Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2018-12

BLOCKCHAIN TECHNOLOGY IN THE DEPARTMENT OF DEFENSE

Doskey, Teresa; Johnson, Stacylee

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/61355

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL PROJECT

BLOCKCHAIN TECHNOLOGY IN THE DEPARTMENT OF DEFENSE

December 2018

By: **Teresa Doskey**
Stacylee Johnson

Advisor: **William A. Muir**
Second Reader: **Bryan J. Hudgens**

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2018	**3. REPORT TYPE AND DATES COVERED** MBA Professional Project

4. TITLE AND SUBTITLE
BLOCKCHAIN TECHNOLOGY IN THE DEPARTMENT OF DEFENSE

5. FUNDING NUMBERS

6. AUTHOR(S) Teresa Doskey and Stacylee Johnson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

As is arguably common knowledge among defense procurement professionals, the Department of Defense (DoD) acquisitions process is slow, expensive, and inefficient. Since 1990, the Government Accountability Office (GAO) has highlighted DoD Weapons Systems Acquisition and Supply Chain Management as two high-risk areas requiring focused effort to meet cost, schedule and performance goals. Blockchain technology has the potential to advance these goals. Congress agrees. By transforming how we conduct business, the DoD can realize significant benefits from blockchain technology. Private industry is testing blockchain and offers an opportunity for the DoD to learn from established practices. This research centers on how industry is implementing blockchain technology and leads to illustrate parallels where the DoD can apply similar practices to achieve efficiencies. We aimed to do this with an analysis of specifically selected case studies in which private companies use blockchain technology to solve issues comparable to those of the DoD. Our analysis revealed common elements during the successful implementation of blockchain within the private companies. After performing the case study analysis, we discuss the findings and determine what elements appear to be relevant and potentially significant to the DoD and public procurement sector. Furthermore, we include a list of recommendations based on the trends identified during data analysis.

14. SUBJECT TERMS Blockchain, block chain, smart contracts, bitcoin, DoD acquisition, supply chain, supply-chain, air force, contracting	**15. NUMBER OF PAGES** 85
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

BLOCKCHAIN TECHNOLOGY IN THE DEPARTMENT OF DEFENSE

Teresa Doskey, Captain, United States Air Force
Stacylee Johnson, Captain, United States Air Force

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2018

Approved by: William A. Muir
Advisor

Bryan J. Hudgens
Second Reader

Rene G. Rendon
Academic Associate, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

BLOCKCHAIN TECHNOLOGY IN THE DEPARTMENT OF DEFENSE

ABSTRACT

As is arguably common knowledge among defense procurement professionals, the Department of Defense (DoD) acquisitions process is slow, expensive, and inefficient. Since 1990, the Government Accountability Office (GAO) has highlighted DoD Weapons Systems Acquisition and Supply Chain Management as two high-risk areas requiring focused effort to meet cost, schedule, and performance goals. Blockchain technology has the potential to advance these goals. Congress agrees. By transforming how we conduct business, the DoD can realize significant benefits from blockchain technology. Private industry is testing blockchain and offers an opportunity for the DoD to learn from established practices. This research centers on how industry is implementing blockchain technology and leads to illustrate parallels where the DoD can apply similar practices to achieve efficiencies. We aimed to do this with an analysis of specifically selected case studies in which private companies use blockchain technology to solve issues comparable to those of the DoD. Our analysis revealed common elements during the successful implementation of blockchain within the private companies. After performing the case study analysis, we discuss the findings and determine what elements appear to be relevant and potentially significant to the DoD and public procurement sector. Furthermore, we include a list of recommendations based on the trends identified during data analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CPARS	Contractor Performance Assessment Reporting System
DoD	Department of Defense
DAU	Defense Acquisition University
DCAA	Defense Contract Auditing Agency
DCMA	Defense Contract Management Agency
DFAS	Defense Finance Accounting System
GPC	Government purchase card
IG	Inspector General
OMB	Office of Management and Budget
PIPRS	Past Performance Information Retrieval System
SAM	System for Award Management

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank our advisors, Dr. Bill Muir and Bryan Hudgens, for their guidance and support in our research endeavors. We appreciate your trust in our unconventional area of research. Thank you to our amazing families for your love and encouragement. We are grateful for your sacrifice and willingness to hold down the fort in our absence.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Blockchain technology has garnered widespread attention spanning from congressional politicians to computer technology hobbyists. Some authors suggest that blockchain will eventually improve nearly every transaction in the economy (Tapscott & Tapscott, 2016), while others caution society to have realistic expectations of the benefits (Iansiti & Lakhani, 2017; Johansen, 2017). Regardless, one common theme emerges across the literature: Businesses and consumers must pay attention to the technology and understand that it is likely to fundamentally alter the way our world works (Jaikaran, 2018; Joint Economic Committee, 2018; Morris, Mirkovic, & O'Rourke, 2018). Just as the internet has changed the way we interact, shop, and learn, blockchain can change the way we do business, verify information, and create trust in interactions with unfamiliar people.

The key aspects of blockchain technology that provide demonstrable benefits are the distributed ledger and cryptographic hashing process (Sharma, 2018; Stevens, 2018). Distributed ledgers are present in our current environment, but they lack the security functions required for sensitive transitions (Drescher, 2017). However, when distributed ledgers are coupled with a consensus protocol using cryptographic hashing, this creates a secure, efficient, and convenient method for transacting with others (Zheng, Xie, Dai, Chen, & Wang, 2017). This new way of transacting can address issues witnessed in private procurement sectors. Companies are currently investing in blockchain technology to solve issues.

While differences exist between public and private procurement, similarities also exist, such as the need for auditability, reducing duplicative verifications, and providing transparency and traceability. Since 1990, the Government Accountability Office (GAO) has consistently highlighted weapons systems acquisitions and supply chain management as two high-risk areas requiring effort to meet cost, schedule, and performance goals (GAO, 2017a). Efforts are underway by some federal agencies in utilizing blockchain technology to improve their unique difficulties. However, the current research fails to bridge the gap between blockchain technology and the public procurement process within the DoD.

The purpose of this research is to take an in-depth look at the way industry has applied this emerging technology to improve various procurement functions, and to gauge whether specific use cases exist for DoD acquisitions. We aimed to do this with an analysis of specifically selected case studies in which private companies use blockchain technology to solve issues comparable to those of the DoD. Our analysis revealed common elements during the successful implementation of blockchain within the private companies. After performing the case study analysis, we discuss the findings and determine what elements appear to be relevant and potentially significant to the DoD and public procurement sector. Furthermore, we include a list of recommendations based on the trends identified during data analysis.

II. BACKGROUND

A. BLOCKCHAIN

As the enabling technology behind various cryptocurrencies, the interest in blockchain technology grew as a result of the drastic rise and fall in Bitcoin's valuation in 2017. Research shows that blockchain technology as a solution to issues such as cybersecurity and transaction processing found within various industries like finance, healthcare, insurance, and supply chain management without the oversight of a third-party organization (Ponemon Institute, 2017; Yli-Huumo, Ko, Choi, Park, & Smolander, 2016).

Blockchain is a technology that can fundamentally change the way we track and record transactions, information, and assets. The interworking of the technical aspects of blockchain are not vital to our discussion. Many people enjoy the benefits of a microwave, a cell phone, or the internet without a technical understanding of the micro-level operations that allow those technologies to exist (Drescher, 2017). In this chapter, we provide a high-level of explanation on the most vital elements of the technology for decision makers and users.

The basis of blockchain technology is a distributed ledger that is validated and secured through a network of peers (Sharma, 2018). (Note: In the following sections, we will define and discuss the technical terms we use in this brief overview.) Transactions become part of the blockchain after they are confirmed mathematically by the computers, or nodes, working on the blockchain platform (Sharma, 2018). Specific consensus protocols outline which, or how many, nodes must confirm the transaction prior to system acceptance (Berke, 2017). Each transaction is cryptographically hashed and contains the hashes of prior blocks plus the new information (Cachin & Vukolic, 2017). The most recent hash is a unique string of numbers and letters which is easy to verify, once solved by the computer, but computationally improbable to reverse engineered or duplicate (Berke, 2017; Peters & Panayi, 2016). Any changes in the prior verified transactions on the blockchain creates an error in the hash that the platform will not accept (Cachin & Vukolic,

2017). This unique quality creates an immutable ledger that cannot be tampered with or unknowingly altered without setting off red flags.

1. Key Aspects

The decentralized, distributed ledger and the cryptographic hashing process are two of the key aspects that make blockchain technology so powerful (Sharma, 2018). The distributed ledger and hashing process (Stevens, 2018) have existed for many years. Haber and Stornetta (1991) linked the concepts over 20 years ago in their research related to time-stamping documents. However, with the release of the Bitcoin whitepaper in 2009 (Nakamoto, 2008), which has been cited over 4,000 times on Google Scholar, and with the 2016 boom in the cryptocurrency space as measured by an influx of millions of active digital cryptocurrency wallets (Hileman & Rauchs, 2017), the power of blockchain technology emerges as an area of great potential. While we must be realistic about the advantages of blockchain, multiple potential applications for the technology exist in the government which will facilitate auditability, streamlined processes, and transparency and traceability.

a. Distributed Ledger

The concept of a ledger, or list, has existed for over 5,000 years (Schmandt-Besserat, 2014). It can contain transactions, names, book titles, contract clauses, or any number of other things. A distributed ledger is a list maintained by multiple users and not housed in a single, central location. If a person wrote a list of three names and provided a copy of that list to two other individuals, that list would essentially be distributed. If a name should be added to the ledger, the three parties would communicate, and all three people would update their ledgers to add the new name. This is the basis of distributed ledger technology—a digital form of the previous example.

Distributed ledgers are present in our current business environment. The Google docs application provides distributed documents, where multiple users can edit a document simultaneously, and updates made by one user are visible to all users. However, the distributed ledger technology of Google Docs lacks security functions required for financial, business, and other sensitive transactions (Drescher, 2017). Understandably,

financial institutions do not maintain banking records on a Google Doc. Instead, and to "manufacture" a layer of trust, transacting parties rely on intermediaries such as banks, clearinghouses, and lawyers to maintain a centralized ledger (Casey & Vigna, 2018). Transacting parties transfer trust from each other to regulated intermediaries. Society consider these intermediaries as unbiased third parties. Unfortunately, security issues are not eliminated with centralized systems. Evidence of residual vulnerabilities is exposed in media headlines on a daily basis.

While centralized systems were created to transfer trust, they are costly, timely, and vulnerable to attacks (Drescher, 2017). Additionally, housing a firm's data on servers at a single location puts that data at risk of loss from physical disasters such as fire, flood, or natural disaster. As our economy becomes more and more digital, cyber security attacks happen with greater frequency (Ponemon Institute, 2017). Companies are spending millions of dollars on protecting personal information, and hackers still gain access and compromise many customers' data. In an eight-year study (Ponemon Institute, 2017), researchers found a 27.4 percent net increase in the average number of security breaches per year over eight years. Additionally, the cost of these attacks is rising each year and accelerates past $11 million on average for a large company of 1,000 people or more (Ponemon Institute, 2017). To combat these attacks, companies make investments to deter and detect incidents, which lead to redundancies and permissioned systems which lack transparency.

However, with blockchain, the ledger is not housed in a single location with an intermediary company; it exists on each computer operating on the network. This eliminates the single location issue that is susceptible to physical compromise and reliance on third parties to maintain the security of one's personally identifiable information or sensitive details. The computers running the platform individually maintain a copy of the encrypted distributed ledger, so if one computer is damaged, the information is available from any number of other computers on the platform. Figure 1 shows the differences between a centralized ledger and a distributed ledger. An objector may argue that with information distributed to many users, security is a greater concern. However,

cryptographic hashing is the second vital element of blockchain technology, which addresses the security of information originally discussed with the distributed ledger.

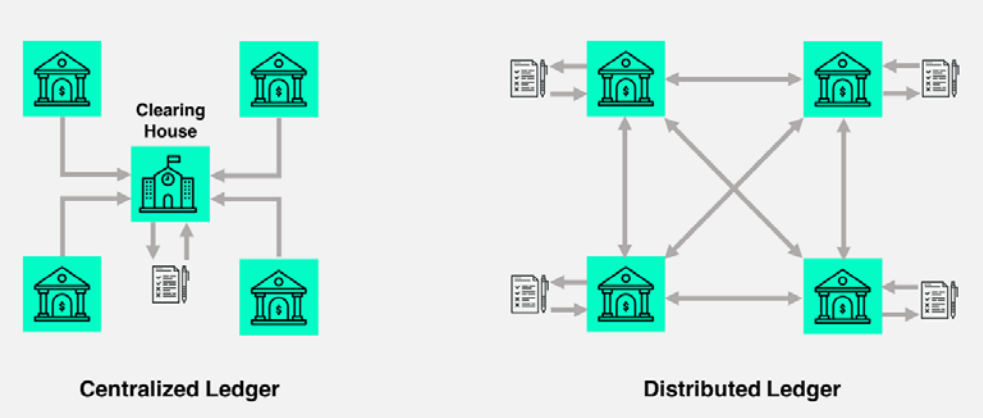

Figure 1. Centralized Ledger versus Distributed Ledger. Source: Berlin (n.d.).

b. Cryptographic Hashing

Cryptographic hashing works in tandem with the distributed ledger technology to create an instantly verifiable and immutable ledger entry (Cheng, Daub, Domeyer, & Lundqvist, 2017). Instead of maintaining the exact transaction data, the data is hashed into a specified number of alphanumeric characters. The hashing process was developed in the 1950s to sort and verify information faster (Stevens, 2018). A hashing function begins with an input of any size and returns a string of alpha-numeric characters unique to that information (Adamchick, 2009). The number of characters in the output is system-specific; Bitcoin, for example, uses 256 characters (Asolo, 2018). If the input is "Hello," the hash function returns 256 characters. Any slight change in the input, such as "Hello!" returns a completely different string of 256 characters. Carter & Wegman (1977) provide more information on the various hashing functions. Hashing is different than encryption. Encryption involves both encrypting and decrypting data, while hashing creates a unique string of alphanumeric characters of a set length regardless of the amount of data input. For example, a phone number, the previous example of "Hello," and the full text of a long book would all be hashed into different strings of exactly 256 characters.

