the DOD supply chain?”

This research project provided me with the opportunity to explore the feasibility of implementing blockchain technology to the DOD supply chain to increase the cybersecurity of DOD assets.

I would like to thank my wife and kids for their support as I worked on this research paper. I would also like to thank my instructor and advisor, Dr. Greg Intoccia, who patiently guided me.

ABSTRACT

This research investigates how the application of blockchain technology into the DOD supply chain could affects the cyber security of DOD assets. The explanatory case study framework is used for this research to analyze existing use-cases of blockchain being implemented into the pharmaceutical industry supply chain to deter counterfeit products, then explore what the implications may be for understanding what the introduction of blockchain technology into the DOD supply chain may mean for the cyber security of DOD assets. Areas of success in the pharmaceutical context were analyzed to determine the feasibility of DOD applying similar approaches within its own supply chain to deter counterfeit parts, resulting in the increased cyber security of assets. However, this paper finds that it is not economically feasible to implement current blockchain technology into the DOD supply chain, primarily due to energy efficiency concerns, data privacy issues, and the lack of standardized blockchain interfaces among all participants. Therefore, blockchain technology cannot currently impact cyber security of DOD assets.

The paper recommends further development of second generation blockchain technology such as Proof of Stake (PoS) within the Ethereum or Hyperledger blockchain networks that address energy issues. The research also recommends development of a governance centered blockchain that will allow DOD to act as a regulator, ensuring all actions within the blockchain are monitored and secured. This will address data privacy issues as DOD will determine who can participate, and standardize all interfaces among participants.

INTRODUCTION

Modern weapons systems have depended on microelectronics since the inception of integrated circuits over fifty years ago.[1] Today, most electronics contain programmable components of ever increasing complexity. Although the electronics industry has continued to implement security measures to protect against counterfeit parts, counterfeit electronics have proliferated through corporations and the military, costing $169 billion annually.[2] Besides creating huge negative economic impacts, counterfeit parts create vulnerabilities for corrupt microelectronic hardware, software, and firmware to gain access to the supply chain of cyber assets which can lead to mission failure in modern weapon systems.

It is difficult to imagine that an organization with the world's largest defense budget[3] could allow this scenario to happen, but counterfeit parts are commonly found within the DOD supply chain. For example, in 2012, the United States Government Accountability Office (GAO) reported the discovery of counterfeit integrated circuits in several platforms: in a U.S. Navy's P-8A Poseidon airplane, in a U.S. Air Force cargo plane, and in parts intended for U.S. Army Special Operations helicopters.[4] GAO went so far to even create a fictitious company to find suspect counterfeit electronic parts available for purchase from companies selling military-grade parts on the Internet. A senate investigation supported the GAO's findings reporting approximately 1,800 instances of suspect counterfeit parts in a two-year period, and that the vast majority of cases appeared to have gone unreported.[5]

Technologies such as RFID (Radio Frequency Identification) and barcodes have been used in the past to address the counterfeiting issue within the DOD supply chain.[6] However, those solutions have not fully resolved the counterfeiting issue due to two issues. First, counterfeiters are able to copy the genuine product's RFID tag or barcode, which meant that a

counterfeit part could be verified by a counterfeit physical tag. Second, once a product had been purchased, product authenticity could no longer be guaranteed since tags are removed at the point of sale, thus second-hand purchases could not be easily verified.[7] Identifying counterfeits is further compounded by poor asset visibility, or the ability to know where an asset is at any given time. This meant that counterfeit parts could enter the DOD supply chain undetected even with physical security measures in place, as the oversight of legitimate parts are lacking. GAO reported in 2016 that an integral part of minimizing the risk of counterfeit parts entering the DOD supply system is the ability to account for and trace electronic parts back to the original manufacturer and lower supply chain levels.[8] However, DOD's inventory management practices and procedures have lacked this ability, to the point that GAO has placed DOD Supply Chain on their bi-annual High-Risk series, which lists the U.S. Federal Government's highest risk areas; thus, requiring Congressional attention.[9]

This situation has left the DOD vulnerable to attacks where non-conforming or counterfeit parts infiltrate the DOD supply chain, introduce malware or exploit latent vulnerabilities in firmware or software, and create undetected cyber-physical threats ultimately disrupting operations and endangering service members. Counterfeit parts are being addressed by emerging physical security technology, such as unique markers and DNA tracking, but without a robust accountability and verification solution, DOD will continue to allow counterfeit parts into the supply chain.

Blockchain technology is being used by multiple industries to address this problem of accountability and counterfeit parts. Blockchain technology was introduced in 2008 by Satoshi Nakamoto to address spending issues of cryptocurrency (digital currency that only exists electronically).[10] Blockchains publicly store data blocks on a shared network in a way that will

ensure every piece of information is accounted for, as well as the origin of said information is verifiable. Each "block" stores a finite set of data and transactions, while the "chain" connects all the blocks in a fixed order. Following the chain from the first to the last block provides a complete, unalterable, transaction history, which can be used to determine accountability of any data: banking, food, and even the digital information within a supply chain.[11] Maintaining a complete, unalterable, transaction history of components within the inventory to ensure valid products is the purpose for which private industry is attempting to use blockchain, but to what extent, if at all, could the introduction of blockchain technology into the DOD supply chain affect the cyber security of DOD assets?

Blockchain technology claims to create a transparent, secure, and tamper-proof data ledger without an intermediary. If applied to the DOD supply chain, this technology would ensure an immutable chain of transactions, accurate tracking of products, and counterfeit and non-conforming parts detection through data verification algorithms. This increased ability to account for, and trace electronic parts back to the original manufacturer, minimizes the risk of counterfeit or malicious parts entering the DOD supply system; thus, improving cyber security of DOD's assets.

Blockchain technology has thrived within the cryptocurrency industry based on its ability to provide a transparent, secure, and tamper-proof data ledger without an intermediary. Transparency is based on a distributed ledger where every action is recorded publicly, allowing anyone to verify correct information. With no central point to be exploited, the system is secure against hacking and fraud. Data that has been recorded on the ledger is securely linked to all past data, creating a tamper-proof history. And the ability to confidently conduct peer-to-peer transactions without an intermediary will lead to a more efficiently run process.

Applying these benefits of blockchain technology to the DOD supply chain would ensure an immutable chain of transactions, accurate tracking of products, and detection of counterfeit and non-conforming parts through data verification algorithms. DOD can learn from industries that are applying blockchain technology to ensure the integrity of the supply chain, particularly the pharmaceutical industry where the immutability and accuracy of drug supply from manufacturer to consumer is vital. The ability to identify the provenance (chronology of ownership from origin) of a product is key to providing accurate tracking across the supply chain. Implementing data verification algorithms from blockchain technology will require each transaction to be validated against a legitimate database key. Maintaining an immutable, accurate, and verifiable transaction history ensures accountability in each parts' life cycle management; thus, ensuring counterfeit and non-conforming parts are unable to unknowingly infiltrate the DOD supply chain. This assurance that DOD assets are legitimate and unaltered, results in improved supply chain accountability and increased cyber security of DOD assets.

The explanatory case study framework will be used to conduct an in-depth look at the application of blockchain technology in the pharmaceutical industry's supply chain, and the impact on their asset security. The case study framework is suitable for this paper as recent research has been performed on blockchain technology's impact on supply chains, and several use-cases have been accomplished. These use-cases provide DOD a realistic pattern how blockchain can be applied to supply chain, specifically to deter counterfeit products. Several industries were identified to have sufficient use-cases; however, the pharmaceutical industry was chosen as a prime candidate for purposes of this study as it holds similar interests to DOD: like DOD, the pharmaceutical industry requires the secure delivery of controlled items with an emphasis on eliminating counterfeit items that present a risk to health and safety.

The first section introduces weaknesses in the DOD supply chain that permit malicious intrusions which can cause cyber-physical harm, the question of how blockchain technology will impact the cyber security of DOD assets, a thesis and argument that blockchain technology will improve cyber security of DOD assets, and a roadmap of the paper.

In the second section, the background of the DOD supply chain, current efforts of DOD to implement blockchain technology, and the background of blockchain technology will be reviewed. This will help the reader understand the current status of these areas, as well as technical aspects of the presented cases.

The third section will introduce three pharmaceutical industry use-cases to explore how blockchain technology is being implemented into existing supply chains. The cases consist of: Modum.io AG's pharmaceutical blockchain software application, Philippine's implementation of blockchain to their pharmaceutical supply chain, and Taiwan's use of Gcoin blockchain software within their pharmaceutical supply chain. These cases will be studied to understand how the introduction of blockchain technology into a pharmaceutical supply chain influences the integrity of the supply chain of related drug transactions.

The fourth section of the paper will apply lessons learned from these pharmaceutical cases to show how blockchain technology could be applied successfully to the DOD supply chain process to ensure the integrity of DOD assets from cradle to grave. Each case will be analyzed for applications that can be implemented into the DOD supply chain process, and issues that may prevent blockchain from being implemented into the DOD supply chain.

The paper concludes within the fifth section, stating that although there are beneficial applications of blockchain technology to the DOD supply chain, multiple issues may prevent it from being currently implemented effectively. The paper recommends two actions that can be

taken to utilize certain aspects of blockchain technology to improve DOD supply chain integrity. The objective of this research is to determine impacts of applying blockchain technology to the DOD supply chain, and if it is a viable option to improve supply chain cyber asset security.

BACKGROUND OF THE DOD SUPPLY CHAIN AND BLOCKCHAIN TECHNOLOGY

Supply chain management and blockchain technology are both complex subjects, and an in-depth explanation of their backgrounds and processes should be discussed. The subsequent section will provide a background and issues of the DOD supply chain, followed by a background and explanation of blockchain. Once these subjects are understood, the reader will better understand the ensuing pharmaceutical case studies, and eventually how blockchain impacts the cyber security of DOD assets.

