NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL PROJECT

APPLICATION OF BLOCKCHAIN TECHNOLOGY ON ENLISTED DETAILING PROCESS

June 2019

By: **Benjamin M. Petrisin**
Geoffrey N. Johnson

Advisor: **Amilcar A. Menichini**
Second Reader: **Chong Wang**

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2019	**3. REPORT TYPE AND DATES COVERED** MBA Professional Project

4. TITLE AND SUBTITLE
APPLICATION OF BLOCKCHAIN TECHNOLOGY ON ENLISTED DETAILING PROCESS

5. FUNDING NUMBERS

6. AUTHOR(S) Benjamin M. Petrisin and Geoffrey N. 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)

The current enlisted detailing process is completely centralized, requiring a time-intensive system to negotiate and match Sailor preferences to job gaps. The process is managed by Bureau of Naval Personnel (BUPERS) detailers through coordination with placement officers, command representatives, and the individual Sailors seeking available billets. Individual Sailor records are also maintained at BUPERS, using multiple databases. This report researches the use of blockchain technology to provide a decentralized marketplace to streamline the process while still protecting sensitive data. While this report concludes that it is entirely feasible to encode Sailor records on a blockchain ledger, further research is recommended in the form of a cost-benefit analysis (CBA) to determine whether this solution is right for BUPERS.

14. SUBJECT TERMS blockchain, detailing, marketplace, records, retention	**15. NUMBER OF PAGES** 63
	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.

APPLICATION OF BLOCKCHAIN TECHNOLOGY ON ENLISTED DETAILING PROCESS

Benjamin M. Petrisin, Lieutenant Commander, United States Navy
Geoffrey N. Johnson, Lieutenant Commander, United States Navy Reserve

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
June 2019

Approved by: Amilcar A. Menichini
Advisor

Chong Wang
Second Reader

Don E. Summers
Academic Associate, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

APPLICATION OF BLOCKCHAIN TECHNOLOGY ON ENLISTED DETAILING PROCESS

ABSTRACT

The current enlisted detailing process is completely centralized, requiring a time-intensive system to negotiate and match Sailor preferences to job gaps. The process is managed by Bureau of Naval Personnel (BUPERS) detailers through coordination with placement officers, command representatives, and the individual Sailors seeking available billets. Individual Sailor records are also maintained at BUPERS, using multiple databases. This report researches the use of blockchain technology to provide a decentralized marketplace to streamline the process while still protecting sensitive data. While this report concludes that it is entirely feasible to encode Sailor records on a blockchain ledger, further research is recommended in the form of a cost-benefit analysis (CBA) to determine whether this solution is right for BUPERS.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIP	assignment incentive pay
AQD	additional qualification designator
BBD	billet based distribution
BUPERS	Bureau of Naval Personnel
CAC	common access card
CMS-ID	Career Management System Interactive Detailing
C-WAY	career waypoints
FLTMPS	Fleet Management and Planning System
KSI	keyless signature infrastructure
NDS	National Defense Strategy
NEC	Navy enlisted classification
NFAAS	Navy Family Accountability and Assessment System
NPC	Navy Personnel Command
NSIPS	Navy Standard Integrated Personnel System
PII	personally identifiable information
PKI	public key infrastructure
PRD	projected rotation date
PRIMS	Physical Readiness Information Management System
SEAOS	soft expiration of active obligated service
SHA-256	secure hash algorithm

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to, first and foremost, thank our families for the support you have shown us. We have spent quite a bit of time away from you while working on this report. It is with the love and support from our families that we have been able to focus and succeed.

We would also like to thank our advisor, Amilcar Menichini, and second reader, Chong Wang, for your dedication and advice throughout this process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The U.S. Navy uses many different systems to store and manage personnel record information and data. These databases are used for many different reasons to include, but not limited to, detailing of Sailors, promotions, placing for special assignments, disciplinary, legal, designation and re-designation, separation from service, and statistical analysis for the Department of the Navy (DoN). This is clearly not an all-inclusive list of personnel record use within the Navy, but it highlights the importance and broad use of every Sailor's data and personal information.

The Bureau of Naval Personnel (BUPERS) is the centralized command for many of these personnel record databases. BUPERS collects and retains information on individual Sailors from a variety of systems and ways in order to manage each Sailor's career. However, not all of these different systems interact with and share data with one another, which at times, makes data collection difficult and manpower intensive. Navy enlisted detailing is one process that takes information from a variety of sources in order to place the right Sailor in the right job.