On a blockchain, each new block contains a hash of the new information, including the prior block's hash. If an attempt is made to alter past transaction information, the current hash would become invalid because it is created from the original input (a hash of all previous hashes). The invalid hashes are not accepted during the consensus protocol, which protects the validity of the information and creates a tamper-resistant and reliable single source of truth (Miles, 2017). Nakamoto (2008) discussed the immense disk space that would be required to store the history of each and every transaction. However, by leveraging a Merkle tree,[1] as show in Figure 2, storage requirements can be drastically reduced while maintaining the integrity of the data. In Figure 2, the bottom row of boxes labeled Tx0 through Tx3 represent individual transactions, such as "Bob paid Sally 20 dollars." Regardless of the information in the transaction, whether it is a single word or a 10-page document, the transaction is hashed into the predetermined number of alphanumeric characters, represented by Hash0 in Figure 2. From there, Hash0 and Hash1 are combined and rehashed to create Hash01. In this example, combining Hash01 and Hash23 is the final step in the algorithm and becomes the root hash in the block header. Only the block header is rehashed with new transaction eliminating the need to store interior transactions (Nakamoto, 2008).

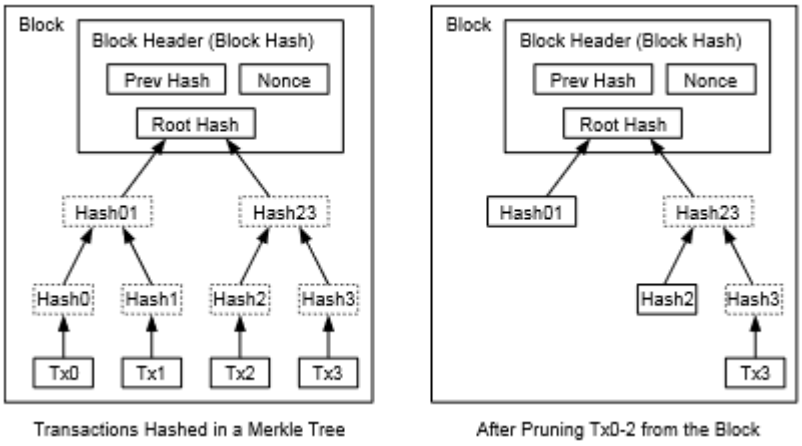

Figure 2. Hashing Process Using Merkle Trees Source: Nakamoto (2008).

[1] For more information on a Merkle tree, see Merkle (1988).

Similar to many current online transactions, blockchain leverages public and private keys to encrypt and decode data. The difference, however, is that the encrypted data is hashed, making it instantly verifiable but so immensely difficult to recreate that the cost of doing so is nearly unmeasurable. While nothing is impossible, reverse-engineering a cryptographic hash is computationally improbable (Peters & Panayi, 2016). Peters and Panayi (2016) used the term *computationally improbable* to mean "that no known algorithm can recover the input message from the hash within a time that is polynomially related to the size of the input" (p. 4). Plainly, this translates to an extraordinary amount of time.

c. Consensus Protocols

In the current business environment, interacting parties do not trust those with whom they conduct business (Williamson, 1985). In turn, organizations use intermediaries such as banks, clearinghouses, and third parties to manage business transactions. However, the use of intermediaries affects transaction costs, and transactions costs influence business decisions. Transaction costs are so significant that Williamson's 1985 research on transaction cost economics is cited nearly 50,000 times on Google Scholar. With trillions of dollars moving through the financial system each day, even a fraction of a percent in transaction costs equates to a significant amount of non–value-added spending by millions of customers. However, the integrity of each transaction is vital to firms and organizations (Tapscott & Tapscott, 2017). Without an alternative, entities are at the mercy of the intermediaries.

Blockchain technology does not use intermediaries to verify the accuracy of transactions. Instead, it uses consensus protocols to verify information that requires the network nodes to solve complex mathematical equations or cryptographic puzzles that can quickly confirm cryptographic information (Zheng et al., 2017). Such information would be nearly impossible to duplicate (Zheng et al., 2017). Once a transaction is verified by the computers operating on the network in accordance with the consensus protocol, the information is added to the blockchain and redistributed to the ledgers held by each node (Zheng et al., 2017). When combined with distributed ledger technology and cryptographic

hashing, consensus protocols create a secure, efficient, and convenient method for transacting with others (Zheng et al., 2017).

Importantly, these consensus protocols determine which nodes, or how many nodes, must agree on the correctness of information prior to acceptance by the platform. Table 1 list some of the common consensus protocols and outlines the pros and cons of each. This is not an exhausted list; the specific business problem dictates the use of the appropriate protocol. "Developing consensus protocols is difficult and should not be taken in an ad-hoc manner" (Cachin & Vukolic, 2017, p. 2).

Table 1. Common Consensus Protocols

	Pros	Cons	Examples
Proof-of-Work (PoW)	Scalable [A]	Massive energy consumption [A]	Bitcoin [B]
Proof of Stake (PoS)	Energy saving alternative to PoW [C]	Vulnerable to >51% stake [C]	Peercoin [D]
Practical Byzantine Fault Tolerance (pBFT)	ability to provide transaction finality without the need for confirmations [E]	Susceptible to Sybil attacks [E]	Hyperledger Fabric [F]
Delegated Proof of Stake (DPoS)	Speed through representative democracy [C]	Vulnerable to >51% validators [C]	Bitshares [G]

Adapted from
A Vukolic (2015)
B Nakamoto (2008)
C Zheng et al (2017)
D King & Nadal (2012)
E Curran (2018)
F Bitshares.org (2018)
G Hyperledger.org (2018).

Some protocols specify that certain individuals, perhaps a warranted contracting officer, must validate the transaction prior to the acceptance. This may provide a level of control that is appealing to the DoD, whereas platforms like Bitcoin require a percentage of users to verify the transaction (Nakamoto, 2008). Regardless, when new blocks are hashed, the past information cannot be altered without affecting the hash of all future transactions. This ensures data integrity and eliminates the need to redundantly verify information; trust is transferred to the technology. If the hash is not valid, an algorithm determines that the transaction is invalid and rejects the block or transaction (Zheng et al., 2017). The platform will not accept this information as trustworthy because the other nodes on the network identify the hash as incongruent with their version of the ledger (Peters & Panayi, 2016).

d. Smart Contracts

The blockchain can maintain records of self-executing follow-up actions to occur after the verification process (Christidis & Devetsikiotis, 2016). "If–then" conditions introduced on "smart contracts" can automate certain parts of a contractual agreement (Zhang & Wen, 2017). A widely used example of a smart contract is to compare it to a vending machine. A vending machine is programed with a set of agreements such that when the terms are met, an asset is transferred. If the price of water is one dollar, and a person inserts one dollar, the water is released.

On the blockchain, once information is verified, if the transaction occurs as part of a smart contract, and the terms of the agreement are met, the transaction automatically executes in accordance with the contract. For example, a contracting officer could write a contract on a blockchain platform. The computer would turn this into a script in the form of "if this, then that" instructions. Once the contract is executed and the parties agree that the product is delivered or the services are rendered, the predetermined and agreed upon amount transfers to the contractor without any additional effort on behalf of the contracting officer or DFAS. Figure 3 shows how this process occurs, leading to lower overhead costs and a reduced administrative burden (Marvin, 2016).

Unlike cryptocurrencies, which use an open blockchain, on a permissioned blockchain (shown in Figure 3), only specifically identified users are authorized to create or view transactions on the blockchain. A permissioned blockchain still hashes, encrypts data, and uses a decentralized ledger, but permissions may be more acceptable for transactions the government conducts. As discussed in the consensus protocol section of this report, there are benefits and drawbacks to each protocol. Determining the appropriateness of an open or permissioned blockchain is of equal importance.

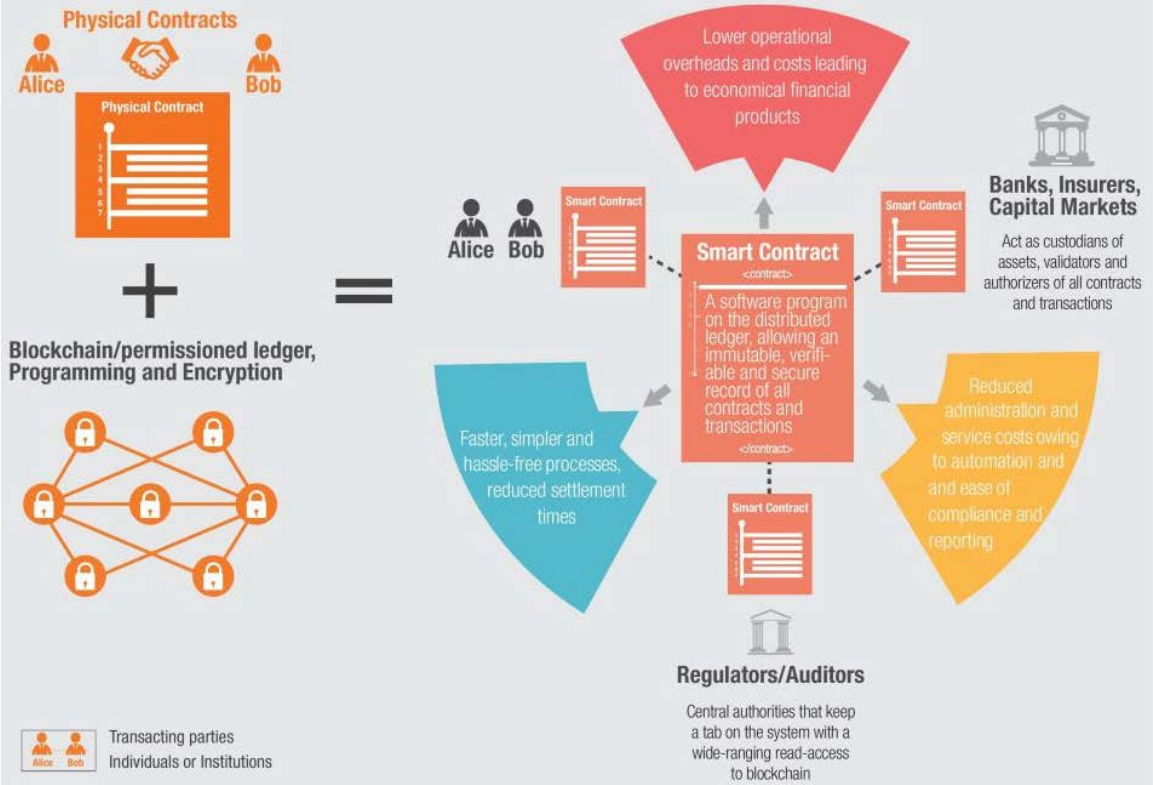

Figure 3. Smart Contract Process on a Permissioned Blockchain. Source: Marvin (2016).

2. Current Government Efforts

Cuomo, Nash, Pureswaran, Thurlow, and Zaharchuck (2017) report that nine out of 10 government executives they interviewed listed contracting management, regulatory compliance, citizen services, and identity management as the top four areas that would

benefit most from blockchain technology. Congress is formalizing the exploration of potential applications of blockchain technology through regulator direction, and governments around the world are eager to find more effective ways to conduct various operations from asset tracking to regulatory compliance to identity management.

a. Domestic Efforts

Numerous domestic government agencies are evaluating blockchain technology, but they may be far behind other nations. Chairman of the United States Commodity Futures and Trading Commission (CFTC) J. Christopher Giancarlo spoke during a session of the House Committee on Agriculture, stating that the United States is four years behind in the development of blockchain solutions as compared to major world players (*Examining the Upcoming Agenda*, 2018). We highlight two agencies to illustrate the various applications U.S. government entities are exploring. Furthermore, Table 1 lists nine additional initiatives underway in the United States, according to the state of Illinois, which oversees the Illinois Blockchain Initiative (Morris et al., 2018).

(1) United States Postal Service (USPS)

In 2016, the Office of the Inspector General for the United States Postal Service (USPS) released a report highlighting the possibility for blockchain technology to "disrupt services that traditionally require intermediaries" (p. 1) stating four applications for primary use: "financial services, identity services, device management, and supply chain management" (p. 2).

(2) Defense Advanced Research and Procurement Agency (DARPA)

In 2016, Galois and Guardtime Federal announced receipt of a $1.8 million joint contract award from the Defense Advanced Research and Procurement Agency (DARPA) to "fund a significant effort that aims to advance the state of formal verification tools and all blockchain-based integrity monitoring systems" (para. 1). Later, in 2017, Indiana Technology and Manufacturing Companies (ITAMCO) announced receipt of a grant from DARPA to build a secure and non-hackable messaging platform for use by the military.

Table 2. List of United States Federal Government Blockchain Initiatives.

Government Entity	Project Name
Department of the Navy	Blockchain to Securely Share Additive Manufacturing
Federal Reserve Bank	Distributed ledger technology in payments, learning, and settlement
General Services Administration (GSA)	Federal Blockchain Forum
Department of Energy	Small Business Innovation Research (SBIR)
Health and Human Services (HHS)—ONC	Blockchain and Its Emerging Role in Healthcare and Health-related Research
Department of Homeland Security (DHS): Science and Technology (S&T) Directorate and the Domestic Nuclear Detection Office (DNDO)	Applicability of Blockchain Technology to Privacy Respecting Identity Management
General Services Administration (GSA)	FAStLane Automation RFQ
Institute of Museum and Library Services	Investigation of Possible Uses of Blockchain Technology by Libraries-Information Centers to Support City-Community Goals
Health and Human Services (HHS)—ONC	Blockchain in Healthcare Code-A-Thon

Adapted from database referenced in Morris et al. (2018).

b. International Efforts

The international community is arguably leading the way in blockchain technology advancements and implementation. The Illinois Blockchain Initiative tracker records eight known projects in the works in China. These projects address applications such as centrally-issued currency, taxes, and national blockchain strategy. In 2016, China also created the Jiangsu Huaxin Blockchain Research Institute, which aims to radically transform the world through blockchain (Morris et al., 2018).

Likewise, in Canada, the government, various state officials, and the Bank of Canada have partnered with prominent blockchain authors, Don and Alex Tapscott, to support blockchain development through the Blockchain Research Institute (BRI, 2017). With a multi-million-dollar research program and over 70 projects, "the Blockchain Research Institute is conducting the definitive study of the impact of blockchain technology on business, government and society" (BRI, 2017, p. 1). Friend or foe, the international markets are moving forward with blockchain development.

B. DOD ACQUISITION PROCESS

The goods and services procured by both public and private sectors do not significantly differ. However, public procurement operates under certain constraints that govern contracts and the award mechanisms. Private agencies are not held to these same constraints, therefore allowing increased flexibility and efficiency advantages (Tadelis, 2012). Unlike private sector purchasing functions, the government is not driven by profit and losses. Instead, according to the FAR, the government acquisition process is driven to maintain the public's trust and fulfillment of public policy objectives, such as achieving socioeconomic goals by prioritizing small business utilization for contract award (FAR 1.102(a)).