Despite the implementation of programs and the technology to defer counterfeit parts from entering the supply chain, the number of counterfeit parts found in the DOD supply chain continues to rise. The number of counterfeit parts in electronic military systems more than doubled between 2005 and 2008, rising from 3,868 incidents to 9,356 incidents.[12] DOD's Supply Chain is complex, involving multiple industry sectors and multiple supply chains. Each sector sells to each of the others, and parts may be returned to manufacturers or distributors which subsequently reenter the supply chain, making both pedigree (recorded history), and provenance, difficult to track using current procedures.[13]

GAO supports DOD's concerns of cyber-physical intrusions into the DOD supply chain, stating, "The DOD supply chain is vulnerable to the risk of counterfeit parts, which have the potential to delay missions and ultimately endanger service members."[14] Counterfeit parts in the

aviation industry best exemplify this issue: the US National Transportation Safety Board (NTSB) found unapproved parts were causal factors in numerous accidents and emergency landings with airlines, small private planes, cargo carriers, crop dusters and helicopters.[15] The US Federal Aviation Administration (FAA) went further to estimate that 166 accidents or serious mishaps within a 20 year period were due to counterfeit parts.[16] Counterfeit parts not only pose a serious physical performance issue, but also pose a potential software and firmware issue, requiring DOD to accept a paradigm shift in their cyber supply chain defense strategy. The introduction of blockchain technology could be this shift.

Current DOD Efforts to Introduce Blockchain into Supply Chain

The nation's top leadership took notice of this new technology in the 2018 National Defense Authorization Act (NDAA), which ordered DOD to conduct a comprehensive study of blockchain technology as it may relate to cybersecurity. [17] DOD has since viewed blockchain technology with piqued interest as a potential solution to its supply chain problems.

In 2016, Maj. Neil Barnas wrote the paper "Blockchain in National Defense," to research the possibility of developing blockchain technology for the U.S. Air Force, and leveraging it to increase national defense. In the paper, it was specifically mentioned how the application to supply chain would offer a solution that could establish the provenance of every circuit board, processor, and software component from "cradle to cockpit."[18] Barnas maintained the application of blockchain technology to the DOD supply chain would improve the efficiency and security due to providing provenance. His recommendations influenced the decisions of the U.S. Air Force to develop organic Government blockchain expertise through the U.S. Air Force Institute of Technology (AFIT). [19]

Taking the suggestion of Maj. Barnas, in 2018 AFIT developed a free blockchain-for-supply-chain-management-tool, providing logistical professionals a complementary series of tutorial videos that walk learners through a blockchain simulation.[20] AFIT intends to incorporate these tutorial videos in classroom exercises and business meetings. AFIT partnered with SecureMarking and the University South Dakota Beacom School of Business to develop this supply chain scenario with a blockchain application around it.[21]

The U.S. Air Force Research Laboratory (AFRL) teamed up with blockchain startup SIMBA Chain through a Defense Advanced Research Projects Agency (DARPA) grant in 2017 for $1.8 million. [22] The platform, which was developed by ITAMCO and the University of Notre Dame, has been awarded the government contract to explore how blockchain can enhance supply chain capabilities.[23]

After the original grant in 2017, DARPA has examined multiple blockchain-based systems to include: anti-hacking blockchain strategies, blockchain within communications, and hardware network interactions.[24] DARPA has proceeded with caution in its implementation of blockchain technology due to major issues that have yet to be resolved to ensure proper and efficient implementation.[25] Looking to the pharmaceutical industry provides some of the best insights on possible DOD blockchain applications, and potential solutions to issues that may impact implementation.

Blockchain Technology Background

Satoshi Nakamoto created blockchains to maintain a decentralized, permanent, and public means of recording the creation and distribution of cryptocurrency and developed the first blockchain ledger system for Bitcoin.[26] “Blockchain” has since permeated mainstream

vernacular, going from a technical term only known by cryptocurrency enthusiasts, to a common phrase applied to over 50 industries with a promise of improved performance.[27] A simple analogy with blockchain terminology might best explain the basics:

Basic Blockchain Explanation

Imagine four strangers ("four nodes") sitting in a room, each with their own notebook ("ledger") all with the same information (making this a "distributed ledger"). Because they are strangers, they do not know or trust each other. One stranger gives money to another stranger, and everyone records this transaction in their respective notebooks. All notebooks are compared to ensure they match ("Proof of Work" or 51 percent consensus among all nodes). If all four notebooks match up, everything is fine and the transaction is approved by everybody. If one notebook is different from the other three, it means one stranger is lying about the transaction. We also know which stranger is lying as it will be the one with the notebook that does not match the others. As a result, the transaction is not approved.[28] This process will continue, creating a chain of information that are in blocks; thus, blockchain. See Figure 1.

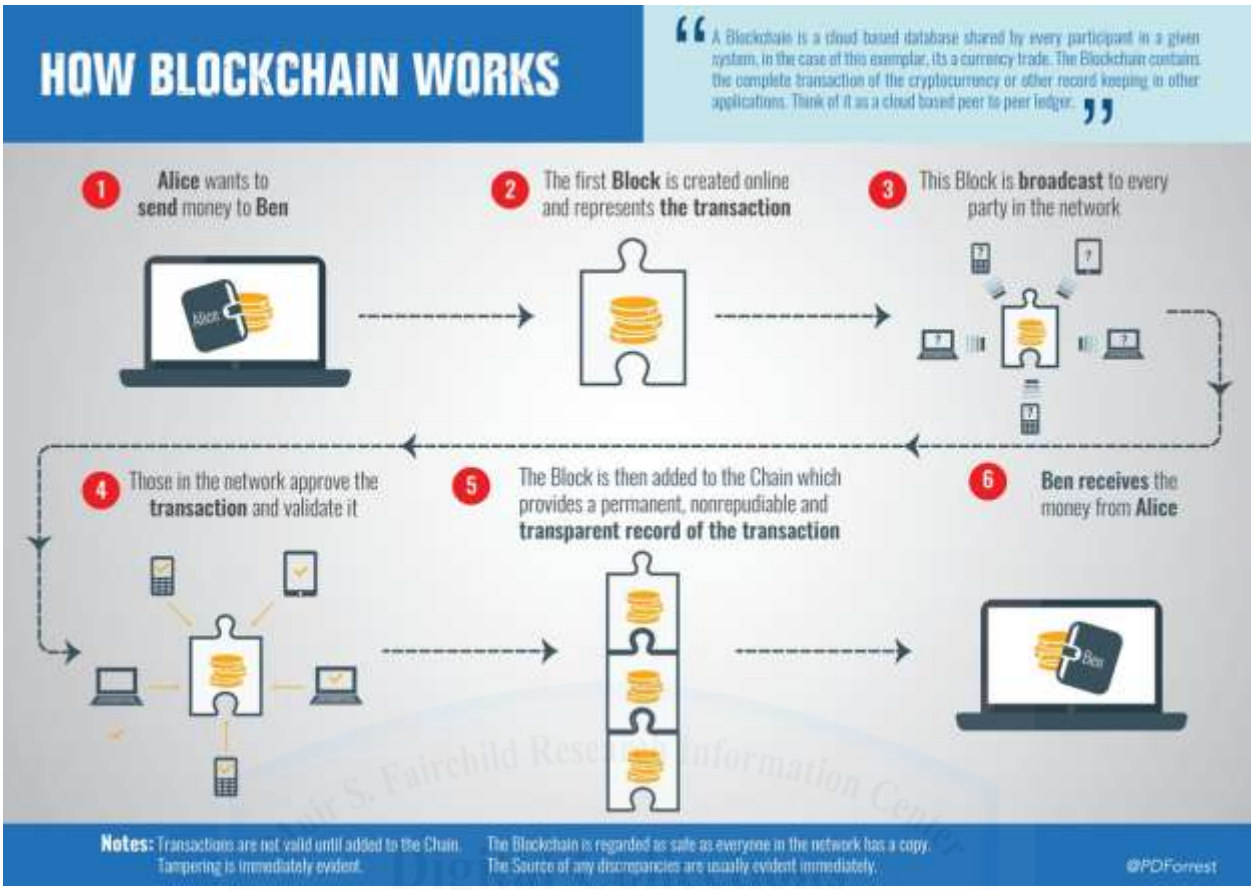

Figure 1: How Blockchain Works[29]

At this point, Proof of Work (PoW) must be explained further. The PoW concept existed even before blockchain, but was propagated by Satoshi Nakamoto in 2008. As stated, PoW is a distributed consensus requiring the majority of nodes to accept the addition of the next block in a blockchain, but there are multiple steps to this process. A block must first be created within the blockchain system and validated as legitimate. This is done by an automated mathematical puzzle being assigned to the block (called a Proof of Work problem) that must be solved by humans called "miners".[30] Miners race to solve the PoW problem, which has been made moderately difficult to solve, with the promise of a reward (usually Bitcoins) for the first to solve

it. After the PoW problem has been solved, it is sent to all nodes to verify it was solved correctly, and once verified by at least 50 percent of nodes the block will be added to the blockchain.

This process takes a large amount of energy required by computing power to solve PoW problems. In 2015 it was stated one Bitcoin transaction required the same amount of electricity as powering 1.57 American households for one day, and will continue to increase as the blockchain grows.[31] To solve this problem, a second generation of blockchain technology was created to validate transactions with energy efficient distributed consensus, called "Proof of Stake" (PoS). The major difference between PoW and PoS, is PoW uses multiple miners competing to solve a PoW problem, whereas PoS chooses one miner (now called a "forger") based on the amount of their wealth to validate the block. To be chosen, forgers essentially bet their funds (stakes), and the highest bid wins. They receive their funds, plus 2-15 percent of the transaction fee, once validated and accepted by at least 50 percent of nodes. [32] These concepts are the foundation of Blockchain technology, and must be addressed prior to implementation into the DOD supply chain. The following example will help the reader further understand the blockchain process, as well as how it relates to DOD supply chain cyber security.

Detailed Blockchain Explanation

For blockchain to become secure, immutable, and tamper proof, a detailed process must take place when creating the blocks. Imagine several blocks that each hold exactly 1 MB of documents (transaction data). See Figure 2.

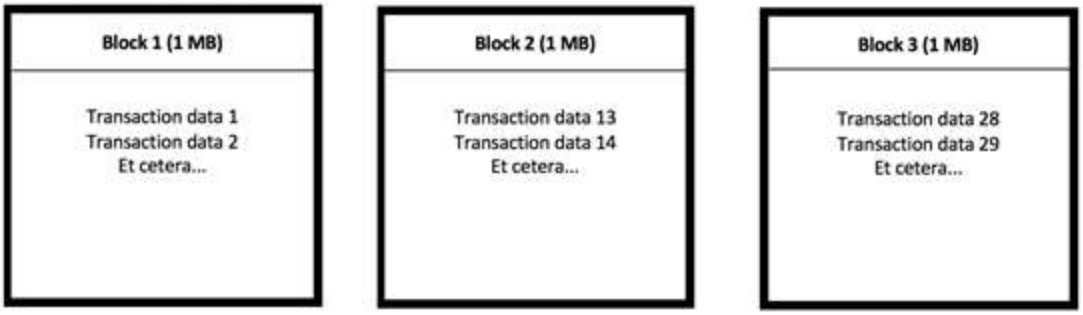

Figure 2: Blocks of Transaction Data[33]

Every block gets a unique digital signature, also known as hashing which will be explained later, that corresponds to exactly the string of transactions in that block. If anything inside a block or document changes, even just a single formatting change, the block will get a new signature.[34] This happens through hashing as described later.