Since 1990, the Government Accountability Office (GAO) has highlighted DoD Weapons Systems Acquisition and Supply Chain Management as two high-risk areas requiring focused effort to meet cost, schedule, and performance goals (GAO, 2017a). In addition, the GAO added DoD Contract Management to the high-risk series in 1992. From a senior leadership perspective, inefficiencies are also evident. In 2015, Senator John McCain asserted, "our broken defense acquisition system is a clear and present danger to the national security of the United States" (p. 2). While Senator McCain's comments may be considered an extreme opinion, government procurement professionals experience the inefficiencies of government contracting on a daily basis.

The DoD acquisition process is lengthy and cumbersome. Services must begin by requesting funding years in advance of the acquisition. The budget process works in a cyclical fashion where requests must be submitted 17 months before the start of the fiscal

year (Heniff, Lynch, & Tollestrup, 2012). Each service submits its budget to the Office of Management and Budget (OMB), which reviews the request and sends it back to the service for changes. Once the service returns the budget to the OMB, and after the OMB approves, the budget moves through the legislative branch and eventually is delivered to the president for signature. While overly simplified for the purpose of this chapter, even this brief description suggests that the budget approval process is lengthy and requires many levels of coordination.

Unfortunately, this process rarely happens in accordance with the expected timeline. The Pew Research Center (2018) found that Congress has passed all 12 of the appropriations necessary to fund the entire government before the end of the fiscal year on only four occasions in the last 40 years (Figure 4). The inability of Congress to approve the budget in a timely manner is the first of many substantial difficulties in the DoD's acquisition process.

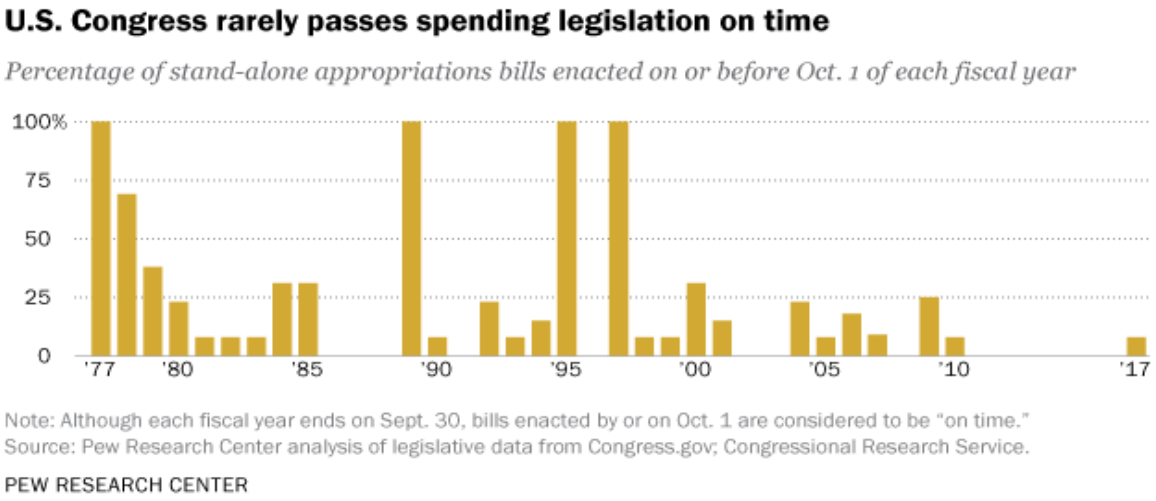

Figure 4. Percent of Appropriations Passed on Time. Source: Desilver (2018).

When the budget is approved, it contains specific restrictions regarding how to spend funds. Once the requesting unit receives the funding, there is much more to be done. Unlike private companies or in one's household, money must be spent on the product or

was allocated for the purchase (31 U.S.C. 1341; "Anti-Deficiency," 2018). Any changes to the purpose, time, or amount must be reviewed and approved by officials outside of the local requesting or purchasing unit. This process, known as reprogramming of appropriated funds, comes with its own challenges and extended timelines (Office of the Under Secretary of Defense [Comptroller; OUSD(C)], 2015).

Moreover, the government must spend the money in accordance with numerous laws and statutes. Unlike private sector purchasing functions, the government is not driven by profit and losses. Instead, according to the FAR, the government acquisition process is driven to maintain the public's trust and fulfillment of public policy objectives, such as achieving socioeconomic goals by prioritizing small business utilization for contract award (FAR 1.102(a)). Contracting officers, the personnel legally authorized to obligate the government's money through contracts, are confined by numerous federal laws, regulatory policies, DoD directives, and instructions to ensure that federal funds are equitably distributed in a way that provides the best value to the government (Wolters Kluwer, n.d.). Most of these laws were created to ensure proper stewardship of taxpayer dollars, while others exist because someone made an error (unintentionally or otherwise). Either way, contracting officers are required to comply, and ensure contractors comply, with many specific laws and statutes for even the most straightforward commodity or service purchase.

The number of charts that exist to describe the DoD's process for procuring various items is astounding. Figure 6, as an example, is a commonly used chart in the procurement of major programs or weapons systems. Figure 6 is not meant to be read; instead, it is an illustration to show the complexity of the acquisition system. The process is highly structured, consists of many steps, and leaves little flexibility or room for delays without affecting the entire timeline. Before and after award, various substantial reviews require days of preparation consisting of practice briefs, documentation edits, and justifications. For programs that are significant in cost or impact, the reviews are made by an individual of substantial rank. Therefore, the program manager (PM) or program executive officer (PEO) may require a local review prior to the official review.

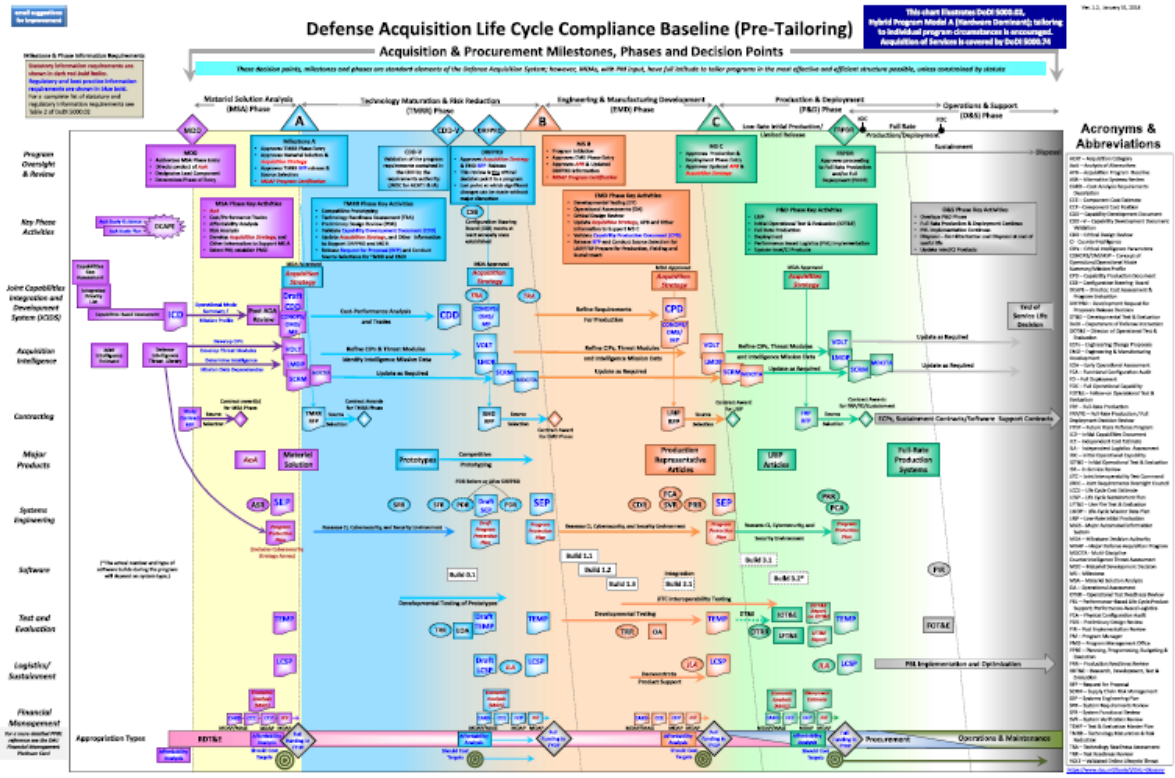

Figure 5. Defense Acquisition Life Cycle Chart. Source: Defense Acquisition University (DAU) (2018).

Moreover, the Federal Acquisition Regulations (FAR), one of many regulations contracting officers are required by law to comply with, is extensive in length and detail. Additionally, United States Title Codes, DoD- and service-specific instructions, and various other directives steer the actions of an acquisitions team member. Considerable consequences loom over signature authorities in the event that he or she diverges from any one of the required regulations. In response, duplication of effort and redundant verification take place which affects transaction costs, timely procurements, and appropriate technical performance.

C. OUR CONTRIBUTION

To the best of our knowledge, no one has analyzed the viability of a blockchain technology-based solution to address the main concerns of auditability, duplication, and traceability and transparency in the public procurement sector. The lack of research in

this area creates a gap in the specific use cases of blockchain technology. However, given the emergence of the technology and widespread interest across various domains, we aim to close this gap by analyzing three commercial firms with similar problems that implemented a blockchain solution. From this analysis, we draw conclusions and make recommendations as to the appropriateness of applying similar solutions to public sector procurement processes.

III. METHOD

The application of blockchain technology is so new to the industry that collecting data proved challenging. Our research began with a structured literature review of blockchain technology and current applications in private sector firms. To obtain the most current information, we attended the Third Annual Blockchain Conference in Washington, DC, where we heard presentations and engaged with government officials, private industry, and tech developers on the topic of blockchain. Additionally, we reviewed various government reports, Congressional hearings, and reputable news sources to identify the main issues in the DoD acquisition process. We selected three prominent issues in the procurement process that we deemed addressable by a blockchain platform. Next, we cast a wide net and searched the internet for companies that implemented blockchain solutions. We down-selected to three companies which used blockchain technology to remedy problems that best matched the significant issues identified in the DoD procurement process. We analyzed each case to gain an understanding about the firm's problem, solution, and any outcomes.

A. STRUCTURED LITERATURE REVIEW

With a potentially infinite search space, we structured a literature review to the scope of this paper. Our research is primarily focused on finding applications of blockchain-based solutions. Therefore, we bounded our search to find applied material within Google Scholar, NPS Archive Calhoun, academic and trade journals, and reputable news sources. We searched these sources using variations of primary terms such as "blockchain and supply chain," "blockchain and procurement," and "blockchain and contracting." Table 3 shows the summary of our search terms.

Table 3. Summary of Search Terms, Blockchain

Blockchain	Acquisitions	Supply Chain	Department of Defense
block chain	procurement	supply	DoD
Distributed ledger (DTL)	purchasing	smart contract (s)	government
Bitcoin	contracting	contract (s)	Federal agencies
cryptocurrency		shipping	military

During this time, we also attended the Third Annual Blockchain Conference in Washington, DC, to hear presentations from various stakeholders on the most recent applications and discussions on blockchain technology. The agenda outlining topics and presenters is attached the Appendix (Noyes, 2018).

We conducted a second search to identify the main concerns in the DoD acquisition process. The structure of this search was focused on government reports, Congressional hearings, and reputable news sources. We used variations of search terms as listed in Table 4. After collecting data on the issues in the DoD acquisition process, we briefly analyzed and arranged the problems into groups based on the primary characteristics of the root cause. Because the purpose of our research was to determine the viability of a blockchain-based solution to remedy concerns in the DoD acquisition process, we selected three main concerns that blockchain technology claims to address: auditability, duplicative verification, and traceability and transparency.

Table 4. Summary of Search Terms, Acquisition Issues

Problem	Department of Defense	Acquisitions
issue	DoD	procurement
risk	government	contracting
concern	federal	program management

B. CASE STUDY

Previously published research states the appropriateness of this method due to the nature of our topic as an exploration of the linkage between an emergent or transformative technology and existing acquisition processes. Yin (1994) states that when answering questions such as "why" or "how," a case study approach is useful. According to Eisenhardt (1989), a case study approach is

> particularly well suited to new research areas or research areas for which existing theory seems inadequate. This type of work is highly complementary to incremental theory building from normal science research. The former is useful in early stages of research on a topic or when a fresh perspective is needed, whilst the latter is useful in later stages of knowledge. (pp. 548–549)

Likewise, MacNealy (1997) and Eisenhardt (1989) state that the purpose of a case is to learn about a single, or select few, situations or events. Our research looks at three situations to gain a better understanding of the feasibility of applying blockchain technology in the DoD acquisition process.

There are common objections to the validity of using the case study method to conduct research. Hamel (1993) explains a number of issues such as a lack of objectivity and the microscopic view from looking at only a few cases. While we acknowledge the limited number of cases available for use in this research, we also apply a rigid research method governed by MacNealy (1997). Our case selection method is intentional and seeks to find examples that most likely reveal how blockchain is useful and where industry has proven the implementation of such protocols as supported by Eisenhardt (1989), Siggelkow (2007), and Flyvbjerg (2006). With this technology still in its infancy, findings on this technology are advancing at rapid speeds, and we will not be able to capture them all in this report. Additionally, the method of research does not address the development of the technology. Our research is focused on the benefits after implementation. While some scholars find objections to the case study method, significant research supports the use of it in this instance. And, as Walton (1992) stated, "case studies are likely to produce the best theory" (p. 192).

At the onset of our research, we conducted an extensive search online for blockchain in industry and found few results that did not involve cryptocurrency. However, in the last quarter of 2017 through the first quarter of 2018 when the price of Bitcoin surged and crashed, attention turned to the technology behind the currency—blockchain. In October 2017, Pham reported in a Bloomberg article that there was so much interest in blockchain technology and its promising benefits that simply adding "blockchain" to a company's name could increase the value of a firm's shares. Overstock.com saw similar results in their shares after announcing their blockchain interest (Cheng, 2017). Simultaneously, our search results began returning a number of companies who publicly announced their investment in blockchain.

We searched various terms including "blockchain technology," 'blockchain supply chain," and "blockchain traceability." We found the following companies (listed in Table 4) and noted the main problem blockchain solved for the firm. We scrutinized these sources to determine whether adequate information existed about the problem and solution implementation process. Our selection method was intentional (Patton, 2015), and an assortment of different cases may lead to a different result. However, in the case study approach, exploratory analyses are appropriate (Siggelkow, 2007).

Table 5. Blockchain Case Selection and Main Issue

Company	Problem
PricewaterhouseCoopers, LLC, Deloitte Touche Tohmatsu, Ernst & Young, and KPMG	Auditability
IBM and Maersk	Reduced duplication of paperwork, increased speed of shipping
Walmart	Transparency and traceability in the supply chain

Researchers have found that data collected during a case study analysis such as this tends to be rich in detail (Silverman, 1993; Stake, 1994; Yin, 1989). Therefore, using multiple-case study method (Yin, 2003), we structured our search around identifying commonalities and differences. We recognized that our research sought out successful examples of blockchain technology applications in industry, but we didn't know what trends would emerge. To avoid our reliance on memory throughout the research process, we collected data along the way as advised by MacNealy (1997).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS AND FINDINGS

In this chapter, we present the facts and findings of our analysis using the methods listed in Chapter III. The purpose of our research was to determine whether blockchain technology could be applied to the DoD's acquisition process to achieve a benefit. In the following sections of this chapter, we present trends in the data, commonalities, and differences that emerged over the course of our research. Importantly, we intentionally selected successful business cases as part of our method, and a different case selection may result in different findings.

A. FINDINGS FROM LITERATURE REVIEW

While various GAO reports and other regulatory compliance agencies have raised numerous concerns regarding the DoD acquisition process, based on our structured literature review, we found three prominent characteristics underlying many issues in the DoD acquisition process. These include the lack of auditability, overly duplicative verification processes, and the lack of traceability and transparency at several steps in the process.

1. Need for Auditability

Significant deficiencies are evident in how the DoD accounts for the $639 billion allocated for defense spending in 2018 (DoDaro, 2017). The DoD does not have to comply with private-sector accounting standards such as the Sarbanes-Oxley Act (SOX), which, among other things, holds senior leaders responsible for establishing and enforcing controls within a firm and requires them to certify the accuracy of financial reports. However, Congress has directed the DoD, on multiple occasions, to develop auditable records. Nearly 30 years later, the DoD is still unable to produce a trail of transactions (Grassley, 2016). In 1990, the Chief Financial Officers (CFO) Act was the first direction to create financial statements. Then in 2010, the National Defense Authorization Act (NDAA) allotted seven years for the DoD to clean up its financial records. The agency failed to do so (DoDaro, 2017).

After auditing the Fiscal Year 2016 Financial Report of the United States Government, Comptroller General of the United States, Mr. DoDaro (2017), concludes that significant concerns exist about the auditability of the federal government and the DoD specifically. In this report (GAO 17–283R), DoDaro states:

> independent public accountants (IPA) issued disclaimers of opinion for all three DoD components' [Schedule of Budgetary Activity] SBA for both of these fiscal years [2015 and 2016] and identified material weaknesses in internal control at all three DoD components. These material weaknesses included the inability to reasonably assure that the SBAs reflected all of the relevant financial transactions that occurred and that documentation was available to support such transactions. (p. 3)

GAO (2017a), a high-risk series report, states that the "DoD remains one of the few federal entities that cannot demonstrate its ability to accurately account for and reliably report its spending or assets" (p. 26). On the surface, auditability appears to be an accounting and finance issue. However, DoD funds flow through contracting officers, and since 1992, DoD Contract Management has also been cited in the GAO's high-risk series report for its inefficiencies and need for substantial reform (GAO, 2017a). The GAO's high-risk report highlights the need for increased visibility into the planned spending for contract services and greater alignment and collaboration on the highest spend categories (GAO, 2017a). Moreover, auditability and planned spending allow for analysis of opportunities within categories of spend.

The DoD website announced the commencement of the first DoD-wide official audit in 2017. Defense Department Comptroller David Norquist stated, "It is important that the Congress and the American people have confidence in DoD's management of every taxpayer dollar" (Garamone, 2017, para. 5). The scale and scope of such an audit is a massive undertaking. For the DoD alone, leaders project that approximately 1,200 auditors will be needed to complete the task. The audit announcement also reported that future audits would take place annually (Garamone, 2017).

The total amount obligated in Fiscal Year 2017 on federal contracts by the DoD is greater than all other government agencies combined (Schwartz, Sargent, & Mann, 2018). As hundreds of billions of taxpayer dollars are obligated each year, it is critical to ensure

that contract funds are not being lost or spent improperly. This requires the government to have strong controls that provide reasonable assurance of proper distribution of funds (GAO, 2011).

The federal government must transform operations in an attempt to become more easily auditable, not only to comply with the direction of Congress but to carry out its duty as a good steward of taxpayers' dollars. According to the *Acquisition Encyclopedia* ("Audits," 2018), "Congress has a vital interest in seeing that taxpayer monies are spent in accordance with applicable laws, regulations, and sound practices" (para. 2). Currently, the DoD enforces standards by conducting audits in two main areas: the acquisition process and a contract's financials ("Audits," 2018). Acquisition oversight audits focus on federal procurement and contract administration policies and regulation to analyze proper adherence to regulations. The contract audits analyze the financial and accounting elements of specific government contracts.

The governing body for both types of audits is the GAO. According to the "About" section of the GAO (n.d.) website, "GAO is an independent, nonpartisan agency of Congress" (para. 1). In a Congressional Research Service report, Gnanarajah (2017) explains the agency's mission: "GAO's mission is to support Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of taxpayers" (p. 13). Additionally, the DoD Inspector General (IG) also assists in audits including the audit for the government purchase card (GPC) program.

We spotlight the level of difficulty in auditing the GPC program. The GPC program provides federal agencies with a flexible and effective way of purchasing but also increases the need for audits to ensure compliance with decentralized spending. When not properly controlled, transactions by an authorized purchase cardholder can be a significant liability (GAO, 2008). Interestingly, according to the *Government Charge Card Guidebook*, if a purchase is made on a card and is later determined to be unauthorized, the government is still liable for the payment to the vendor (DoD, 2017). Furthermore, the government has limited centralized visibility into the specific items or categories of spending (GAO, 2016).

The secretary of the Air Force inspector general (SAF/IGQ) released a *Guide to Fraud, Waste, or Abuse Awareness* (SAF/IGQ, 2014) that specifically pointed out the GPC program as susceptible to the risk of card misuse (unintentional) and abuse (intentional). The guide draws awareness to the potential for collusion between GPC Approving Officials (AO) and cardholders to conduct unauthorized purchases as a specific example of abuse. Audits on the GPC program occur from the lowest level all the way to the DoD Inspector General (DoD IG) to identify and analyze risks of illegal, improper, or erroneous purchases and payments, and the results are reported to the director of the OMB and Congress (DoD, 2017, para. 2.2).

The GPC program operates under guidance from the undersecretary of defense for acquisition, technology and logistics (USD[AT&L]) published in the DoD's *Government Charge Card Guidebook for Establishing and Managing Purchase, Travel, and Fuel Card Programs* (DoD, 2017). The purpose of this guidance is to help DoD officials establish and implement charge card programs within their organizations. The guidance indicates many program outcomes but places specific emphasis on the following: "Management controls shall effectively identify, correct, and minimize charge card violations" (DoD, 2017, para. 1.1).

Furthermore, section 2.2.2, paragraphs (a) through (c), lists guidance that departmental programs should have the following controls to minimize losses—all annotated with a bold red "mandatory" heading (DoD, 2017):

> 1. Reviews, at a minimum annually, of all managing/billing accounts and associated cards, to identify sources of charge card violations and assess compliance with governing regulations, policies, and procedures.
>
> 2. Specific controls in place to ensure that losses due to charge card violations are minimized. The adequacy of the control environment shall be continuously assessed to ensure that controls are working as intended.

These mandatory processes indicate that there is a need to review and verify many things within the GPC program to ensure the program can support a DoD-wide audit. Depending on the extent of the items that require manual verification, this has the opportunity to take an extensive amount of time. We understand that sometimes audits are

law-driven. However, the law was developed to fix a problem and should be changed if such a problem can be fixed in another manner.

2. Duplicative Verification

From requesting funding to ensuring contractor compliance, the acquisition process is riddled with inefficiencies. The proverb "trust but verify" is frequently used in the DoD and in U.S. business. Although the origins of this phrase trace back hundreds of years, President Ronald Regan brought it into American households during his term in the White House while dealing with Russia and discussing nuclear power ("Trust but Verify," 1987). Research shows that supplier–buyer relationships improve in the presence of trust for different reasons. Enhanced relations lead to reduced transaction costs and more efficient business interactions (Gundlach & Cannon, 2010). Anderson and Weitz (1989), Ganesan (1994), and Morgan and Hunt (1994) attribute the improvement to the buyer's confidence regarding the seller's performance and the value added to the buyer by the good intentions of the seller. Likewise, some authors find that an increased amount of trust acts as a proxy in place of more formal controls (Bradach & Eccles, 1989; Gundlach, 1994; Rindfleisch & Heide, 1997).

However, trust is not inherent and presents a variety of vulnerabilities. To mitigate the risk of trusting those with whom we do business, we often use verification strategies. Gundlach and Cannon (2010) categorize these strategies as monitoring, assurance, and corroboration. While the DoD performs actions in all three classifications during the acquisition process of various goods and services, monitoring, primarily in the form of formal supplier evaluation, is the most applicable to this conversation.

Entire systems and agencies exist in the government to verify a contractor's information and performance, and to determine the eligibility of a contractor to receive a contract award. While well-intentioned acquisition personnel and suppliers feel the day-to-day pain of working in these systems, the System for Award Management (SAM), Contractor Performance Assessment System (CPARS), and the Past Performance Information Retrieval System (PIPRS) are three systems that track and manage a supplier's performance and status as a vendor. Directed by regulation to use these web-based

applications, contracting personnel and vendors must expend considerable effort to make the systems work, because they do not always work as intended. Similarly, sizeable organizations such as the Defense Contract Management Agency (DCMA), Defense Contracting Audit Agency (DCAA), and Defense Finance and Accounting Service (DFAS) exist to verify cost, price, and payment information and perform administrative actions related to ensuring compliance with contract terms.

Systems and agencies perform redundant actions—duplicating verification efforts at every step—because they lack assurance that information has not changed from one step to the next; not duplicating these efforts poses too great a risk. For example, on a commodity contract for a commercial item using Simplified Acquisition Procedures in Federal Acquisition Regulation (FAR) Parts 12 and 13, the contracting officer must verify that the contractor is registered in the System for Award Management (SAM) on two separate occasions, at a minimum, in accordance with FAR 4.11—System for Award Management and 9.4—Debarment, Suspension, and Ineligibility. In accordance with FAR 4.1103(a)(1) and 9.405, the contracting officer shall verify SAM registration and review exclusions upon receipt of the offer (or early enough in the acquisition process so a potential contractor could obtain proper registration) and immediately prior to award.

However, in reality, the contracting administrator will search SAM three times: during the market research phase to search for sources, upon receipt of an offer after solicitation, and when the award document draft is sent to the contracting officer. Additionally, the contracting officer will verify SAM twice more, once before approving the combined synopsis/solicitation to ensure sources identified in market research phase are eligible for award, and second, prior to releasing the award. According to Eisenhardt (1989), these issues relate to agency theory, whereby contractors and the government have asymmetrical information and competing objectives and will act in their own self-interest.

Short of any system outages, verifying a contractor's status in SAM only takes a few minutes. However, with multiple agencies writing hundreds of contracts each year, the amount of time spent verifying a checked box or single word compounds into a substantial amount of wasted personal hours annually. Moreover, the contractor also invests resources into maintaining the firm's SAM registration. The costs to comply with the SAM

requirement are passed onto the government. Additionally, the requirement may also reduce the supply base by increasing the perception of barriers to entry, which deter contractors from wanting to do business with the government.

One may argue that the cost of duplicating the verification process is necessary to mitigate the risk of awarding to an ineligible contractor who attempts to hide information from the government. Section 1.102 of the FAR states that one primary goal of the Federal Acquisition System is to maintain the public's trust and fulfil public policy objectives. If contracting officers fail to verify a contractor's information, they risk losing the public's trust and awarding to ineligible contractors.

3. Traceability and Transparency

The DoD IG reports in the *Summary Report of DoD Compliance with the Berry Amendment and the Buy American Act* (DoD Inspector General [DoD IG], 2018) that upon inspection of 109 contracts requiring compliance with the Berry Amendment, 40 contracts failed to comply. Additionally, upon inspection of 171 contracts requiring compliance with the Buy American Act, 41 contracts failed to adhere to the requirements of the law. The summary report included findings from four separate audits occurring between 2014 and 2017. The most common explanation for the noncompliance is attributed to unfamiliarity with the requirements of the laws. In the findings section, DoD IG (2018) stated,

> For 40 of the 109 contracts reviewed, DoD contracting personnel had limited assurance that items purchased on contracts complied with the Berry Amendment; did not notify the public of the lack of domestically-produced products; and committed potential Antideficiency Act violations by using appropriated funds to procure items not grown, reprocessed, reused, or reproduced in the United States.
>
> As a result, DoD contracting personnel had limited assurance that items purchased on contracts complied with the Buy American Act and committed potential Antideficiency Act violations by using appropriate funds to procure foreign-made items. (p. ii)

In response to the audits and prior to the release of DoD IG (2018), the president signed Executive Order No. 13788 (2017), "Buy American and Hire American," stating that every government agency shall "scrupulously monitor, enforce, and comply with Buy

American Laws" (Executive Order No. 13788, 2017). The Executive Order (No. 13788, 2017) also required agencies to include recommendations for strengthening compliance with the Buy American Act.

Evidence suggests that the DoD acquisition process needs a better way to ensure compliance. Audits are costly, but in this single case with a targeted scope, the IG found $214.2 million in contract spending that was awarded with potential Antideficiency Act violations (DoD IG, 2018). Even with multiple layers of verifications and reviews, between 24 and 36 percent of contracts in the two samples failed to comply with required laws and regulations. These findings suggest that there is room for improvement. The recommendations from the IG report include reemphasizing the existing regulations and ensuring the electronic contract writing systems are including the appropriate provisions and clauses in solicitations and contracts (DoD IG, 2018), but further guidance may be forthcoming.

In addition to the cumbersome process for simple contractor verification, before purchasing an item, the contracting officer must ensure it complies with various provisions in the solicitation. For example, many commodities require compliance with The Buy American Act to ensure items are purchased from certain countries as outlined by 41 U.S.C. § 8302. Currently, a contract manager does this through correspondence with the vendor prior to award. The government official may require proof of origin from an invoice or sales documents; however, such documents are prone to manipulation or at least require time to obtain. Furthermore, the costs of providing such documentation likely reflect in the amount charged to the government. Differently, some contracting officers simply accept a signature on the contract formalizing acceptance of the terms and conditions, including compliance with the Buy American Act.