When applying this example to the supply chain, the transaction data would represent all supply data that is recorded as components move through the supply chain: Original Equipment Manufacturer (OEM), certificate of authenticity, standard configurations, location, serial number, materials, and so forth. As data is recorded it will be stored into blocks chronologically up to the 1 MB storage, and then linked to the next block with a digital signature.

Block 1 in this example registers two transactions, transaction 1 and transaction 2, showing transactions between Damian and George, and between Bernard and Gerald. This block now gets a signature for this specific string of transactions, X32. See Figure 3.

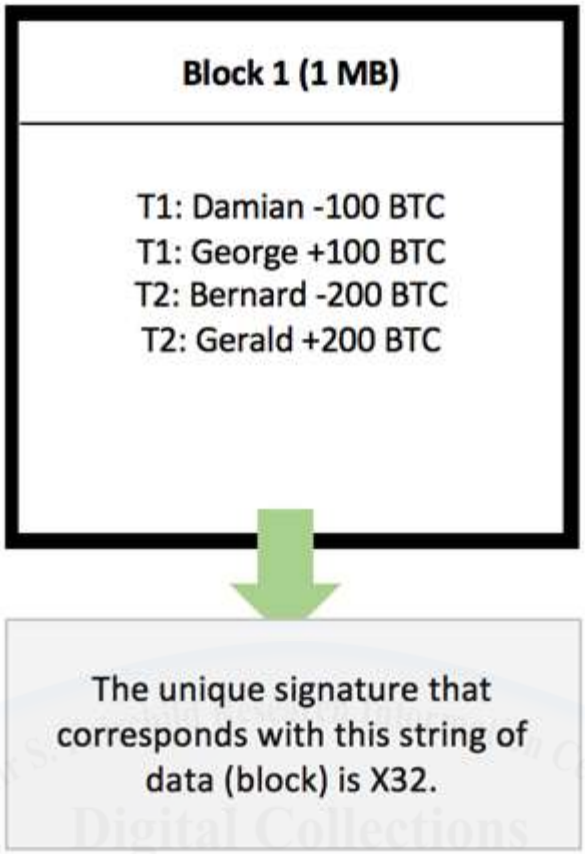

Figure 3: Block with Digital Signature[35]

Recall that a single digit change to the transactions in block 1 would now cause it to receive a different signature. The transactions in block 1 are now linked to block 2 by adding the signature of block 1 to the transactions of block 2. The signature of block 2 is now partially based on the signature of block 1, because it is included in the string of transactions in block 2. See Figure 4. Applying this to supply chain, the certificate of authenticity, manufacturer, or serial number that was input into block 1 receives a signature, which will be tied into the data of block 2, such as shipping date, port of entry, cost of shipping, and so forth. Then block 2's information will be given a signature.

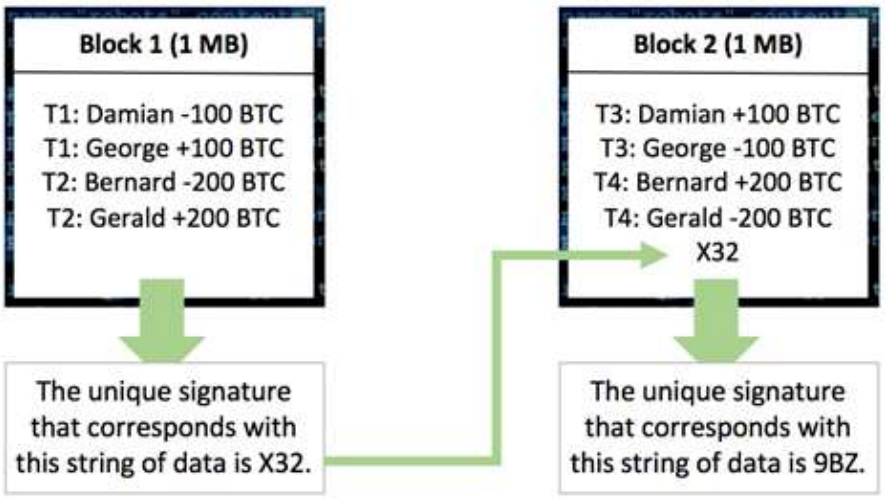

Figure 4: Linking Block 1 to Block 2 through Digital Signatures[36]

The signatures link the blocks together, making them a chain of blocks. Now add another block 3. See Figure 5:

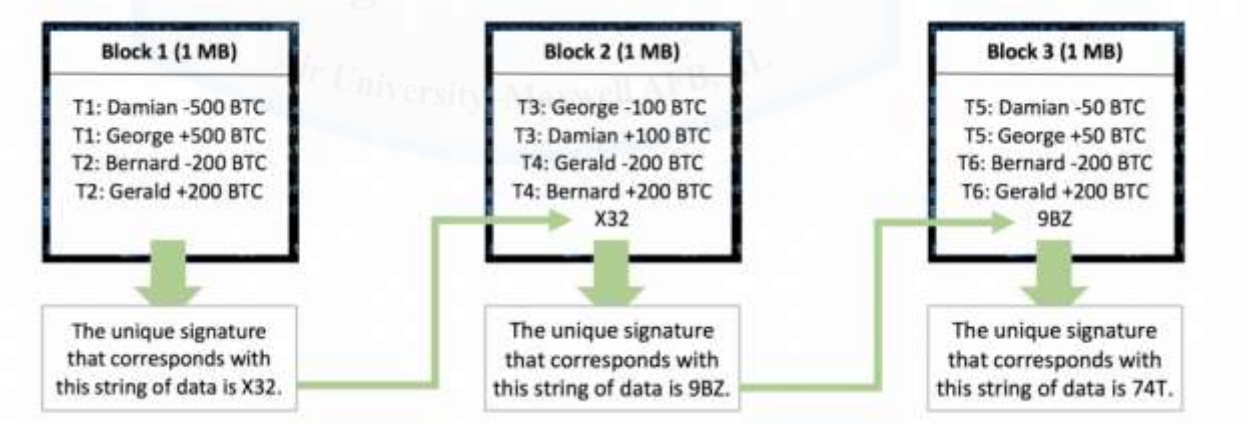

Figure 5: Addition of Third Block to Blockchain with Digital Signatures[37]

Now imagine if the transactions in block 1 are altered. The string of transactions in block 1 are now different, meaning the block also gets a new signature. The signature that corresponds with this new set of transactions is no longer X32, but is now W10. See Figure 6. Again, looking

at supply chain, this would equate to a manufacturer attempting to manipulate the component in some way. Inserting malicious software into a component would alter the digital signature of that component, causing a new signature.

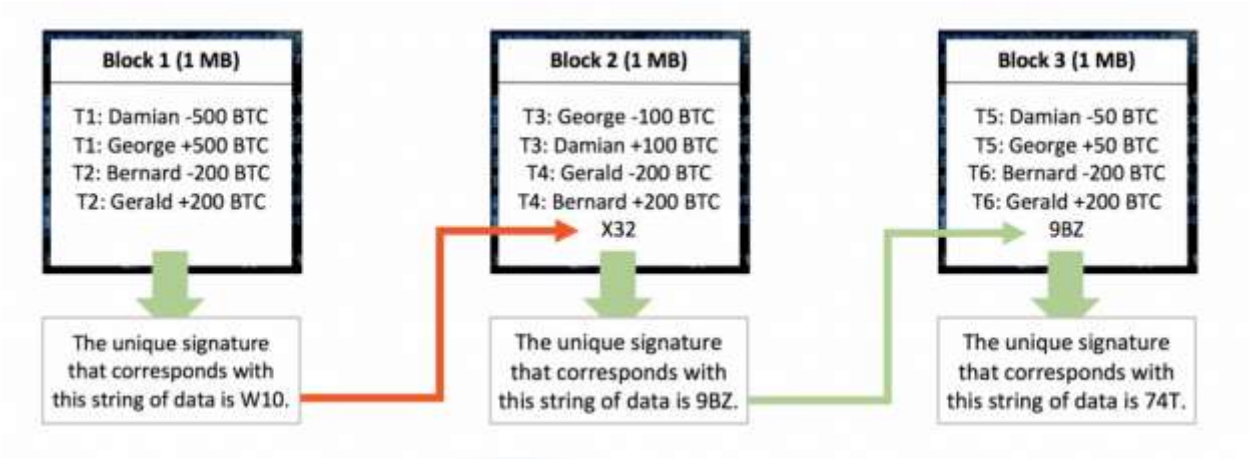

Figure 6: Impacts of Altering Data in Block 1 on Block 2 and Block 3[38]

The signature W10 does not match the signature that was previously added to block 2 anymore. Block 1 and 2 are now no longer chained to each other. This indicates to other users of this blockchain that some transactions in block 1 have been altered. Applying this to the supply chain, the malicious software that was added to the component changed the digital signature. As the component reaches the next point along the supply chain, it will be flagged since the digital signature does not match the standard software stored within the blockchain ledger, and also does not match the previous block software signature, causing the chain to be broken.

The only way that an alteration can stay undetected, is if the new signature of block 1 replaces the old one in the transactions of block 2. But if the transactions of block 2 changes, this will cause block 2 to have a different signature as well. Doing this causes transactions in block 2 to include W10 to match the signature of block 1, which in turn causes the signature of block 2 to become PP4 instead of 9BZ. Now block 2 and 3 are no longer chained together. See Figure 7.