Chapter I discusses the findings from the *Summary Report of DoD Compliance with the Berry Amendment and the Buy American Act* (DoD IG, 2018). Some contracts fail to enforce compliance because the contracting officer is inexperienced. In this instance, the contract may not contain the appropriate clauses to hold the contractor liable for compliance with such laws. With a blockchain-based platform, the government could leverage the technology by coding appropriate provisions into smart contract applications

that rely neither on the contractor's manual verification of the asset nor on the awareness of the contracting officer. Moreover, the system can instantly trace the origin of an asset provided by the contractor in the response to the request for quote (RFQ) and execute the contract only if it meets the specified "if-then" terms such as those prescribed by the Buy American Act.

B. CASE STUDIES

1. Big Four Accounting Organizations Blockchain Program

Current technology platforms offer tremendous improvements to the auditing community compared with processes from even 20 years ago. However, as demonstrated by consistent news headlines, mistakes and fraud still occurs. Therefore, publicly traded companies are required to open their books to external auditors to meet the requirements of financial regulators. It is not unlikely that a single firm could hold an immense volume of transactions on their books that require auditing. As a result, auditors often pull samples of transactions to examine, leaving the chance of missing fraudulent actions at large.

PricewaterhouseCoopers (PwC), LLC; Deloitte Touche Tohmatsu; Ernst & Young; and KPMG are the world's four largest accounting firms (Big 4 Accounting Firms, 2018). They have announced that they are joining a group of 20 banks in Taiwan to test a blockchain service for the purpose of auditing financial reports (Zhao, 2018). Zhao reports the blockchain trial will improve the process of obtaining and evaluating audit evidence by utilizing the technology to conduct external confirmations for this group of selected organizations publicly traded in Taiwan (Zhao, 2018). The developer of this particular blockchain platform, Taiwan's Financial Information Service Company (FISC), expects the new technology to streamline and automate the confirmation process through a traceable and tamper-proof chain of data, reducing the confirmation time from about 15 days to less one day (Zhao, 2018).

The Public Company Accounting Oversight Board (PCAOB), a non-profit corporation established by Congress in response to the Sarbanes-Oxley Act of 2002, charged the auditors of publicly traded organizations to plan and perform the audits necessary to obtain reasonable assurance about whether the financial statements are free of

material misstatement, whether caused by error or fraud (PCAOB, n.d.). Prior to implementation of this blockchain trial, the process of assessing audit evidence to verify the authenticity of public companies' financial transactions was completed manually (EconoTimes, 2018).

PricewaterhouseCoopers, LLC, leveraged blockchain technology with a validation solution that accommodates scalable transaction volume and provides real-time data using propriety framework to evaluate the current state of various blockchains (Panjwani, 2017). According to PwC, their "solution combines our patent-pending risk framework with our proprietary continuous auditing software. It is currently the only standard that exists for risks and controls in the blockchain space for private business blockchain processes" (PwC, 2017b). Their "blockchain risk framework" is used to identify the risk factors against six different risk categories and 100+ risk sub-categories (PwC, 2017a). The Blockchain Validation Solution Software is configured using the information gained by this framework.

The nodes within this blockchain software are set up as a "read-only" nodes to monitor and log all transactions as they occur. This allows continuous controls and testing of all transactions. PwC reports that their Blockchain Validation Solution gives stakeholders the confidence they need, due to consistent risk and validation services, to encourage innovation (PwC, 2017b).

The Big Four auditing firms place great emphasis on the external confirmation procedures as they are a critical part of their auditing process. Kevin Feng, COO of Vechain, received feedback from PwC with concerns about public blockchains, versus private blockchain, like Ethereum, due to large enterprise clients being uneasy. The concerns highlighted by Vechain are associated with the lack of having a stable governance model and the lack of economic stability (Feng & Lu, 2018). The application of a decentralized blockchain provides the ability to bypass external confirmation, hence saving time and resources. In May 2016, Deloitte established their first blockchain lab in Dublin in an effort to successfully establish blockchain initiatives. These developments are expected to reshape auditing procedures to give blockchain a more crucial role in the future of auditing.

2. Maersk International Shipping Blockchain

On May 8, 2018, there was a joint congressional hearing titled *Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods*. Oversight Subcommittee Chairman Ralph Abraham (R-LA) and Research and Technology Subcommittee Chairwoman Barbra Comstock (R-VA) heard testimony from Michael White, head of global trade digitization at Maersk, about the inefficiencies in the shipping industry. He described the number of separate but mutually dependent players who collect and verify information using disjointed and aging systems. He stressed the fact that the shipping industry suffers from redundant paperwork and verification issues which delay shipments and widely increase costs (*Leveraging Blockchain*, 2018).

Academics, industry and government have long recognized the presence of inefficiencies in supply chains. Evident by the emergence of lean production and manufacturing processes, reducing waste in the supply chain is necessary for businesses to survive in today's global market: "Non-lean practicing companies face competition from foreign made goods—competition which can have significant impacts on their business and industry" (Barac, Milovanović, & Andjelković, 2010, p. 321). Maersk Line, part of Maersk Group, a worldwide integrated transport and logistics company and key player in a number of supply chains, understands the need to streamline processes and reduce waste. Furthermore, as a common node in many supply chains, lean practices at Maersk Line have the potential to increase the efficiency of supply chains of thousands of customers.

In 2018, Maersk and IBM announced a joint venture aimed to digitize the entire shipping ecosystem using blockchain technology. Maersk, as a leader in container shipping, and IBM, as a major leader in the digital technology space and advancement of blockchain technology, have progressed the shipping environment through their use of a blockchain platform leveraging Hyperledger technologies, which are modular in nature and allow for plug-and-play applications (IBM, 2018). In 2016 and 2017, they successfully created a blockchain-based platform and conducted a pilot study to determine how effective the system was at reducing redundancies and costly paper-based tracking systems. In 2017, Maersk included the following statement in its Sustainability Report:

> Together with IBM, we have created the first two applications for this platform, one called Paperless Trade and the other targeting the Shipping Information Pipeline. The first digitizes trade documentation using blockchain technology to securely submit, stamp and approve documents for clearance and cargo movement. The second gives complete visibility of shipment events through a supply chain. The aspiration is that these two applications are just the beginning, and that other players in the supply chain develop and offer new applications based on our shared data and technologies. (p. 10)

Since the proof-of-concept project and announcement of the joint venture, other industry leaders have joined Maersk and IBM. In February 2018, Agility, a publicly traded logistics company with over $4 billion in annual revenue, announced its commitment to collaborate on the platform now known as TradeLens to manage and track shipping container operations (Port Technology, 2018). In April 2018, Holt, an independent domestic port operator in Philadelphia, announced its intentions to embark on a pilot study using the same platform (Marex, 2018). Additionally, various other domestic, international, private- and public-sector parties have commenced pilot runs leveraging the Maersk and IBM blockchain platform.

In the interim financial report for the second quarter of 2018, A.P. Møller–Mærsk A/S, the parent company of Maersk Line, reported a 24% increase in revenue and individual segment growth in all segments as compared to the same time period last year (2018). Additionally, "terminal hubs port moves per hour performance improved by 8.6% compared to Q2 2017 driven by operational synergies and initiatives materializing" (A.P. Møller–Mærsk A/S, p. 15). With increasing revenue and improved throughput at the terminal hubs, one would reasonably expect Maersk to report favorable earnings for the period. However, A.P. Møller–Mærsk A/S reported nearly a 4% decline in earnings before interest, taxes, depreciation, and amortization (EBITDA). The interim report attributes the decline in EBITDA to various causes across the conglomerate such as higher bunker costs (fuel) and negative impacts from foreign exchange rates. Specifically, the logistics and services segment of Maersk Line report "EBITDA decreased by 38% to USD 28m (USD 46m), negatively impacted by higher IT costs including continued investments in new digital solutions and customer implementations and lower profitability in inland services" (A.P. Møller–Mærsk A/S, p. 16).

A.P. Møller–Mærsk A/S recognizes that budget outlays are required for technology upgrades. Published in the annual magazine for 2016/2017, Gokcen, chief digital officer, explained in an article that A.P. Møller–Mærsk A/S is determined to lead the digital transformation in the shipping and logistics segment (Gokcen, 2017). Similarly, Bruus, head of Future Solutions, Fleet Management and Technology, Maersk Line, stated, "The short-term focus is to realise the efficiency benefits of more accurate, real-time data to optimise our operations. We expect that the impact of this data flow on our operational efficiency will be a significant positive" (Goken, p. 19).

Maersk and IBM's blockchain-based shipping platform TradeLens has grown to nearly 100 global trade participants and performed hundreds of millions of shipping events across 235 marine gateways around the world (Castillo, 2018). By using a private blockchain, Maersk and IBM are addressing the concerns of various partners about how data is seen and shared. However, private blockchains, by their very nature, negate some of the safeguards created by the decentralized operations of a public blockchain. Additionally, by developing a private blockchain platform, major competitors are likely to develop their own system instead of using TradeLens overseen and managed by Maersk and IBM. Maersk and IBM argue that using an open-source code for the key application programming interfaces of TradeLens provides space for evolutions of the platform to operate on various blockchains (King, 2018).

3. Walmart Blockchain Pilot Program

Frank Yiannas, vice president of Walmart's Food Safety Department, believes that food transparency is imperative to guard against foodborne illnesses, prevent food fraud, and ensure regulatory compliance (Nuce, Yiannas, Pradhan, & Zabrocki, 2017). In 2016, IBM introduced Walmart to blockchain technology with a proposal to improve traceability and transparency within supply chain operations (Nuce et al., 2017). The proposed platform was built on the Hyperledger Fabric as a permissioned network and operates on IBM's cloud services (Miller, 2018).

As one expert states, "[t]ransparency of a supply chain is the degree of shared understanding of and access to product-related information as requested by a supply

chain's stakeholders without loss, noise, delay, or distortion" (as cited in Hofstedel, Schepers, Spaans-Dijkstra, Trienekens, & Beulens, 2005). For this discussion, we define transparency in the supply chain as the extent to which stakeholders have access to higher-level information under the main components as explained by Trienekens, Wognum, and van der Vorst (2012). These components include information about government and consumer actors, food companies, quality and safety standards, arrangements between supply chain participants and IT systems. Egels-Zandén, Hulthén, and Wulff (2015) and Tapscott and Ticoll (2003) explained how transparency is important to all stakeholders but especially important to external stakeholders who may otherwise lack access to such details in the supply chain as compared to internal customers.

Doorey (2011) and Laudal (2010) define transparency as the ability to track a product as it flows through the system. However, in agreement with Dabbene, Gay, and Tortia (2014), we consider the ability to track a product from origin to end use through the supply chain a characteristic of traceability. Aung and Chang (2014) clarified that traceability includes access to the what, how, where, why, and when regarding an item in the supply chain.

Today's modern food supermarket is filled with tens of thousands of different options. The food system has changed drastically. In the 1980s, a typical grocery store had about 15,000 items (Nuce et al., 2017). Today, the options for consumers are almost endless regarding what consumers can purchase and where they can purchase it from. Abeyratne and Monfared (2016) expanded on this idea:

> There are billions of products being manufactured everyday globally, through complex supply chains that extend to all parts of the world. However, there is very little knowledge of how, when and where these products were originated, manufactured, and used through their life cycle. (p. 1)

Nuce et al. (2017) described the lack of transparency as a huge risk in the food supply chain. The fact that there is not enough transparency in the food system is the main vulnerability of this type of supply chain.

One of many examples of this is the E. coli outbreak from spinach in 2006. This outbreak caused 199 reported cases across 26 states that resulted in three deaths (Nuce et al., 2017). Early on, health officials said they believed it was associated with bagged spinach. Authorities advised consumers to immediately stop eating the suspect spinach and stores removed it from their shelves. It took the health officials about two weeks to find the source of that spinach (Nuce et al., 2017). In the end, it was determined the spinach that caused the outbreak came from a single lot, a single supplier, on one particular day (Nuce et al., 2017). However, stores all over the country pulled all their spinach; which resulted in lost revenue and unhappy customers for several weeks.

Today, consumers are expected to trust labeling on a product, such as it being organic or in compliance with another certification, without any way to determine whether the item complies. In many cases, the certification process depends on local factors such as in-country regulations and corrupt authorities (Elder, Zerriffi, & Le Billon, 2013).

Walmart used the mango supply chain process, starting from the farm to consumer, for their pilot blockchain program for proof of concept to enhance its ability to track and trace (Nuce et al., 2017). The first thing they did was place a package of sliced mango on the table and asked their employees to search and find out where these exact mangos came from. It took the team six days, 18 hours, and 26 minutes (Nuce et al., 2017). To put this into perspective, Walmart is considered to be faster than most with traceability—which highlights the inefficiency.

However, with use of Walmart's blockchain platform, traceability for these sliced mangos was reduced from six days and 18 hours to 2.2 seconds, or the "speed of thought" as Walmart describes it (Nuce et al., 2017). Walmart can trace each step of a single package of sliced mangos from the farm to their shelves. Figure 7 is the image Walmart used to illustrate the flow of goods at each step. This information is maintained on the blockchain platform and accessible in real time.

Figure 6. Walmart and IBM Provide Traceability in Supply Chain. Source: Galvin (2017).

In the end, Walmart's food supply chain was able to identify the source of potentially-contaminated mangos within 2.2 seconds, versus nearly seven days as was the case prior to the blockchain initiatives, and the overall benefits were overwhelming. Walmart continues to evolve this research by implementing a similar application in the pork industry in China. Not only does this system provide the potential to save lives, as in the E. coli example, but it can also reduce the amount of lost revenue by other market participants in the event of contamination. Furthermore, with blockchain, Walmart has the opportunity to increase confidence in today's food supply network.

Walmart's pilot program improved traceability within the company's supply chain. With blockchain solution, a retailer or consumer has the ability to see that a certain package of mangos came from two farms and can see the entire route of travel until the item reached the Walmart stores that sold this specific lot of mangos. Additionally, the blockchain solution showed the bottleneck of the process, which was the time it took to cross the border—four days. The platform also improves Walmart's supply chain transparency. The

new platform provides information to regarding compliance with the main concerns, such as sustainability practices and product safety standards., voiced by Trienekens et al. (2012).

Blockchain has the potential to shine a light on all nodes of a supply chain, which leads to increased accountability and greater levels of responsibility. In Nuce et al. (2017), Yiannas conveyed his belief that people typically self-govern and moderate their actions and behaviors when they are aware of transparency. Nuttavuthisit and Thøgersen (2015) stated, “Consumer trust is a key prerequisite for establishing a market for credence goods, such as ‘green’ products, especially when they are premium priced” (p. 1). In the face of business scandals and a general distrust of corporations, consumers are less willing to blindly rely on certifications for higher food standards (Choi, Eldomiaty & Kim, 2007). Therefore, transparency and traceability can provide much-needed support in the face of food fraud and consumer confidence.

THIS PAGE INTENTIONALLY LEFT BLANK

V. DISCUSSION AND RECOMMENDATIONS

In this chapter, we discuss the findings of our analysis to uncover any common threads between the three cases. We do not generalize this discussion for the application to any larger population. Instead, we intend to apply the apparent lessons learned from industry cases to the DoD acquisition process by outlining specific use cases for blockchain technology as a solution for the main concerns of auditability, duplicative verification, and traceability and transparency. As one expert notes, "[a]s with any emerging technology, it can be difficult to separate promise from probability" (Catalini, 2017, para. 2). The DoD must be realistic about the potential benefits and current maturity of this technology while focusing on the actual business problems in the acquisition system.

A. TRENDS

Based on our case study analysis of the Big Four accounting firms, Maersk, and Walmart, all three organizations are major players in their respective markets and have significant influence on industry standards. It is likely that if smaller, uninfluential companies were to drive blockchain initiatives, the utilization of blockchain would be much different. Because of the interconnectedness required for successful blockchain applications, smaller firms cannot drive change in the same way that larger firms can. As industry leaders, these companies have power over their suppliers to encourage conformity with innovation efforts such as blockchain platforms. Likewise, because large firms have many suppliers, blockchain efforts quickly gain momentum as many dependent suppliers cultivate blockchain solutions.

Although the subjects of the case studies are major market players in their respective industries, they all used joint ventures, partners, or consortiums. Each case had two distinct parties: a technology subject matter expert and an industry subject matter expert. Industry experts are familiar enough with blockchain technology to recognize its importance; still they lack the technical expertise to build a functional program. In the Big Four case study, the accounting firms had industry expertise, while FISC held the technical expertise. In the Walmart and Maersk cases, both relied on IBM for the technical expertise.

We are cautious to analyze trends in the use of a specific blockchain framework because both Walmart and Maersk used IBM, which has a preference for the Hyperledger Fabric framework. There are various blockchain frameworks to consider when developing enterprise solutions. Ethereum, for example, is widely used to support smart contract applications (Ethereum.org), while R3 Corda focuses on supporting the banking, financial services and insurance (r3.com). More research is required to analyze how an organization should select the specific framework and determine the appropriateness of a private versus public blockchain. Evidence suggest that companies currently favor private blockchains over public chains likely due to the uncertain nature of required computation power for operation, proper governance, and privacy of sensitive information (Jayachandran, 2017; Lannquist, 2018).

A major milestone in all three cases was the launch of a proof of concept, or trial run, of the platform and associated processes. This was followed by a pilot study prior to company-wide system rollout. They used the proof of concept to determine system functionality and the pilot study to obtain real-world results from the solution. The pilot studies for Maersk and Walmart both lasted approximately one year. The Big Four case study revealed that the proof of concept for the auditing solution is active but not yet complete. Furthermore, they have not started the pilot study. The individual companies of the Big Four auditing firms are, however, actively developing internal blockchain projects for future implementation.

Similar to technology advancements of the past, such as the internet and GPS, the DoD must recognize its unique vantage point in driving meaningful adoption of blockchain technology. Like the industry leaders of our research, the DoD can act as a conduit to funnel financial resources to the research and development of emerging technologies such as blockchain. Additionally, and similar to the companies in our case studies, the DoD is a major industry player. With relationships across a diverse network of suppliers, the DoD can influence widespread adoption of blockchain technology.

We agree with experts that blockchain technology is here to stay (Tapscott & Tapscott, 2016). Industry is moving forward with or without the DoD, which can cause future challenges in our defense supply base if we are not able to achieve interoperability

with industry's blockchain-based systems. The GAO cites several challenges that currently deter firms from working with the DoD, including long contracting timelines and complex processes (GAO, 2017b). Failing to stay relevant in the technology space would cause further frustrations among potential suppliers.

B. BLOCKCHAIN AS A SOLUTION

Blockchain technology enables the functionality of cryptocurrencies like Bitcoin and Ethereum. Originating in 2008, blockchain was synonymous with Bitcoin and disregarded by much of the general public (Gupta, 2017). Since then, blockchain has emerged as a foundational technology with the potential to alter the way we conduct many of our current day-to-day interactions (Iansiti & Lakhani, 2017). Bolstered by discussions in the Pentagon and direction from Congress, the concept of blockchain in the government is quickly advancing.

In the 2017 National Defense Authorization Act (NDAA), section 1646 requires the secretary of defense to brief Congress on cyber applications of blockchain technology:

> SEC. 1646. BRIEFING ON CYBER APPLICATIONS OF BLOCKCHAIN TECHNOLOGY.
>
> (a) BRIEFING REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the heads of such other departments and agencies of the Federal Government as the Secretary considers appropriate, shall provide to the appropriate committees of Congress a briefing on the cyber applications of blockchain technology.
>
> (b) ELEMENTS.—The briefing under subsection (a) shall include—
>
> (1) a description of potential offensive and defensive cyber applications of blockchain technology and other distributed database technologies;
>
> (2) an assessment of efforts by foreign powers, extremist organizations, and criminal networks to utilize such technologies;
>
> (3) an assessment of the use or planned use of such technologies by the Federal Government and critical infrastructure networks; and
>
> (4) an assessment of the vulnerabilities of critical infrastructure networks to cyber attacks.

Blockchain is not a single solution to the complex process of DoD acquisitions. However, we contend that blockchain technology has the potential to improve or solve the main concerns listed above, thereby creating efficiencies. In fact, Congress agrees. The *2018 Economic Report* (Joint Economic Committee, 2018) says, "Government agencies at all levels should consider and examine new uses for this technology [blockchain] that could make the government more efficient" (p. 226). By transforming how the DoD conducts business, the government can realize significant benefits from this technology. Furthermore, as the technology advances, the United States federal government may not have the option to shy away from blockchain. Industry, allies, and enemies are devoting extraordinary resources to expand their blockchain competencies (Morris et al., 2018).

Private-industry companies are testing the advantages of blockchain and offer an opportunity for the DoD to learn from established practices. We explored this concept using a case study evaluation approach and inspected relevant cases, which exemplified industry's successful implementation of blockchain technology to solve issues similar to those of the government acquisition process. Parallels exist where the DoD can apply similar practices to achieve efficiencies.

C. RECOMMENDATIONS

The following recommendations join the main concerns within the DoD acquisitions process, auditability, duplicative verification, traceability and transparency, with blockchain solutions. Our recommendations are based on finding a solution to known business problems. We embarked on this research with the understanding that the selected cases solved concerns similar to the ones we identified using blockchain technology. However, it is vital to recognize that an exact parallel may not be the ideal solution to remedy government or DoD specific business problems.

1. Develop Necessary Organic Capabilities

The DoD should recognize the significance of developing organic capabilities within the rapidly changing blockchain technology space. Tapscott and Tapscott (2017) recommends that leaders find this talent within the walls of the organization. At a minimum, the DoD needs to know enough to effectively manage contracts for

blockchain systems. In the era of contracting out for the majority of products and services, the DoD requires the internal capacity to properly manage any future requirement related to blockchain. Accordingly, "[g]iven the tendency to greater outsourcing and increased organizational specialization in the private sector, we expect to see those tendencies reflected in government management now and in the future" (Cohen & Eimicke, 2008, p. 15).

Evidenced by the case studies with both Maersk and Walmart, industry leaders have utilized the expertise of IBM to develop their blockchain platforms. Developing the competency that IBM currently holds would take time and resources that are not best spent allocated to these efforts. Similarly, it is in the best interest of the DoD to outsource. It is important to note, based on the law of supply and demand, when demand is high and supply is low, prices increase, and the DoD should prepare to pay a premium for blockchain engineers.

Due to the nature of blockchain based platforms, computer-centric functional areas are the appropriate lead to drive this effort. It is not necessary that every installation hold blockchain experts. Instead, using the hub concept as a model, our recommendation is to create centralized hubs to manage blockchain projects with multi-functional integrated project teams. As blockchain technology is woven into the fabric of our business processes, base level communication personnel should hold a basic understanding of the technology. This could be included in entry level technical training.

The first step is to develop a working group targeted at a specific business case such as the government purchase card program. It is critical for the working group to identify key members of the multi-functional integrated project team, such as computer engineers, program managers, contracting, and legal. This working group should be co-located and solely assigned to the development of this solution. This collaborative team will clarify the goals of the platform, develop key focus areas, and determine the way forward.

Currently, there is an increased demand and a shortage of supply for blockchain talent. According to the PwC Global Blockchain Survey (2018), 84% of 600 executives interviewed reported that their organization have at least some involvement with

blockchain technology (PwC, 2018). Similarly, Deloitte surveyed more than 1000 executives to determine where blockchain is headed. They found "74 percent of all respondents report that their organizations see a 'compelling business case' for the use of blockchain—and many of these companies are moving forward with the technology" (Deloitte, 2018, para. 3). With this increased demand, organizations are challenged by a shortage of blockchain talent (Deloitte, 2018; Marr, 2018; Upwork, 2018).

2. Government Purchase Card Pilot

A significant issue with the GPC program is that audits are necessary, costly and incomplete, which has the ability to cause powerful consequences. PwC leveraged blockchain technology with a validation solution that accommodates scalable transaction volume (Panjwani, 2017). Therefore, based on the trends found in our case study analysis, we recommend partnering with the issuing bank of the GPC and blockchain experts such as IBM or Deloitte, to develop a blockchain system for transaction processing. In addition, we recommend developing a proof of concept to determine the feasibility of the system.

On multiple occasions, Congress has directed the DoD to develop auditable records. The DoD is still struggling to produce a trail of transactions nearly 30 years later (Grassley, 2016). The GPC program provides federal agencies with a flexible and effective way of purchasing but also increases the need for audits to ensure compliance with decentralized spending. When analyzing the expected benefits found within the blockchain-based validation solution tool developed by PwC, many benefits can easily be relatable. Similar to PwC, the DoD can improve the auditing sector with the GPC program through streamlining and automating the confirmation process through a traceable and tamper-proof chain of data, reducing the confirmation time significantly (Zhao, 2018).

With a partnership between service-level leads within the communication and acquisition communities, the first step would be to create a process map that would aid in identifying the most significant issues to be addressed. Barring any major concerns from the process map, the next step would be to proceed with a pilot program with a limited number of users to obtain real-world data.

3. Procurement and Supply Chain System

The DoD labors to comply with the various laws and regulations that govern the federal acquisition process, such as the Buy American Act. This act, outlined by 41 U.S.C. § 8302, ensures items are purchased from certain countries. Currently, a contract manager uses various avenues to validate this requirement. For example, the vendor may provide proof of origin by providing an invoice or sales documents; however, such documents are prone to manipulation or at least require time to obtain. Differently, some contracting officers simply accept a signature on the contract formalizing acceptance of the terms and conditions, including compliance with the Buy American Act.

We recommend that these challenges, among others, be addressed through the creation of a blockchain-based procurement and supply chain system. This system can be look similar to the unique systems employed by Walmart and Maersk. Maersk successfully launched a blockchain-based platform and conducted a pilot study to determine how effective the system was at reducing redundancies and costly paper-based tracking systems (IBM, 2018). Walmart's blockchain system proved successful when their mango supply chain using a blockchain program improved traceability from 6 days to 2.2 seconds (Nuce et al., 2017).

Through a multifunctional system, DoD logistics and acquisitions can utilize tools developed to be interoperable and compatible from a single platform. We recommend this single system be created to complete many functions leveraging blockchain, such as smart contracts to automate compliance with various regulations and asset tracking associated with supply chain management. In efforts to address the duplicative verification of various isolated systems, such as SAM, we recommend interoperability with the ability to verify contractor responsibility.

Given the trends from our research, we recommend a partnership, preferably with an established blockchain expert such as IBM, to develop this integrated system through guidance from service-level logistics and acquisitions personnel. Using other transaction authority (OTA), the DoD can make an initial first step by contracting for a proof of concept project.

The firms we studied used a private blockchain because they experienced concerns with computational power requirements, proper governance, and privacy of sensitive information. For these reasons, we recommend operating a procurement and supply chain system on a private blockchain initially. Importantly, the application program interfaces should be modular in nature to allow a plug and play method in the face of the changing blockchain environment.

VI. CONCLUSION

A. LIMITATIONS

We are not generalizing any of our findings because supply chains differ and would benefit from a targeted analysis. Because of time constraints and access to resources, we investigated only three cases to analyze any common threads or patterns. Our case selection was intentional so that we could study organizations that used blockchain to solve problems similar to those of the acquisition process within DoD. With limited time and resources, we recognize that there are various elements to each case, which could affect the outcome of future studies.

B. FUTURE RESEARCH

The next step is to encourage a research team to consider the actual development of a blockchain platform geared towards solving a specific business problem to gain a better understanding of the technical workings of such a system. The recommendations presented in chapter five are based on the trends from our business case analysis. Because of these trends, the development of a platform would benefit from a partnership involving an expert from the business case and an expert in blockchain development

C. CONCLUSION

There are varying opinions on the degree on which blockchain will transform the current state of business interactions. While some industry players believe it will affect a wide variety of specialties such as healthcare and insurance (Tapscott & Tapscott, 2016), others see a more targeted application limited to banking and supply chain. It is important to differentiate when applying the key aspects of blockchain are excessive and when they can add value to a business process. Conversationally, presenting blockchain as a solution to everything erodes its legitimacy as a transformational technology.

After conducting a structured literature review, we elected to address the concerns of auditability, duplicative verification, and transparency and traceability in the DoD acquisition process. Simultaneously, we discovered emergent key aspects of blockchain

technology. Using a case study method, we uncovered trends between three selected business cases who are major industry players in their respective markets. While we did not use a statistically representative sample of the population, we intentionally selected cases to analyze their use of blockchain to remedy similar business problems.

Our analysis suggests that opportunities exist to apply blockchain technology to the concerns identified in the DoD procurement realm. One of our goals from our research was to further move the discussion along with blockchain technology and discuss the potential it brings to the DoD. We present specific recommendations in Chapter V based on the analysis of data collected. As a whole, this research represents an initial step toward the continued exploration of how blockchain can improve the DoD acquisition process.