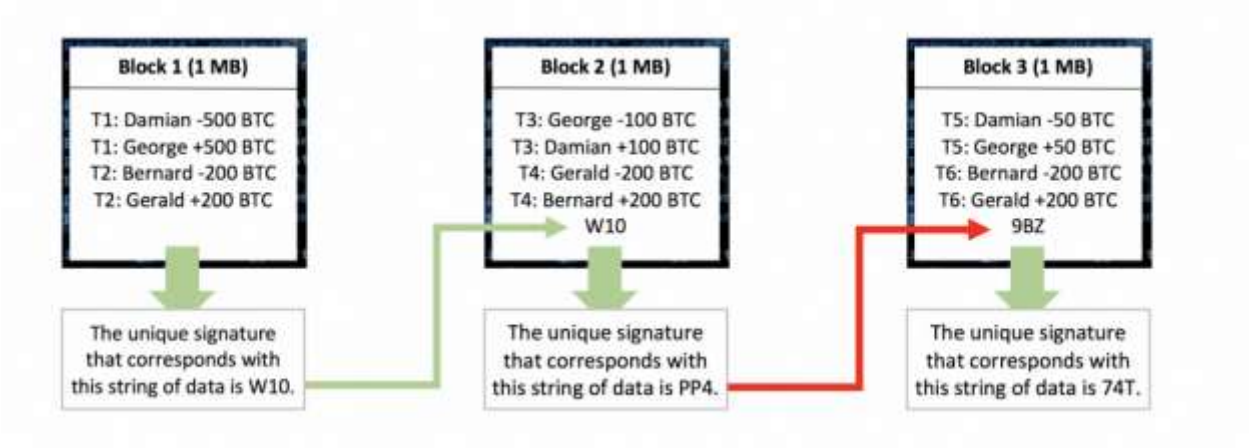

Figure 7: Attempting to Adjust Block 2 to Match Block 1 Digital Signature[39]

Altering a single block requires a new signature for every other block that comes after it simultaneously. Otherwise, the alteration will be detected. Within supply chain, this means if any change is made to a component, the previous blocks of data as well as any future blocks must also be altered. This is considered to be impossible. In order to understand why, an understanding of how signatures are created is needed.

The signature of a single block is produced using a cryptographic hash function, which is a very complicated formula that takes any string of input (such as a list of transactions) and turns them into a unique 64-digit string of output. For example, inputting "Jinglebells" into the cryptographic hash function would result in 761A7DD9CAFE34C7CDE6C1270E17F773025A61E511A56F700D415F0D3E199868.[40] A cryptographic hash function always gives the same output for the same input, but always a different output for different input. The inputs of the cryptographic hash function in this case are the transactions in the block, and the output is the signature that relates to that block. If a single digit of the input changes, including a space, changing a capital letter, or adding a period for example, the output will be totally different. Applying cryptographic hash functions within the

supply chain works similarly as each transaction can be verified legitimate by the receiver of any part.

Continuing the example; a corrupt user tries to alter a block of transactions, and therefore, has to calculate new signatures for the subsequent blocks in order to have the rest of the network accept the fraudulent change. The problem is the rest of the network is simultaneously calculating new signatures for new blocks being added to the blockchain. The corrupt user would have to calculate new signatures for these new blocks too as they are being added to the end of the chain. After all, the corrupt user needs to keep all of the blocks linked, including the new ones constantly being added, otherwise they will be exposed. Unless the corrupt user has more computational power than the rest of the network combined, they will never catch up with the rest of the network adding signatures.[41] This PoW consensus design is what allows blockchain to be secure, immutable, and tamper proof, but also takes time and massive computing power to achieve this.

In summary, blockchain is an electronic cryptographic ledger that follows a decentralized network model—instead of storing all information in one database such as in conventional cloud-based applications, the information is distributed and synchronized across all nodes in the network.[42] A consensus algorithm is deployed within the network allowing nodes to verify true information. Once verified, information is then added to the hash value of a previous block, and the new sequence is hashed to form a new block using a cryptographic (i.e., one-way) hash function.[43] Blockchain technology's transparency, accountability, and impermeable resistance against hacking makes it an attractive solution to DOD supply chain's problems.

Blockchain Infrastructure

As technology continues to advance at a rapid rate, the DOD needs to embrace new ways of rethinking old processes in the digital era to be increasingly effective in an evolving technology environment. Blockchain relies on several new technologies to function. Application Programming Interface (API) is needed to act as a software intermediary that allows two applications to talk to each other.[44] For example, a user's computer browser will communicate with the blockchain database to obtain the current status of supplies. The proliferation of high-speed internet globally has increased the need for APIs as applications communicate instantly with other applications anywhere in the world.[45]

One of the most popular applications today that deals with blockchain is Ethereum. Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications. A decentralized application, or DApp, serves a particular purpose to its users. Bitcoin, for example, is a DApp that provides its users with a peer to peer electronic cash system that enables online Bitcoin payments.[46]

A company can now utilize blockchain by creating a DApp on Ethereum, and implement it into their processes. For supply chain, this DApp will be used for asset tracking and the physical status of the asset. This is done by continually inputting asset data into the DApp, whether with a barcode scanner or automatically using automated technology such as RFID. Blockchain can further be combined with a smart contract to improve supply chain transactions. A smart contract is defined as a "computerized transaction protocol that automatically executes the terms of a contract".[47] The idea of smart contracts is to have a protocol, or code, representing a contract that is self-executing, making a contractual clause and the inclusion of a trusted third party, like a notary service, unnecessary by exchanging it with the consensus system provided by

the blockchain.[48] From a business point of view, blockchain and smart contracts allow for compliance with regulations and tracing for auditing purposes because smart contracts are self-executing on the data stored in the blockchain. Moreover, since less manual intervention will be required, this reduces the number of intermediaries necessary to be involved in the process and reduces both operational expenses and the manipulation risks.[49]

The pharmaceutical industry has become a leader in implementing blockchain technology into supply chains, specifically to deter counterfeit drugs, and is a prime candidate for purposes of this study in assessing how blockchain technology will impact parties with stakeholder interests that must be highly secure. By emulating the methods used by the pharmaceutical industry, DOD will better implement blockchain technology into the DOD supply chain, leading to the exposure of counterfeit and non-conforming parts, resulting in the increased security of DOD's cyber assets. To prove this, the following case studies will be analyzed to determine to what extent, if at all, the introduction of blockchain technology into the DOD supply chain could affect the cyber security of DOD assets.

CASE STUDIES OF PHARMACEUTICAL INDUSTRY'S APPLICATION OF BLOCKCHAIN INTO SUPPLY CHAIN

The World Health Organization (WHO) defines counterfeit drugs as "Products that are deliberately and fraudulently produced and/or mislabeled with respect to identity or source to make it appear to be a genuine product".[50] Experts have passively accepted the argument that 10 percent of medicines around the world could be counterfeit, and improving management of drug supply chain is the most direct and holistic approach to preventing counterfeit drugs.[51] From the

procurement of drug ingredients, production, and distribution to the use of drugs, every step of the drug supply chain has an important role in drug safety.

Application of blockchain into pharmaceutical supply chain

Modum.io AG Case

Modum.io AG is a Zurich-based supply chain intelligence and automation software program that utilizes blockchain technology.[52] Modum.io AG monitors all necessary data during the transport of medicinal products by combining wireless sensors with blockchain technology. This allows a distributor of temperature sensitive medical products to set a temperature threshold within a smart contract, and use the wireless sensors placed within medical products' packaging to automatically input temperature data into the blockchain throughout the supply chain. Upon the delivery, the smart contract is executed to ensure temperature category compliance. Once in the blockchain, the data is immutable and verifiable by any party.[53] These results are publicly accessible and reported back to the receiver as well as to the distributor.

The Modum.io AG architecture is structured into back-end (behind the scenes), front-end (user interface), and wireless sensor devices (such as smart thermometers). See Figure 8.

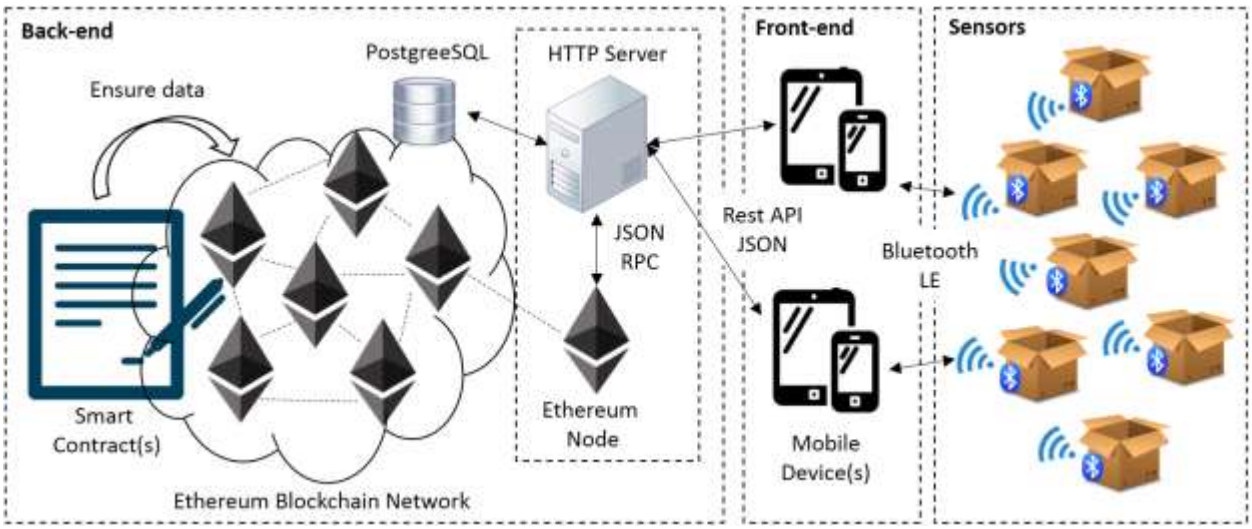

Figure 8: Modum.io AG Blockchain Architecture[54]

In the back-end, the Ethereum Blockchain Network[55] is used as the distributed ledger to verify temperature data recorded by sensors in the front-end. Smart contracts run on Ethereum, enabling the verification of data by automatically executing the predetermined set of rules. [56]

In the front-end, the Android client (smartphone) communicates with the Modum.io AG server using an API to decode requests and responses. Therefore, using a mobile phone, users can register new shipments including regulatory details, and a smart contract is created for each shipment. The API should also allow the receiver of a shipment to upload the temperature measurements recorded by the sensor to the server. Both the sender and the receiver should be made aware of the result of the contract and be able to get access to the temperature measurements.[57] Temperature data is provided by sensors that can be placed in strategical points of the shipment. The sensor has both identification and sensing capabilities which allows to communicate the precise temperature in specific points.[58]

To start the process, a track-and-trace number, which is typically found on the packet, has to be linked to the sensor device. The Ethereum Blockchain Network stores the association

between sensor and its current track-and-trace number, creates the smart contract, and stores the smart contract ID on the sensor device. Now the sensor device can be placed inside the medical products packet. At each supply point, the track-and-trace number is scanned by an Android client, which automatically downloads all temperature data at once via Bluetooth LE, and sends it to the smart contract. The sender will be notified immediately if the temperature has been outside the set thresholds. This is done until the package reaches its destination, with an assurance that all data is correct based on the Ethereum Blockchain Network validating data within the smart contract.[59]