APPENDIX. CONFERENCE AGENDA

3RD ANNUAL BLOCKCHAIN CONFERENCE: WASHINGTON D.C. 2018

8:00am - 9:10am – Coffee, Registration and Networking

9:10am - 9:35am – Panel 1: Blockchain Trends – 2018 & Beyond

MODERATOR – Wendy Henry, Specialist Leader – Federal Blockchain Lead, Deloitte Consulting, LLP
Theodora Lau, Founder, Unconventional Ventures
Tom Plunkett, Consulting Solutions Director, Oracle
Yannis Kalfoglou, AI and Blockchain Advisor
Fletcher McCraw, Partnership Lead, Blockchain & DLT Practice, Cognizant

9:35am - 10:20am – Company Intros 1

Calvin Wiese, CEO, Kalibrate Blockchain, Inc.
Ryan Derks, Owner, Ryans Hodl Fund
Garlam Won, Head of Global Partnership, ICONIZ – ICONIZ is an international crypto VC/Incubator based in Beijing and LA
Charles Finfrock, CEO, Crypto Charles LLC

10:25am - 10:50am – Panel 2: ICOs: The Good, The Bad & The Dangerous

Adil Wali, Founder and CEO, Merit Labs
John Wise, CEO, Loci Inc.
David Drake, Managing Partner, The Soho Loft

10:50am - 11:10am – Nikola Tesla Unite

Dean Jessop, Founding Director at Nikola Tesla United Ltd, Nikola Tesla Unite Ltd
Steve Dryall, Founding Director, Nikola Tesla Unite

11:10am - 11:25am – EverID

Bob Reid, CEO, EverID

11:30am - 11:40am – Company Intros 2

Deepak Tyagi, Founder, Artischain

11:40am - 12:00pm – FinTech Worldwide

Luis Carranza, Founder & CEO, Fintech Worldwide Ltd

12:00pm - 12:30pm – Panel 3: Regulation Update

MODERATOR – Jeff Truit, Chief Corporate Development and Legal Officer, Securrency, Inc.
Brandon Hudgeons, COO, General Counsel, Unchained Capital
Carol Van Cleef, CEO, Luminous Group, LLC

12:35pm - 1:30pm - LUNCH BREAK

1:35pm - 1:45pm – Brief Announcement

1:50pm - 2:10pm – Company Intros 3

Popo Chen, Founder, DEXON Foundation

2:15pm - 2:40pm – Panel 4: Blockchain & Government

MODERATOR – Darryn Jones, Director, Business Development, Grater Phoenix Economic Council
Chelsea Parker, Director of Operations, Blockchain Alliance
Adam Healy, CISO, Digital Asset Custody Company (DACC)
Joel Braithwaite, Partner, Cogent Law Group

2:45pm - 3:15pm – Company Intros 4

Orion Agarwal, Capital Markets Advisor, CriptoHub
Blake Richardson, CEO & Co-founder, CryptoPets
Ross Krasner, Co-founder and CEO, Ryu Blockchain Technologies

3:15pm - 3:30pm – The 2018 Bitcoin UPRISING Begins on…

Bo Polny, CEO, Gold 2020 Forecast

3:30pm - 4:00pm – Panel 5: Intellectual Property

David Holt, Principal, Fish & Richardson
Ryan Quick, Principal and Co-founder, Providentia Worldwide
Monica Talley, Director, Sterne, Kessler, Goldstein & Fox
Richard Bemben, Associate, Sterne, Kessler, Goldstein & Fox
Jon Wright, Director, Sterne, Kessler, Goldstein & Fox

3RD ANNUAL BLOCKCHAIN CONFERENCE: WASHINGTON D.C. 2018

8:00am - 9:00am – Coffee, Registration and Networking

9:00am - 9:25am – Panel 1: Investor Panel

MODERATOR – Brett Noyes, MBA, Managing Partner, Unbank.Ventures
Xiaochen Zhang, President, FinTech4Good
Alex Gostomelsky Managing Partner, Switchboard Ventures
Marshall Greenwald, CEO, Cray Pay
Reggie Middleton, CEO, Veritaseum

9:30am - 10:00am – Company Intros 1

Robert Salvador, Co-Founder & CEO, DigiBuild

10:00am - 10:15am – Security Tokens

Patrick Baron, Founder, Blockchain Consulting Group LLC

10:15am - 10:40am – Break

10:40am - 10:55am – Nikola Tesla Unite

Dean Jessop, Founding Director, Nikola Tesla Unite Ltd
Steve Dryall, Founding Director, Nikola Tesla Unite

11:00am - 11:45am – Ledger Cast

Brian Krogsgard, Owner, Under Vulcan, LLC
Josh Olszewicz, Trader, Techemy Capital Ltd

11:45am - 12:30pm – Company Intros 2

Ricky Ng, Co-Founder, iClick Interactive Asia Limited
Ray Zhang, CEO, Cointime.com

12:30pm - 1:25pm - LUNCH BREAK

1:30pm - 1:55pm – Unbank.Ventures

Brett Noyes, MBA, Managing Partner, Unbank.Ventures

2:00pm - 2:45pm – Company Intros 3

Panisa Srithong, Chief Growth Officer, BullPay
Ryan Berkun, CEO, CoinPlan

2:45pm - 3:15pm – Break

3:15pm - 3:35pm – STEMchain

George J. Awad, Founder & Executive Chairman, STEMchain

3:40pm - 5:00pm – Coffee & Networking

LIST OF REFERENCES

A.P. Møller–Mærsk A/S. (2018*). Interim financial report for Q2 2018*. Retrieved from http://investor.maersk.com/static-files/244f1309-bc54-4661-a3a4-7afc3e272626

Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, *5*(9), 1–10. Retrieved from http://doi.org/10.15623/ijret.2016.0509001

Adamchick, V. (2009). Concept of hashing. Retrieved from https://www.cs.cmu.edu/~adamchik/15-121/lectures/Hashing/hashing.html

Anderson, E., & Weitz, B. A. (1989). Determinants of continuity in conventional industrial channel dyads. *Marketing Science, 8*, 310–323.

Anti-deficiency. (2018). In *Acquisition Encyclopedia*. Retrieved from https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=aef70505-7ef4-43a0-a616-04e21ca4d5af

Asolo, B. (2018). What is SHA-256 and how is it related to Bitcoin? Retrieved from https://www.mycryptopedia.com/sha-256-related-bitcoin/

Audits. (2018). In *Acquisition Encyclopedia*. Retrieved from https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=1588d04b-34f4-4c0a-8ad0-3a6b4d5bd2d5

Aung, M. M., & Chang, Y. S. (2014). Traceability in a food supply chain: Safety and quality perspectives. *Food Control*, *39*, 172–184.

Barac, N., Milovanović, G., & Andjelković, A. (2010). Lean production and Six Sigma quality in lean supply chain management. *Economics and Organizations, 7*(3), 319–334. Retrieved from http://facta.junis.ni.ac.rs/eao/eao201003/eao201003-07.pdf

Berke, A. (2017). How safe are blockchains? It depends. *Harvard Business Review*. Retrieved from https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

Bradach, J. L., & Eccles, R. G. (1989). Price, authority, and trust. *Annual Review of Sociology, 15*, 97–118.

Berlin, O. (n.d.). The difference between blockchain and distributed ledger technology. Retrieved from https://tradeix.com/distributed-ledger-technology/

Big 4 Accounting Firms. (2018). Top 10 Accounting firms in the world 2018. Retrieved August 9, 2018, from https://big4accountingfirms.com/top-10-accounting-firms/

Bitshare.org (2018). Bitshares—your share in the decentralized exchange. Retrieved from https://bitshares.org/

Blockchain Research Institute (BRI). (2017). Retrieved from://www https.blockchainresearchinstitute.org/

Brinkmann, S. (2014). Interview. In T. Teo (Ed.), *Encyclopedia of critical psychology* (pp. 1008–1010). New York, NY: Springer.

Cachin, C., & Vukolic, M. (2017). Blockchain consensus protocols in the wild. *31st International Symposium on Distributed Computing, 1*, 1–16. doi:10.4230/LIPIcs.DISC.2017.1

Carter, J., & Wegman, M. (1977). Universal classes of hash functions. In *Proceedings of the Ninth Annual ACM Symposium on Theory of Computing* (pp. 106–112). doi:10.1145/800105.803400

Casey, M., & Vigna, P. (2018). In blockchain we trust. Retrieved from https://www.technologyreview.com/s/610781/in-blockchain-we-trust/

Castillo, M. (2018). IBM-Maersk blockchain platform adds 92 clients as part of global launch. Retrieved from https://www.forbes.com/sites/michaeldelcastillo/2018/08/09/ibm-maersk-blockchain-platform-adds-92-clients-as-part-of-global-launch-1/#4d07241b68a4

Catalini, C. (2017). Seeing beyond the blockchain hype. Retrieved from https://sloanreview.mit.edu/article/seeing-beyond-the-blockchain-hype/

Cheng, E. (2017). Overstock.com shares spike after blockchain unit announces for-profit property registry. Retrieved from https://www.cnbc.com/2017/12/13/overstock-com-spikes-after-blockchain-unit-announces-for-profit-property-registry.html

Cheng, S., Daub, M., Domeyer, A, & Lundqvist, M. (2017). Using blockchain to improve data management in the public sector. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector

Choi, C., Eldomiaty, T., & Kim, S. (2007). Consumer trust, social marketing, and ethics of welfare exchange. *Journal of Business Ethics, 74*, 17–23.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303.

Cohen, S., & Eimicke, W. (2008). *The responsible contract manager*. Washington, DC: Georgetown University Press.

Cuomo, J., Nash, R., Pureswaran, V., Thurlow, A., & Zaharchuck, D. (2017). Building trust in government: Exploring the potential of blockchains. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03801USEN

Curran, B. (2018). What is practical byzantine fault tolerance? Complete beginner's guide. Retrieved from https://blockonomi.com/practical-byzantine-fault-tolerance/

Dabbene, F., Gay, P., & Tortia, C. (2014). Traceability issues in food supply chain management: A review. *Biosystems Engineering, 120*, 65–80.

Defense Acquisition University (DAU). (2018). Interactive life cycle wall chart. Retrieved from http://acqnotes.com/wp-content/uploads/2014/09/Interactive-Life cycle-Wall-Chart-Jan-18.pdf

Deloitte. (2018). 2018 global blockchain survey. Retrieved from https://www2.deloitte.com/us/en/pages/consulting/articles/innovation-blockchain-survey.html

Department of Defense (DoD). (2017). *Government charge card guidebook for establishing and managing purchase, travel, and fuel card programs.* Retrieved from https://www.acq.osd.mil/dpap/pdi/pc/policy_documents.html

Department of Defense Inspector General (DoD IG). (2018). *Summary report of DoD compliance with the Berry Amendment and the Buy American Act* (DoDIG-2018-070). Retrieved from https://www.oversight.gov/sites/default/files/oig-reports/DODIG-2018-070.pdf

Desilver, D. (2018). Congress has long struggled to pass spending bills on time. Retrieved from http://www.pewresearch.org/fact-tank/2018/01/16/congress-has-long-struggled-to-pass-spending-bills-on-time/

DoDaro, G. (2017). *U.S. government's 2016 and 2015 consolidated financial statements* (GAO-17-283R). Washington, DC: Government Accountability Office. Retrieved from https://www.gao.gov/assets/690/682081.pdf

Doorey, D. J. (2011). The transparent supply chain: from resistance to implementation at Nike and Levi-Strauss. *Journal of Business Ethics, 103*(4), 587–603.

Drescher, D. (2017). *Blockchain basics*. Berkeley, CA: Apress. doi:10.1007/978-1-4842-2604-9.

EconoTimes. (2018, July 23). "Big Four" auditing firms to test blockchain for financial reporting in Taiwan. Retrieved from https://www.econotimes.com/Big-Four-auditing-firms-to-test-blockchain-for-financial-reporting-in-Taiwan-1406842

Egels-Zandén, N., Hulthén, K., & Wulff, G. (2015). Trade-offs in supply chain transparency: The case of Nudie Jeans Co. *Journal of Cleaner Production, 107*, 95–104.

Elder, S., Zerriffi, H., & Le Billon, P. (2013). Is Fairtrade certification greening agricultural practices? An analysis of Fairtrade environmental standards in Rwanda. *Journal of Rural Studies, 3,* 264–274. doi:10.1016/j.jrurstud.2013.07.009

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, *14*(1), 57–74.

Eisenhardt, K. (1989). Building theories from case study research. *The Academy of Management Review, 14*(4), 532–550. doi:10.2307/258557

Examining the upcoming agenda for the Commodity Futures Trading Commission: Hearing before the House Committee on Agriculture, 115th Cong. (2018) (testimony of J. Christopher Giancarlo). Retrieved from https://agriculture.house.gov/calendar/eventsingle.aspx?EventID=4416

Exec. Order No. 13788, 3 C.F.R. (2017). Retrieved from https://www.whitehouse.gov/presidential-actions/presidential-executive-order-buy-american-hire-american/

Federal Acquisition Regulation (FAR), 48 C.F.R. ch. 1 (2018).

Feng, K., & Lu, S. (2018). VechainThor, with COO Kevin Feng and CEO Sunny Lu. Retrieved from https:/www.cryptoambit.com/blog/2018/3/4/vechainthor-with-kevin-feng-and-sunny-lu

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry*, *12*(2), 219–245. doi:10.1177/1077800405284363

Galois. (2016). Galois and Guardtime Federal awarded $1.8m DARPA contract to formally verify blockchain-based integrity monitoring system. Retrieved from https://galois.com/news/galois-guardtime-formal-verification/

Galvin, D. (2017). IBM and Walmart: Blockchain for food safety [Presentation slides]. Retrieved from https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/6%20Using%20Blockchain%20for%20Food%20Safe%202/$file/6%20Using%20Blockchain%20for%20Food%20Safe%202.pdf

Ganesan, S. (1994). Determinants of long-term orientation in buyer–seller relationships. *Journal of Marketing, 58*, 1–19.

Garamone, J. (2017). Officials announce first DoD-wide audit, call for budget certainty. Retrieved from https://www.defense.gov/News/Article/Article/1391471/officials-announce-first-DoD-wide-audit-call-for-budget-certainty/

Gnanarajah, R. (2017). *Accounting and auditing regulatory structure: U.S. and international* (CRS Report No. R44894). Retrieved from Congressional Research Service website: https://fas.org/sgp/crs/misc/R44894.pdf

Gokcen, I. (2017). Welcome to the future Maersk app store. *Annual Magazine: Charting a New Direction.* Retrieved from http://investor.maersk.com/static-files/c87cebd0-6905-4eeb-b6c6-33e61e16dbe7

Government Accountability Office (GAO). (n.d.). About GAO. Retrieved from https://www.gao.gov/about/

Government Accountability Office (GAO). (2008). *Governmentwide purchase cards: Actions needed to strengthen internal controls to reduce fraudulent, improper, and abusive purchases* (GAO-08-333). Washington, DC: Author. Retrieved from https://www.gao.gov/new.items/d08333.pdf

Government Accountability Office (GAO). (2011). *Contract audits: Role in helping ensure effective oversight and reducing improper payments* (GAO-11-331). Washington, DC: Author. Retrieved from https://www.gao.gov/assets/130/125445.pdf

Government Accountability Office (GAO). (2016). *Government purchase cards: Opportunities exist to leverage buying power* (GAO-16-526). Washington, DC: Author. Retrieved from https://www.gao.gov/assets/680/677349.pdf

Government Accountability Office (GAO). (2017a). *High-risk series: Progress on many high-risk areas, while substantial efforts needed on others* (GAO-17-317). Washington, DC: Author. Retrieved from https://www.gao.gov/assets/690/682765.pdf

Government Accountability Office (GAO). (2017b). *Military acquisitions: DoD is taking steps to address challenges faced by certain companies* (GAO-17-644). Washington, DC: Author. Retrieved from https://www.gao.gov/assets/690/686525.pdf

Grassley, C. (2016, July 7). *Keeping track of the people's money may not be in the Pentagon's DNA* [Senate floor speech]. Retrieved from https://www.grassley.senate.gov/news/news-releases/grassley-pentagons-audit-readiness-remains-elusive-goal

Gundlach, G. T., & Cannon, J. P. (2010). "Trust but verify"? The performance implications of verification strategies in trusting relationships. *Journal of the Academy of Marketing Science, 38*(4), 399–417.

Gupta, V. (2017). A brief history of blockchain. *Harvard Business Review*. Retrieved from https://hbr.org/2017/02/a-brief-history-of-blockchain

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3*(2), 99–111. doi:10.1007/BF00196791

Heniff, B., Lynch, M., & Tollestrup, J. (2012). *Introduction to the federal budget process* (CRS Report No. 98–721). Retrieved from Congressional Research Service website: https://fas.org/sgp/crs/misc/98-721.pdf

Hileman, G., & Rauchs, M. (2017). *Global cryptocurrency benchmarking study*. Retrieved from University of Cambridge website: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

Hofstedel, C. J., Schepers, H., Spaans-Dijkstra, L., Trienekens, J., & Beulens, A. (2005). *Hide or confide: The dilemma of transparency*. Gravenhage, Netherlands: Reed Business Information.

Hyperledger.org. (2018). Retrieved from https://www.hyperledger.org/

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118–127.

IBM. (2018). Introducing Hyperledger fabric. Retrieved from https://www.ibm.com/blockchain/se-sv/hyperledger.html

Jaikaran, C. (2018). *Blockchain: Background and policy issues* (CRS Report No. R45116). Retrieved from Congressional Research Service website: https://fas.org/sgp/crs/misc/R45116.pdf

Jayachandran, P. (2017). The difference between public and private blockchain. Retrieved from https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Johansen, S. K. (2017). *A comprehensive literature review on the blockchain technology as a technological enabler for innovation* [Working paper]. Retrieved from https://www.researchgate.net/publication/312592741_A_Comprehensive_Literature_Review_on_the_Blockchain_Technology_as_an_Technological_Enabler_for_Innovation

Joint Economic Committee. (2018). *2018 economic report of the president* (Report No. 115–596). Washington, DC: U.S. Government Printing Office. Retrieved from https://www.congress.gov/115/crpt/hrpt596/CRPT-115hrpt596.pdf

King, L. (2018). What does Maersk-IBM's TradeLens tell us about the future of blockchain-logistics? Retrieved from https://www.joc.com/technology/what-does-maersk-ibm's-tradelens-tell-us-about-future-blockchain-logistics_20180820.html

King, S. & Nadal, S. (2012) *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake*. Self-Published Paper, August, vol. 19, 2012.

Laudal, T. (2010). An attempt to determine the CSR potential of the international clothing business. *Journal of Business Ethics*, *96*, 63–77.

Lannquist, A. (2018). Blockchain in enterprise: How companies are using blockchain today. Retrieved from https://blockchainatberkeley.blog/a-snapshot-of-blockchain-in-enterprise-d140a511e5fd?gi=3d0e4f144d65

Leveraging blockchain technology to improve supply chain management and combat counterfeit goods: Hearing before the Oversight Subcommittee and the Research and Technology Subcommittee, House of Representatives, 115th Cong. (2018). Retrieved from https://science.house.gov/legislation/hearings/subcommittee-oversight-and-subcommittee-research-and-technology-hearing-0

MacNealy, M. (1997). Toward better case study research. *IEEE Transactions on Professional Communication*, *40*(3), 182–196.

Maersk. (2017). Sustainability report. Retrieved from https://www.maersk.com/en/about/sustainability

Marex. (2018). Holt logistics joins blockchain venture. Retrieved from https://www.maritime-executive.com/article/holt-logistics-joins-blockchain-initiative#gs.tgIqqSs

Marr, B. (2018). The best blockchain jobs and careers available today. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/06/18/the-best-blockchain-jobs-and-careers-available-today/#222ec3727ca0

Marvin, R. (2016). Blockchain in 2017: The year of smart contracts. Retrieved from https://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts

McCain, J. (2015). *SASC Chairman McCain on National Defense Authorization Act.* Retrieved from https://www.mccain.senate.gov/public/index.cfm/2015/5/senate-armed-services-committee-completes-markup-of-the-national-defense-authorization-act-for-fiscal-year-2016

McDuff, C. (2017). Getting paid by DFAS [Lecture]. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjA3KSH34veAhWOLnwKHXHzAxQQFjAAegQIABAC&url=https%3A%2F%2Fwww.dfas.mil%2Fdam%2Fjcr%3Adb5bfd38-8fca-407b-b72a-13be9d3eb7b3%2FGetting%2520Paid%2520By%2520DFAS.pdf&usg=AOvVaw28hsdc4CdQAyNolv1o7URR

Merkle R.C. (1988) A digital signature based on a conventional encryption function. In: Pomerance C. (eds) Advances in Cryptology—CRYPTO '87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg doi:10.1007/3-540-48184-2_32

Miles, C. (2017). Blockchain security: What keeps your transaction data safe? Retrieved from https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

Miller, R. (2018). Walmart is betting on the blockchain to improve food safety. Retrieved from https://techcrunch.com/2018/09/24/walmart-is-betting-on-the-blockchain-to-improve-food-safety/

Morgan, R. M., & Hunt, S. D. (1994). The commitment–trust theory of relationship marketing. *Journal of Marketing, 58,* 20–38.

Morris, C., Mirkovic, J., & O'Rourke, J. (2018). *Illinois blockchain and distributed ledger taskforce: Final report to the general assembly*. Retrieved from https://www2.illinois.gov/sites/doit/Strategy/Documents/BlockchainTaskForceFinalReport020518.pdf

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System

National Defense Authorization Act for Fiscal Year 2017. (2017). Retrieved from https://www.govtrack.us/congress/bills/114/s2943/text

Noyes, B. (2018). Third Annual Blockchain Conference agenda from July 25, 2018. Presented at the Third Annual Blockchain Conference, Washington, DC.

Nuce, M., Yiannas, F., Pradhan, M., & Zabrocki, D. (2017, September 25). *Blockchain technology* [Webinar]. PWS Webinar Series. Retrieved from https://www.pma.com/content/articles/2017/09/webinar-blockchain-technology

Nuttavuthisit, K., & Thøgersen, J. (2017). The importance of consumer trust for the emergence of a market for green products: The case of organic food. *Journal of Business Ethics, 140*(2), 323–337. doi:10.1007/s10551-015-2690-5

Office of Inspector General: United States Postal Service. (2016). *Blockchain technology: Possibilities for the U.S. Postal Service* (RARC-WP-16-011). Retrieved from https://www.uspsoig.gov/sites/default/files/document-library-files/2016/RARC-WP-16-001.pdf

Office of the Under Secretary of Defense (Comptroller; OUSD[C]). (2015). Volume 3, Chapter 6: Reprogramming of DoD appropriated funds (DoD 7000.14-R). *Financial Management Regulation*. Retrieved from https://comptroller.defense.gov/Portals/45/documents/fmr/current/03/03_06.pdf

Panjwani, V. (2017). Blockchain technologies: Risks, challenges, opportunities. Retrieved from http://raw.rutgers.edu/docs/wcars/40wcars/Presentations/VikramPanjwani.pdf

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Los Angeles, CA: Sage.

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In P. Tasca, T. Aste, L. Pelizzon, & N. Perony (Eds.), *Banking beyond banks and money* (pp. 239–278). Cham, Switzerland: Springer.

Pham, L. (2017). This company added the word 'blockchain' to its name and saw its shares surge 394%. Retrieved from https://www.bloomberg.com/news/articles/2017-10-27/what-s-in-a-name-u-k-stock-surges-394-on-blockchain-rebrand

Ponemon Institute. (2017). The cost of cyber crime study. Retrieved from https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

Port Technology. (2018). Maersk–IBM blockchain JV secures first freight forwarder. Retrieved from https://www.porttechnology.org/news/first_freight_forwarder_joins_maersk_ibm_blockchain_project

PricewaterhouseCoopers (PwC). (2017a). Blockchain technologies risks, challenges, opportunities. Retrieved from http://raw.rutgers.edu/docs/wcars/40wcars/Presentations/VikramPanjwani.pdf

PricewaterhouseCoopers (PwC). (2017b). PwC blockchain validation solution. Retrieved from https://www.pwc.com/us/en/about-us/new-ventures/pwc-blockchain-validation-solution.html

PricewaterhouseCoopers (PwC). (2018). PwC global blockchain survey. Retrieved from https://www.pwc.com/blockchainsurvey

Public Company Accounting Oversight Board (PCAOB). (n.d.). About the PCAOB. Retrieved August 10, 2018, from https://pcaobus.org/About/Pages/default.aspx

Public Company Accounting Oversight Board (PCAOB). (2017). AS 1001: Responsibilities and functions of the independent auditor. Retrieved August 10, 2018, from https://pcaobus.org/Standards/Auditing/Pages/AS1001.aspx

Rindfleisch, A., & Heide, J. B. (1997). Transition cost analysis: Past, present and future applications. *Journal of Marketing, 61,* 30–54.

Schmandt-Besserat, D. (2014). *The evolution of writing.* Retrieved from https://sites.utexas.edu/dsb/tokens/the-evolution-of-writing/

Schwartz, M., Sargent, J. F., & Mann, C. T. (2018). *Defense acquisitions: How and where DoD spends its contracting dollars* (CRS Report No. R44010). Retrieved from https://fas.org/sgp/crs/natsec/R44010.pdf

Secretary of the Air Force Inspector General (SAF/IGQ). (2014). *Guide to fraud, waste, or abuse awareness*. Retrieved from https://www.af.mil/Portals/1/documents/ig/FWA_Guide_Final.pdf

Sharma, T. (2018). 5 critical components of blockchain technology. Retrieved from https://www.blockchain-council.org/blockchain/5-critical-components-of-blockchain-technology/

Siggelkow, N. (2007). Persuasion with case studies. A*cademy of Management Journal, 50*(1), 20–24.

Silverman, D. (1993). *Interpreting qualitative data: Methods for analyzing talk, text, and interaction.* Thousand Oaks, CA: Sage.

Stake, R. (1994). *Handbook of qualitative research.* Thousand Oaks, CA: Sage.

Stevens, H. (2018). Hans Peter Luhn and the birth of the hashing algorithm. Retrieved from https://spectrum.ieee.org/tech-history/silicon-revolution/hans-peter-luhn-and-the-birth-of-the-hashing-algorithm

Tadelis, S. (2012). Public procurement design: Lessons from the private sector. Retrieved from http://faculty.haas.berkeley.edu/stadelis/Pub_Proc_Des.pdf

Tapscott, A., & Tapscott, D. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. New York, NY: Penguin.

Tapscott, A., & Tapscott, D. (2017). How blockchain is changing finance. *Harvard Business Review*. Retrieved from https://hbr.org/2017/03/how-blockchain-is-changing-finance

Tapscott, D., & Ticoll, D. (2003). *The naked corporation: How the age of transparency will revolutionize business*. New York, NY: Free Press.

Trienekens, J. H., Wognum, P. M., Beulens, A. J., & van der Vorst, J. G. (2012). Transparency in complex dynamic food supply chains. *Advanced Engineering Informatics, 26*(1), 55–65.

Trust but verify. (1987, December 10). *New York Times.* Retrieved from https://www.nytimes.com/1987/12/10/opinion/trust-but-verify.html

Upwork. (2018). Upwork releases Q3 2018 Skills Index, ranking the 20 fastest-growing skills for freelancers. Retrieved from https://www.upwork.com/press/2018/11/13/q3-2018-skills/

Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security* (pp. 112–125). Springer, Cham.

Walton, J. (1992). Making the theoretical case. In C. C. Ragin & H. S. Becker (Eds.), *What is a case? Exploring the foundations of social inquiry* (pp. 121–137). Cambridge, England: Cambridge University Press.

Wolters Kluwer. (n.d.). Government contracting rules you need to know. Retrieved August 2, 2018, from https://www.bizfilings.com/toolkit/research-topics/running-your-business/government-contracting/government-contracting-rules-you-need-to-know

Williamson, O. E. (1985). *The economic institutions of capitalism: Firms, markets, relational contracting* (Vol. 866). New York, NY: Free Press.

Yin, R. (1989). *Case study research: Design and methods.* Newbury Park, CA: Sage.

Yin, R. (1994). *Case study research: Design and methods* (2nd ed.). Thousand Oaks, CA: Sage.

Yin, R. (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one, 11*(10), e0163477.

Zhao, W. (2018, July 19). All "Big Four" auditors to trial blockchain platform for financial reporting. Retrieved from https://www.coindesk.com/all-big-four-auditors-trial-blockchain-platform-for-financial-reporting/

Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the Internet of Things. *Peer-to-Peer Networking and Applications, 10*(4), 983–994.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of the Sixth IEEE International Congress on Big Data (BigData Congress)* (pp. 557–564). doi:10.1109/BigDataCongress.2017.85

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California