Modum.io AG built a prototype and completed a pilot project together with pharmaceutical distributors. From July 7th to August 12th 2016, a pilot project was conducted and medical goods were shipped weekly from one supplier to a pharmaceutical wholesaler. A total of 55 shipments were sent, with 52 successfully completed to include associated temperature measurements. In total, 7576 temperature data points were measured, with sensors measuring in an interval of 10 minutes. Currently, Modum.io AG is planning for a second pilot project with over 500 shipments with more distributors and wholesalers.[60]

This case study shed some insights towards implementing blockchain technology in the pharmaceutical supply chain. When a supply point such as a warehouse has bad Internet connectivity, the offline feature which stores data internally could not connect to relay data to the Ethereum Blockchain Network. This data had to be added manually prior to onward shipment. The front end interface should offer as little options as possible. The initial Android app had two buttons: send and receive. Each pilot user was either sending or receiving packages, but rarely both; however, some users mixed up these buttons. Hiding the button to switch the workflow solved this problem. With this pilot, security weaknesses were identified within the sensors

sending data. Future software and hardware development will secure the data inside the sensor with signatures or access control schemes to read out the data.[61]

Philippine's Pharmaceutical Supply Chain Case

In the Philippines, 30 percent of inspected drug stores in 2003 were found with substandard, spurious, falsely labeled, falsified, counterfeit drugs.[62] The Philippine Food and Drug Administration (FDA) developed and utilized a Distributed Application (DApp) to combat this issue, creating it to be used on either Ethereum or Hyperledger Fabric (another blockchain network similar to Ethereum).

The first test was run on the public Ethereum Blockchain Network, which does not come with data encryption as default, causing further development to ensure security protocols are in position. The second test was run on the Hyperledger fabric blockchain platform. Unlike Ethereum, the platform is designed for private networks. It is open-source, modularized, and uses data encryption by default.[63] The system is designed with five starting nodes, one for each participant in the traditional drug distribution model: the manufacturer, the wholesaler, the retailer, the FDA, and the consumer portal website. Smart contracts are used to define contract-based relationships between participants, and the interfaces reflect supply chains in which the logged account is involved. The movement of a drug product along the distribution network is distributed across all nodes. The DApp has the capacity to detect anomalies, unauthorized data insertions, and missing drug products by comparing content with ledger records.[64]

The DApp front end is stored on all nodes. It can track the drug product as it travels along the chain and produces a timeline for each supply chain. Notifications are shown for shipments and anomalies are identified in the chain. It also allows the FDA account to detect authorized

manufacturers and dealers and store the designations in a smart contract. As an additional precaution, RFID tags are linked to drug products. Each node has an RFID scanner. Although RFIDs have had issues in the past, they are incorporated to drug product packages at the manufacturer level, and are added as a data point in pedigrees down the supply chain. The DApp allows the drug supply chain participants to create product manufacture pedigrees, shipping pedigrees, and receipt pedigrees, with each pedigree electronically signed and attached to the overall pedigree by each participant down the supply chain.[65]

Upon verification of identity, and registered distribution contracts linked to the specific brand of drug product, the system determines whether the merchandise moves along a registered chain and verifies consistency of information through each node. Information uploaded by these accounts to the network have credentials and certificates linked and are validated by the system against the registries.[66] When a manufacturer ships a batch of a drug product, a shipping pedigree is submitted into the network and the record is verified and counterchecked against the blockchain ledger by the DApp account of the recipient by using the cryptographic hash function (used in Ethereum). It sends a notification to the network if the hash values do not match. [67]

The system database consists of 4 main parts: The blockchain ledger, the smart contracts repository (where real-world contracts, participants, and drug products are defined), the document repository (where the pedigrees are stored), and the drug distribution history (listing of participants who possessed the drug at some point during the distribution, as well as information on shipments).[68]

This system will only be able to detect drug movements that follow official distribution chains known to the regulatory agency. It cannot track falsified drugs that are distributed through routes outside of official distribution chains.[69] Additionally, several assumptions were made for

this case. There is a regulatory agency monitoring the drug marketspace. The regulatory agency has the practice of certifying manufacturers, wholesalers, retailers, drug products, and reagents, and has the capacity to keep records of the certifications. The participants in the drug supply chains implement, or have the capacity to implement, standards on the metadata surrounding the drug products with which they conduct business. The participants in the pharmaceutical distribution chain are willing to participate in this disruption in the usual conduct of commerce.[70]

Gcoin's Use in Taiwan's Pharmaceutical Supply Chain Case

On 6 September 2016, the Taiwanese government announced new regulations governing the tracking and tracing of medicinal products. The purpose of the system is to reduce the risk of counterfeit drugs entering the legitimate supply chain, to quickly and effectively enforce the quality of drugs and to complete the recall of drugs as well as to protect the security and health of consumers.[71]

The characteristics of RFID, such as wireless and individual identification, are not always accurate, but make it possible to collect information in the drug supply chain more efficiently. However, barcode scanning and RFID for the tracking and tracing of medicines still permits counterfeit-drug debacles to happen on a worldwide scale. Even in relatively developed countries such as Taiwan, during March 2017, Crestor (rosuvastatin, 10 mg tablets) were found to be counterfeited by a similar ingredient called "Atorvastatin". This event caused panic in the public, as some patients already had taken counterfeit drugs with lower efficacy for weeks.[72]

Gcoin is similar to Ethereum, but is known for its governance structure in the blockchain world, meaning more oversight by a single entity. For this study, Gcoin blockchain was used to track every pill for drug identification, in a similar fashion to what blockchain accomplishes in

Bitcoin. For use in the drug supply chain: batch or serial number, quantities, and all required drug information will generate a hash number with a DrugID.[73]

Participants of drug supply chains include manufacturers, wholesalers, retailers, pharmacies, hospitals, and consumers (drug users). At the top of the Gcoin system are alliance members (governing body) who oversee the majority of transactions. In this case study, Taiwan's government acts as alliance members who surveil transactions and drug information while issuing minter and miner licenses. Drug manufactures are given the role of minter, or the organization in charge of issuing drugs. Large manufacturers and government agencies will act as miners who are in charge of verifying transactions and generating blocks. The remaining large wholesalers, hospitals or third parties are full nodes who are responsible for storing a backup of historical transactions.[74]

As for a top to bottom drug supply chain (from drug manufacturers to consumers), manufactures directly give their transaction data to drug receivers, and this information is documented in the Gcoin blockchain. The transaction data of the digital signatures of the drug seller and buyer, the drug information (including the time stamp, location, item name, etc.), and the amount of drugs are all verified on the chain. This data is hashed as a summary to be recorded on the Gcoin blockchain.[75] Whenever an illegal distributor wants to sell counterfeit drugs to buyers, the transaction will be judged invalid because of the presence of fraudulent information based on data stored in the Gcoin blockchain. On the other hand, unauthorized personnel are not able to carry out drug transactions in this system without a correct private key. Hence, the buyer/seller would be immediately aware of any anomalies within the transactions.[76]

In the Gcoin blockchain system, when the proposed conditions meet the set circumstances, contracts will be triggered automatically by the distributed blockchain system.

When it comes to the pharmaceutical supply chain, it is possible to set a series of conditions on the Gcoin blockchain, such as the identities of sellers or buyers, medicine distribution amounts, or the auditing occurrences of medicine distributors and so on. With Gcoin blockchain, there is no central power that has the right to change a smart contract unless every full node on the Gcoin blockchain system comes to a consensus.[77]

With the Gcoin blockchain system, the transaction data of drugs is open but checked automatically through the drug supply chain. In the Gcoin blockchain structure, every drug has only one identification and can only be sold once from one address (account) to another; this will increase the accountability of drugs, leading to increased drug security. Every transaction is broadcast to every participant to check if an anomalous transaction has transpired and will be stopped automatically according to the conditions set in the smart contract. With the Gcoin blockchain system, people including inspectors in the government have access to track and trace drugs in the supply chain without going into factories, warehouses, or pharmacies.[78]

ANALYSIS OF BLOCKCHAIN APPLICATION TO DOD SUPPLY CHAIN

The preceding three pharmaceutical supply chain cases attempted to utilize blockchain technology to increase their efficiency, security, and reliability. However, there were several issues encountered that proved blockchain is still an immature technology, and may not apply to the DOD supply chain yet. The following section will briefly review the possible application of blockchain to the DOD supply chain, and issues encountered that may limit implementation.

Blockchain Applications to DOD Supply Chain

Blockchain technology has been touted as the silver bullet to solve several industry's issues as it provides immutable, auditable, and uncensored truth.[79] The application of blockchain technology into the supply chain of the pharmaceutical industry provides a good template for DOD to follow; however, there are several areas of concern these cases identified that must be addressed prior to implementation.

There were common themes among these cases on how blockchain could be applied to DOD supply chain. First, there must be a system database consisting of four main parts: the blockchain ledger, the smart contracts repository, the document repository, and the component distribution history. The blockchain ledger used in these cases were either Ethereum Blockchain Network or Hyperledger, but it is likely that DOD would wish to create a separate blockchain ledger specifically for the DOD. SIMBA Chain is already contracted by the AFRL, and would be an obvious choice since it has already been integrated into the DOD system. Smart contracts would need to be established clearly by contracting offices and software engineers to ensure accurate requirements, as the contract will automatically execute a predetermined set of rules. A document repository, or document register, would be stored on a shared database (possibly the DOD cloud) to include credentials and certificates issued by the DOD that any smart contract can validate transactions against. Lastly, the component distribution history will be stored on a shared database (possibly the same DOD cloud) and list all participants who possessed the component at some point during the supply chain, as well as information on shipments. These separate databases are necessary as blockchains and smart contracts are unable to retain large quantities of data.

Once a system database is established, the back-end, front-end, and sensors must be established. The back-end should consist of all the databases previously established, and an API to interface between them. The front-end should be a DApp accessed through a website or networked device that has been developed for DOD to use. The front-end will require substantial software, firmware, and hardware development as these items do not exist, as well as a phased rollout plan to integrate it into the current DOD supply system. Wireless sensors are not mandatory, but would help automate the process to a degree. DOD has a robust RFID program, so development of sensors that integrate with new blockchain technology should be minimal.

An RFID will be integral to several aspects of the blockchain to link the physical component to the digital world. Using a track-and trace number, such as a barcode on the package or a microcode built into the component, has been the best way to accomplish this. Each RFID will need to have an internal memory sufficient to store package contents information (condition, quantity, serial numbers), and possibly a built-in GPS to allow each data transfer to the smart contract to include a location. All RFIDs should be initiated at the manufacturer level to ensure provenance of the material.

All sensor data will be combined with transaction data and sent to the DOD blockchain. This information consists of digital signatures of the seller and buyer, time stamps, locations, item name, and the quantity, and will be put into a cryptographic hash function and verified on the smart contract within the blockchain. The component distribution history database will contain the pre-hashed information, which will require a type of data management software to handle the immense size and detail of information. The component database, if organized sufficiently, will allow audits, data calls, and inspections to be performed without going into factories, warehouses, or distribution centers.

Based on the Philippines and Taiwan cases, an authority to surveil transactions, administer certificates, and ensure smart contracts are written correctly, is needed. [80,81] The DOD is already set up to act as an administrator, and will most likely require a group created within the DOD to oversee it. An authority overseeing the blockchain will also allow a secure two layer verification. This will be done by the DOD ensuring certificates are only issued to legitimate manufacturers and distributers, and the hash values of each transaction match the hash values of the blockchain ledger. This will not completely eliminate counterfeit parts, but these two layers of verification will ensure trustworthy manufacturers and distributers, significantly decreasing the likelihood of any counterfeit part entering the supply chain.

If DOD did implement a blockchain with an overall authority, it would have the following structure: at the top of the structure, the DOD would govern all actions being performed within the blockchain. Large manufacturers and government agencies would act as miners who are in charge of Proof of Work (PoW): verifying transactions and generating blocks. The remaining distributers, or third parties, would be complete nodes who are responsible for storing a backup of historical transactions. A governance centered blockchain will allow DOD to act as a regulator, ensuring all actions within the blockchain are monitored and secured. This will address data privacy issues as DOD will determine who can participate, and standardize all interfaces among participants.

Although the application of blockchain technology into the supply chain of the pharmaceutical industry provides a good template for DOD to follow; there are several areas of concern these cases identified that must be addressed prior to implementation.

Issues Encountered

Amongst these cases, there were also issues that proved blockchain technology's application to the DOD supply chain may not be economically feasible. The first concern for any organization implementing an emerging technology should be the participants' willingness to take part in the disruption of the usual conduct of commerce. A prime example of an emerging technology failing to obtain participants' support is the RFID program for IBM and Maersk. Around 2005 RFID was touted to replace all barcodes, and industry leaders IBM and Maersk announced they would establish a worldwide Container Information Framework network based on RFID. However, it never fully replaced existing technology due to the inability to garner support from employees and customers.[82]

Other issues with the RFID technology that was found in the Modium.io AG case were the security and the connectivity of the sensors. The sensors were based on Bluetooth technology, and had little to no security protocols to protect hacking or data mining. Also, when a supply point, such as a warehouse, has bad Internet connectivity, the offline feature which stores data internally could not connect to relay data to the Ethereum Blockchain Network. This data had to be added manually. DOD will require an updated wireless network at all blockchain nodes, and RFID security protocol development prior to implementation to avoid these issues.

An assumption must be made prior to blockchain being implemented into supply chain: blockchain is only as effective as the digital-physical relationship made between component and digital information. For example, a supply system may show a quantity of 50 parts at a certain location; however, upon physical inspection there may be 40 parts, or there may be no parts at all at that location. What is recorded within the blockchain database must be accurately represented physically.

Another issue needing to be addressed prior to implementing blockchain is how to convince all parties to set up interfaces to the blockchain? Low-budget solutions allow error-prone manual entry into web forms, but this would defeat the basic idea of blockchain ensuring accurate data.[83] DOD could force all participating organizations to set up interfaces to the single DOD blockchain, but the enforcement is difficult. An alternative to using a single blockchain is integrating multiple blockchains; however, it is not clear how different blockchains will talk to each other as there is not an industry standard yet.[84]

Similarly, for blockchain to identify counterfeit parts, participating parties must first manually enter legitimate parts into the supply chain at the origin. This remains an issue as the integrity of those who input it into the system must be validated regularly. Blockchain does have the advantage that if any counterfeit part was found within the supply chain it could be traced back to that origin, and that manufacturer could be removed from the process. Understandably, this is a reactive approach and only decreases the risk of a catastrophic event.

Moving to technical issues, blockchains generally rely on Proof of Work (PoW) consensus over a distributed network, which requires massive amounts of computing power to solve complex algorithms and create cryptographic hash functions. The amount of computing power required for one Bitcoin trade in in 2015 could power 1.57 American households for one day. [85] Today, one Bitcoin trade could power a house for *one month*.[86] As blockchain technology continues to become more mainstream, the sustainability of a consensus driven blockchain becomes unfeasible. DOD does have the option to utilize alternative methods to PoW, such as Proof of Stake (PoS). This method awards those with more stake to validate transactions, which usually means those with larger, more efficient, computing capacity.[87]

Two restraints for the implementation of blockchain technology into the DOD arise from the issues of energy consumption and transparency of data. Executive Order 13423 – "Strengthening Federal Environmental, Energy, and Transportation Management" set goals to improve energy efficiency and reduce greenhouse gas emissions of the agency, through reduction of energy intensity by 3 percent annually through the end of fiscal year 2015.[88] Energy efficiency has continued to be a concern for the DOD, causing blockchain technology using PoW to be difficult to implement.

Transparency of information is a major concern for DOD as well. Clearances, background checks, and need-to-know authorizations are required by DOD to be able to view classified data, and the consolidated supply status of a large division becomes classified as it possibly could reveal a weakness in that division's overall readiness.[89] Every blockchain transaction is broadcast to every participant to check if an anomalous transaction has occurred, allowing the transaction information to be exposed. Increasing transparency within supply chains is the crux of blockchain technology benefit, yet most organizations do not want to expose their own data.[90] The DOD is unique in that it is a public entity that would benefit from transparency, yet requires confidentiality to ensure national security.

Security concerns arise with the distributed nature of blockchain technology; however, a larger concern has risen with the recent major blockchain modifications ("hard forks") performed by Bitcoin and Ethereum. These hard forks consisted of a complete reset of the blockchain system either due to a successful hack, or major upgrade such as PoW to PoS. The ability to completely reset a blockchain has caused some concern over the governance of a blockchain and how they will be held accountable. DOD should act as the governance head of any blockchain

they participate into ensure accountability of the system, and also to manage the overall structure as was seen in the Taiwan Gcoin case.

Another result of blockchain's encrypted, distributed nature is the slow processing times of each transaction. Taiwan's case demonstrated that Gcoin generates a block every 15 seconds, processing 1.51 million transactions in one day. However, a standard Bitcoin block takes an average of 10 minutes to generate, and up to several hours to finalize.[91] The inefficiency in processing times easily compounds to create longer lead times. However, the time savings alone from eliminating the need for intermediaries and certain bureaucratic processes within the DOD may offset the slow processing time.

Blockchain works well with digitally tracked items, such as cryptocurrencies, or uniquely identifiable items, such as serialized diamonds, but generic goods are not as easy to account for. The food supply chain is a popular blockchain use-case, but there have been many food scandals – such as the milk powder scandal in China – where the manufacturers wittingly input low-quality products or provided false information into the system.[92] How can DOD make sure that blockchain registered labels or RFID tags are correctly applied at origin, or not exchanged along the supply chain? The Philippines case suggested the Government act as administrator to validate all manufactures and distributers, but there are still areas of risk since enforcement may not be feasible at this scale. Similarly, how can data input into the blockchain system from many different companies, countries, and sources (to include paper-based sources) be validated?[93] DOD would require an entire organization dedicated to the oversight, integration, management, enforcement, and maintenance of a DOD blockchain system.

Equally as important as the information that is input into the system, is ensuring distributers do not circumvent the blockchain system through unofficial channels. The

pharmaceutical supply chain for Philippines found that implementing blockchain technology did not stop counterfeit drugs from being distributed into the market. They noted their system was only able to detect drug movements that follow official distribution chains known to the regulatory agency. Again, the importance of validating manufactures and distributors by an overarching agency will help ensure all components that enter the DOD supply chain have gone through at least one legitimate source.

Lastly, errors happen in the DOD supply chain. Whether it is wrong shipment information or a last-minute change of a carrier. The nature of blockchain does not allow for a mistake to be overwritten as all information is immutable.[94] The DOD has a massive logistics footprint, and it is inevitable that mistakes will be made. Since it is impossible to change a mistake, it will require a new block be added with correct information. However, there are a few problems with this. Since transactions take 10-60 minutes to finalize on average, a correction will need to be made after the transaction is finalized. If a correction is attempted before that time, the system works chronologically and will accept the first, incorrect, entry and reject the second, corrected, entry. Even waiting until after the transaction is finalized causes issues as there will be incorrect data permanently stored in the blockchain.

CONCLUSIONS AND RECOMMENDATIONS

Counterfeit parts have plagued the supply chains of multiple industries around the world, allowing substandard, and sometimes malevolent, components to infiltrate the marketplace.[95] Given this widespread problem, it should be no surprise that microelectronics have become a major new concern as a target and avenue for an adversary to infiltrate the DOD supply chain, as the microelectronics are inexpensive to duplicate but difficult to differentiate from legitimate

parts. Multiple methods have been employed to combat counterfeit goods within the DOD supply chain, but these methods have only slightly decreased the instances of counterfeits.[96]

The introduction of blockchain technology in 2008 to digitally track cryptocurrency has provided the digital generation a new method of tracking and accounting for data, and has quickly been applied to several industries. Within the logistics industry, blockchain technology is attempting to improve supply chains' accountability, visibility, and traceability, which endeavors to decrease the likelihood of counterfeit goods and increase the security of DOD assets. The DOD has already implemented several blockchain initiatives,[97] but these are still in the early stages of development for supply chain.

Three cases of the pharmaceutical industry implementing blockchain to their supply chain were analyzed, and it was found blockchain technology has the potential to identify and decrease counterfeit parts. However, this paper finds that current blockchain technology is not mature enough to be implemented into the DOD supply chain. Implementation is not economically feasible primarily due to energy efficiency concerns, data privacy issues, and the lack of standardized blockchain interfaces among all participants. Thus, blockchain technology will require maturation in several key areas prior to being able to impact the cyber security of DOD assets.

Recommendation #1 – Continue to fund DARPA research with private industry involvement (including SIMBA) to address issues noted above. Specific attention should be placed on the following areas: Implement employee and organization buy-in strategies, create accurate links between the digital and physical asset status, standardize blockchain interfaces, develop blockchain-to-blockchain communications, ensure Proof of Stake (PoS) application through Ethereum or Hyperledger blockchain networks to decrease energy consumption, develop

blockchain circumvention strategies, and secure data privacy within the blockchain. These issues were identified within the case-use studies as areas that restricted the implementation of blockchain technology into any supply chain. Once these issues are resolved, blockchain technology will have a higher chance of successfully being implemented into the DOD supply chain, improving asset accountability, thus, increasing asset security.

Recommendation #2 – After the resolution of several key issues noted above, develop a blockchain structure, similar to the Taiwan Gcoin model, which allows the DOD to govern all aspects of a private blockchain. Blockchain technology is based on large numbers of decentralized public nodes to form its immutable and tamper-proof ability, but large public blockchains create potential transparency and privacy concerns. A blockchain that is controlled by one entity, specifically the DOD, will mitigate these privacy concerns as they are able to regulate who accesses the blockchain. However, DOD must also maintain a sufficient number of decentralized nodes within their blockchain to ensure it remains immutable and tamper-proof.

NOTES

1. Paul Hoeper and John Manferdelli, *Report of the Defense Science Board Task Force on Cyber Supply Chain.* (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017), 3.

2. "Havoscope Global Black Market Information," *Havoscope.com*, accessed 30 January 2019, https://www.havocscope.com/.

3. Nan Tian et al., *Trends in World Military Expenditure, 2017*, (Stockholm International Peace Research Institute, May 2018), 2.

4. Senate, *Senate Homeland Security and Governmental Affairs Committee Hearing*, (Washington, D.C.: Congressional Documents and Publications, Federal Information & News Dispatch, Inc., 13 September 2018), 2.

5. United States Government Accountability Office, *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk*, GAO-16-236, (Washington, D.C.: U.S. Government Publishing Office, Washington, 2016), 5.

6. Hubert Pun; Jayashankar M. Swaminathan, and Pengwen Hou, "Blockchain Adoption for Combating Deceptive Counterfeits," *Kenan Institute of Private Enterprise*, no. 18-18 (27 July 2018), 2-3.

7. Ibid., 3.

8. GAO, *Counterfeit Parts*, 30.

9. United States Government Accountability Office, *High-Risk Series*, GAO-17-317, (Washington, D.C.: U.S. Government Publishing Office, Washington, 2017), 248.

10. "Blockchains: The great chain of being sure about things," *The Economist*, 31 October 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things.

11. Peter Verhoeven, Florian Sinn, and Tino T. Herden, "Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology." *Logistics* 2, no. 3:20, (11 September 2018), 2.

12. Aerospace Industries Association of America, Inc. "Counterfeit Parts: Increasing Awareness and Developing Countermeasures." 2010, accessed 31 January 2019. http://www.aia-aerospace.org/wp-content/uploads/2016/05/counterfeit-web11.pdf.

13. Hoeper, *Task Force on Cyber Supply Chain*, 3.

14. GAO, “Counterfeit Parts.” 1.

15. “Bogus Parts for Aircraft implicated in many crashes.” *The Irish Times*, 6 October 2000. https://www.irishtimes.com/news/bogus-parts-for-aircraft-implicated-in-many-crashes-1.1106164.

16. Ibid.

17. National Defense Authorization Act for Fiscal Year 2018, H.R.2810, 115th Congress Public Law 91. (12 December 2017). https://www.congress.gov/bill/115th-congress/house-bill/2810/text.

18. Neil B. Barnas, “Blockchains in National Defense: Trustworthy Systems in a Trustless World,” (Maxwell AFB, AL: Air Command and Staff College, June 2016), 29.

19. “U.S. Air Force to Teach Blockchain Technology for Supply Chain Management,” *Supply and Demand Chain Executive*. 7 Dec 2018. https://www.sdcexec.com/software-technology/news/21035844/us-air-force-to-teach-blockchain-technology-for-supply-chain-management.

20. Blockchain Demonstration Site, *SecureMarking and AFIT*, accessed 20 Feb 2019. http://blockchain.securemarking.com/.

21. “U.S. Air Force to Teach,” *Supply and Demand Chain Executive*, 7 Dec 2018.

22. Sophie Chapman, “USAF to use Blockchain-Based SIMBA Chain for its supply chain operations,” *SupplyChainDigital.com*, 20 Nov 2018. https://www.supplychaindigital.com/technology/usaf-use-blockchain-based-simba-chain-its-supply-chain-operations.

23. Ibid.

24. David Hamilton, “DARPA Blockchain Programs,” *Coincentral.com,* 1 October 2018. https://coincentral.com/darpa-blockchain-programs/.

25. Carten Cordell, “DARPA wants to take a look at blockchain’s security rules,” *FedScoop.com*, 21 Nov 2018. https://www.fedscoop.com/darpa-wants-take-look-blockchains-security-rules/.

26. "Blockchains," *The Economist*, 31 October 2015.

27. “Banking Is Only The Beginning: 50 Big Industries Blockchain Could Transform,” *CB Insights*, 19 Dec 2018. https://www.cbinsights.com/research/industries-disrupted-blockchain/.

28. “Blockchain Explained,” *Upfolio LLC*, accessed 18 January 2019. https://www.upfolio.com/ultimate-blockchain-guide.

29. Aran Davies, "Blockchain for Supply Chain Management." *DevTeam.Space* (blog), accessed 21 Jan 2019. https://www.devteam.space/blog/blockchain-for-supply-chain-management/.

30. "Proof of Work vs Proof of Stake: Basic Mining Guide," accessed 22 Feb 2019. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/#What_is_the_Proof_of_work.

31. John Lilic, "Bitcoins Energy Consumption An Unsustainable Protocol That Must Evolve?" *Blockgeeks*, accessed 22 Feb 2019. https://blockgeeks.com/bitcoins-energy-consumption/ (accessed 22 Feb 2019).

32. "Proof of Work vs Proof of Stake," accessed 22 Feb 2019.

33. Jimi S., "How does blockchain work in 7 steps—A clear and simple explanation." *Medium Corp.*, 6 May 2018. https://medium.com/coinmonks/blockchain-for-beginners-what-is-blockchain-519db8c6677a.

34. Ibid.

35. Ibid.

36. Ibid.

37. Ibid.

38. Ibid.

39. Ibid.

40. Ibid.

41. Ibid.

42. D.E. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-resistant mobile health using blockchain technology," *JMIR Mhealth Uhealth*, 26 July 2017, 5(7):e111, doi: 10.2196/mhealth.7938. http://mhealth.jmir.org/2017/7/e111/. PubMed: 28747296.

43. Jimi, "How does blockchain work in 7 steps," 6 May 2018.

44. "What is an API? (Application Programming Interface)," *MuleSoft*, accessed 5 February 2019. https://www.mulesoft.com/resources/api/what-is-an-api.

45. Ibid.

46. "What is Ethereum? The Most Comprehensive Guide Ever!" *BlockGeeks*, 12 September 2018. https://blockgeeks.com/guides/ethereum/.

47. N. Szabo, "Smart Contracts," accessed on 30 January 2019. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

48. Thomas Bocek et al., "Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain." *IFIP/IEEE International Symposium on Integrated Network Management.* (Zurich, Switzerland: Communication Systems Group, Department of Informatics, University of Zurich, 2017), 772-777.

49. Ibid.

50. LaKeisha W. and Ellen M., "The real impact of counterfeit medications." *US Pharm*, (2014), 39, 44–46.

51. E.A. Blackstone, J.P. Fuhr Jr., and S. Pociask, "The health and economic effects of counterfeit drugs." *Am. Health Drug Benefits*, (7 June 2014), 216–224. https://www.ncbi.nlm.nih.gov/pubmed/25126373.

52. Modum.io, "About us", *Modum.io AG*, accessed 01 Feb 2019. https://modum.io/company/aboutus.

53. Bocek, "Blockchains Everywhere," 772-777.

54. Ibid.

55. "Ethereum Project," accessed 1 Feb 2019. https://www.ethereum.org/.

56. Bocek, "Blockchains Everywhere," 772-777.

57. Ibid.

58. Ibid.

59. Ibid.

60. Ibid.

61. Ibid.

62. Babar Z., *Pharmaceutical Policy in Countries with Developing Healthcare Systems*, (Cham, Switzerland: Springer International Publishing, 2017).

63. Patrick Sylim et al., "Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention" *JMIR Research Protocols.* 9 September 2018. doi: 10.2196/10163.

64. Ibid.

65. Ibid.

66. Ibid.

67. Ibid.

68. Ibid.

69. Ibid.

70. Ibid.

71. Jen-Hung Tseng et al., "Governance on the Drug Supply Chain via Gcoin Blockchain," *International Journal of Environmental Research and Public Health.* 23 May 2018.

72. "FDA orders recall of all batches of Crestor tablets," *Focus Taiwan,* 7 Mar 2017. Available online: http://focustaiwan.tw/news/asoc/201703070031.aspx.

73. Tseng, "Governance on the Drug Supply Chain."

74. Ibid.

75. Ibid.

76. Ibid.

77. Ibid.

78. Ibid.

79. Adrianne Jeffries, "'Blockchain' Is Meaningless," *The Verge,* 7 Mar 2018. https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning.

80. Sylim, "Blockchain Technology for Detecting Falsified Drugs."

81. Tseng, "Governance on the Drug Supply Chain."

82. Torsten Mallee, "The blockchain hype in SCM: how high can it go?" *AEB,* 9 Feb 2018. https://www.aeb.com/uk-en/magazine/blockchain-hype-scm-supply-chain.php?l=en.

83. Jeffries, "'Blockchain' Is Meaningless."

84. Patricia Friedel, "Six things wrong with blockchain," *CIPS.ORG,* 1 Dec 2017. https://www.cips.org/en/supply-management/analysis/2017/december/six-things-wrong-with-blockchain-/.

85. John Lilic, “Bitcoins Energy Consumption An Unsustainable Protocol That Must Evolve?” *BlockGeeks,* accessed 22 Feb 2019. https://blockgeeks.com/bitcoins-energy-consumption/.

86. Friedel, “Six things wrong with blockchain.”

87. Toshendra Kumar Sharma, “What are the Alternative Strategies for Proof-of-Work?” *Blockchain Council*, 25 Jan 2018. https://www.blockchain-council.org/blockchain/what-are-the-alternative-strategies-for-proof-of-work/.

88. Executive Order (EO) 13423, “Strengthening Federal Environmental, Energy, and Transportation Management.” Federal Register Vol. 72, No. 17, (January 24, 2007), 3919.

89. Department of Defense Manual (DoDM) Vol. 3. *DoD Information Security Program: Protection of Classified Information*, 19 Mar 2013.

90. Mallee, “The blockchain hype in SCM.”

91. Bernard Marr, “The 5 Big Problems With Blockchain Everyone Should Be Aware Of,” *Forbes*, 19 Feb 2018. https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#4a3193f71670.

92. Jeffries, “’Blockchain’ Is Meaningless.”

93. Ibid.

94. Ibid.

95. Senate, *Senate Homeland Security*, 2.

96. Pun, Swaminathan, and Hou, “Blockchain Adoption for Combating Deceptive Counterfeits,” 3.

97. Hamilton, “DARPA Blockchain Programs.”

BIBLIOGRAPHY

Aerospace Industries Association of America, Inc. "Counterfeit Parts: Increasing Awareness and Developing Countermeasures." March 2011. http://www.aia-aerospace.org/wp-content/uploads/2016/05/counterfeit-web11.pdf.

Babar, Z. *Pharmaceutical Policy in Countries with Developing Healthcare Systems.* Cham, Switzerland: Springer International Publishing; 2017.

"Banking Is Only The Beginning: 50 Big Industries Blockchain Could Transform." CB Insights. 19 December 2018. https://www.cbinsights.com/research/industries-disrupted-blockchain/.

Barnas, Maj Neil B. *Blockchains in National Defense: Trustworthy Systems in a Trustless World*. Maxwell AFB, AL: Air University Press, June 2016.

Blackstone, E.A., J.P. Fuhr Jr., and S. Pociask. "The health and economic effects of counterfeit drugs." *Am. Health Drug Benefits*, (7 June 2014), 216–224. https://www.ncbi.nlm.nih.gov/pubmed/25126373.

SecureMarking, and AFIT. "Blockchain Demonstration Site." Accessed 20 February 2019. http://blockchain.securemarking.com/.

"Blockchain Explained." Upfolio LLC. (Los Angeles and Boston, 2018). https://www.upfolio.com/ultimate-blockchain-guide.

"Blockchains: The great chain of being sure about things". *The Economist.* 31 October 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things.

Bocek, Thomas, Bruno B. Rodrigues, Tim Strasser, and Burkhard Stiller. *Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain*. IFIP/IEEE International Symposium on Integrated Network Management 772-777. University of Zurich: Communication Systems Group, Department of Informatics, 2017.

"Bogus Parts for Aircraft implicated in many crashes." *The Irish Times*, 6 October 2000. https://www.irishtimes.com/news/bogus-parts-for-aircraft-implicated-in-many-crashes-1.1106164.

Boyens, Jon, Celia Paulsen, Rama Moorthy, and Nadya Bartol. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* National Institute of Standards and Technology Special Publication 800-161. Washington, D.C.: U.S. Department of Commerce. April, 2015. http://dx.doi.org/10.6028/NIST.SP.800-161.

Chapman, Sophie. "USAF to use Blockchain-Based SIMBA Chain for its supply chain operations." *SupplyChainDigital.com*. 20 November 2018.

https://www.supplychaindigital.com/technology/usaf-use-blockchain-based-simba-chain-its-supply-chain-operations.

Cordell, Carten. “DARPA wants to take a look at blockchain’s security rules.” *FedScoop.com*. 21 November 2018. https://www.fedscoop.com/darpa-wants-take-look-blockchains-security-rules/.

Davies, Aran. “Blockchain for Supply Chain Management.” DevTeamSpace. Product Blog. Accessed 21 January 2019. https://www.devteam.space/blog/blockchain-for-supply-chain-management/.

Department of Defense Manual (DoDM) 5200.01 Vol. 3. *DoD Information Security Program: Protection of Classified Information*, 19 March 2013.

Ethereum official website. “Ethereum Project.” Accessed 01 February 2019. https://www.ethereum.org/.

Executive Order 13423. “Strengthening Federal Environmental, Energy, and Transportation Management.” *Federal Register* 72, no. 17 (January 24 2007): 3919.

“FDA orders recall of all batches of Crestor tablets.” *Focus Taiwan,* 7 March 2017. http://focustaiwan.tw/news/asoc/201703070031.aspx.

Friedel, Patricia. “Six things wrong with blockchain.” *CIPS.ORG*. 1 December 2017. https://www.cips.org/en/supply-management/analysis/2017/december/six-things-wrong-with-blockchain-/.

Hamilton, David. “DARPA Blockchain Programs.” *Coincentral.com*. 1 October 2018. https://coincentral.com/darpa-blockchain-programs/.

Havoscope Global Black Market Information. Accessed 30 January 2019. https://www.havocscope.com/.

Hoeper, Paul, and John Manferdelli. “Report of the Defense Science Board Task Force on Cyber Supply Chain.” Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017.

House. *National Defense Authorization Act for Fiscal Year 2018*. 115th Cong. Public Law 91, 12 December 2017, H.R.2810.

Ichikawa, DE, M. Kashiyama, and T. Ueno. “Tamper-resistant mobile health using blockchain technology.” *JMIR Mhealth Uhealth*. 2017 July 26. doi: 10.2196/mhealth.7938. PubMed: 28747296. http://mhealth.jmir.org/2017/7/e111/.

Jeffries, Adrianne. “’Blockchain’ Is Meaningless.” *The Verge*. 7 March 2018. https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning.

Jenks, Tyler. “Top Blockchain Use Cases for Supply Chain Management.” *Verypossible.com*. 23 February 2018. https://www.verypossible.com/blog/top-blockchain-use-cases-for-supply-chain-management.

Kückelhaus, Markus, and Gina Chung. *Blockchain in Logistics: Perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry.* Troisdorf, Germany: DHL Customer Solutions and Innovation, 2018.

LaKeisha, W., and M. Ellen. “The real impact of counterfeit medications.” *US Pharm*. 2014.

Lilic, John. “Bitcoins Energy Consumption: An Unsustainable Protocol That Must Evolve?” *Blockgeeks*. Accessed 22 February 2019. https://blockgeeks.com/bitcoins-energy-consumption/.

Mallee, Torsten. “The blockchain hype in SCM: how high can it go?” *AEB*. 9 February 2018. https://www.aeb.com/uk-en/magazine/blockchain-hype-scm-supply-chain.php?l=en.

Marr, Bernard. “The 5 Big Problems With Blockchain Everyone Should Be Aware Of.” *Forbes*. 19 February 2018. https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#4a3193f71670.

Modum.io official website. “About us.” Accessed 01 February 2019. https://modum.io/company/aboutus.

“Proof of Work vs Proof of Stake: Basic Mining Guide.” *Blockgeeks.com.* Accessed 22 Feb 2019. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/#What_is_the_Proof_of_work.

Pun, Hubert, Jayashankar M. Swaminathan, and Pengwen Hou. *Blockchain Adoption for Combating Deceptive Counterfeits.* Kenan Institute of Private Enterprise Research Paper No. 18-18. 27 July 2018.

S., Jimi. “How does blockchain work in 7 steps—A clear and simple explanation.” *Medium Corp*. 6 May 2018. https://medium.com/coinmonks/blockchain-for-beginners-what-is-blockchain-519db8c6677a.

Scott, Tracie, Armand L. Post, Johnny Quick, and Sohail Rafiqi. *Evaluating Feasibility of Blockchain Application for DSCSA Compliance.* SMU Data Science Review: vol. 1: no. 2, 2018.

Senate, *Senate Homeland Security and Governmental Affairs Committee Hearing*. Washington, D.C.: Federal Information & News Dispatch, Inc., 13 September 2018.

Sharma, Toshendra Kumar. “What are the Alternative Strategies for Proof-of-Work?” *Blockchain Council*. 25 January 2018. https://www.blockchain-council.org/blockchain/what-are-the-alternative-strategies-for-proof-of-work/.

Sylim, Patrick, Fang Liu, Alvin Marcelo, and Paul Fontelo, "Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention," *JMIR Research Protocols,* (9 September 2018), doi: 10.2196/10163: 10.2196/10163, http://www.researchprotocols.org.

Szabo, N. "Smart Contracts." accessed on 30 January 2019. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Tian, Nan, Aude Fleurant, Alexandra Kuimova, Pieter D. Wezeman, and Siemon T. Wezeman. "Trends in World Military Expenditure, 2017". Stockholm International Peace Research Institute. May 2018.

Tseng, Jen-Hung. Yen-Chih Liao, Bing Zhong, and Shih-Wei Liao. "Governance on the Drug Supply Chain via Gcoin Blockchain." *International Journal of Environmental Research and Public Health.* 23 May 2018.

United States Government Accountability Office. *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk*. GAO-16-236. Washington, D.C.: U.S. Government Publishing Office, 2016.

United States Government Accountability Office. *Cyber security: Actions Needed to Strengthen U.S. Capabilities.* GAO-17-440T. Washington, D.C.: U.S. Government Publishing Office, 2017.

United States Government Accountability Office, *High-Risk Series.* GAO-17-317. Washington, D.C.: U.S. Government Publishing Office, 2017.

"U.S. Air Force to Teach Blockchain Technology for Supply Chain Management." *Supply and Demand Chain Executive*. 7 December 2018. https://www.sdcexec.com/software-technology/news/21035844/us-air-force-to-teach-blockchain-technology-for-supply-chain-management.

Van Etten, Stephen R. *Cyber Supply Chain Security: Can the back door be closed with trusted design, manufacturing, and supply?* Maxwell AFB, AL: Air University Press, June 2016.

Verhoeven, Peter, Florian Sinn, and Tino T. Herden. *Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology.* Logistics 2, no. 3:20, 11 September 2018.

"What is an API? (Application Programming Interface)." *MuleSoft*. Accessed 5 February 2019. https://www.mulesoft.com/resources/api/what-is-an-api.

"What is Ethereum? The Most Comprehensive Guide Ever!" *Blockgeeks*. 12 September 2018. https://blockgeeks.com/guides/ethereum/.

Yli-Huumo, Jesse, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. *Where is current research on Blockchain Technology?—A Systematic Review*. 3 October 2016. PLoS ONE Journal, DOI:10.1371/journal.pone.0163477.

Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain Challenges and Opportunities: A Survey." *International Journal of Web and Grid Services* 14 no. 4. (2017). https://doi.org/10.1504/IJWGS.2018.095647