Advancements in technology are continually being made, which can be used to speed up and streamline processes such as data collection and distribution. One such advancement, which is still fairly new, is the use of blockchain technology. Blockchain is a distributed ledger housed by many different computers, or nodes, that only uses code to verify transactions and update the ledger. By decentralizing this process, transactions can occur between individuals and organizations quicker and potentially safer. It also allows the information to be more readily available. Curating and accessing multiple databases causes inefficiency for the individual Sailor and the Navy as a whole. Blockchain technology could potentially be used to streamline information and save man-hours and is already being used in many different systems to include financial, medical, supply chain management, and even government.

Blockchain technology is also structured in such a way to provide notification when tampering of information takes place. The 2015 Office of Personnel data breach is a glaring

example of a vulnerability associated with housing millions of sensitive records on a centralized server. While blockchain is not a panacea, certain aspects of the technology would have flagged malicious behavior immediately.

A. OBJECTIVE

The objective of this report is to explore if blockchain technology can be used to protect sensitive personal information, specifically within the enlisted detailing marketplace while gathering data from several personnel databases to support detailing and retention incentive decisions.

B. SCOPE AND LIMITATIONS

Blockchain technology has vast uses across both government and private sectors; however, for the purpose of this report, we will be looking at its use within the Navy's enlisted detailing process. A very important aspect of personnel data collection and use revolves around the notion of security of one's personal information. In a centralized system, control resides with the entity in charge of that system, such as BUPERS. Within a decentralized system, theoretically no one has control and security of personal information comes into question. The key question to be answered is whether blockchain technology can be used while still protecting sensitive personal data and maintaining the requisite control that BUPERS needs.

This report will also evaluate the benefits of blockchain technology compared to the current system and will explore where blockchain technologies have been used successfully in similar civilian sector applications such as medical records and the financial industry.

C. ORGANIZATION OF THE RESEARCH

This research follows a structured literature review. Following the introduction, we will explain how the current Navy enlisted detailing process works to include the different systems used, personnel and leadership involved in the process, and management of personnel records. The next chapter will provide background information on blockchain technology to include how it got started and how it works. Chapter III will involve some

discussion on Bitcoin for historical background on how blockchain technology came about and how it was used to develop Bitcoin and other cryptocurrencies. Chapter III will also discuss advantages and disadvantages of blockchain and some current uses of the technology. Chapter IV will focus on applicability within the DoN, specifically within the Navy's enlisted detailing process. Finally, Chapter V will provide a conclusion on the research as well as other possible areas of research on blockchain technology and its uses.

D. HISTORY

In 2008, Satoshi Nakamoto, a pseudonym for an individual or a group published "Bitcoin: A Peer-to-Peer Electronic Cash System." This system proposed a solution to a trusted third party and the "double spend" problem (Nakamoto, 2008). Although several of the technologies used in the Bitcoin blockchain had been developed in previous decades, Bitcoin was the first time that they had been combined to be used as a payment system or "cryptocurrency." In the decade since, an explosion in innovation in the blockchain space has taken place. However, it is still a relatively nascent technology in the public's eye, with only Bitcoin and other cryptocurrencies gaining mainstream media attention.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CURRENT DETAILING PROCESS

A. GENERAL DESCRIPTION OF "NORMAL" PROCESS

Navy enlisted detailing process is designed to meet the overall mission of the Navy while preserving the Sailor's work/life balance. Many individuals are involved in the process: Detailers, Placement Officers, command representatives, and the individual Sailor. Enlisted detailing starts with a two-sided matching process using Career Management System Interactive Detailing (CMS-ID). Both individual Sailors and representative commands are afforded the opportunity to provide their own inputs. The overall decision remains with the detailer in order to fill all required billets. Some billets are more demanding than others, but they are all necessary for the Navy to achieve its mission and promote the National Defense Strategy (NDS).

The detailing process is intended to provide a good balance between three main objectives (Navy Personnel Command [NPC], n.d.-c). The objectives are:

1. To meet the needs of the Navy
2. To maximize and advance the professional development of the individual
3. To include individual desires

Allowing the individual Sailor to provide input into the process lets their own personal and professional desires be known and considered. Representative commands provide input in order to ensure they can meet their mission within the Navy's overall mission. Placement Officers ensure all required billets that need to be filled are advertised to meet the Navy's mission. Finally, detailers try to put the right Sailor in the right job by matching qualified Sailors to all available billets while also trying to meet individual desires. Ultimately, detailers work to meet all three objectives.

The detailing process and timeline described below is summarized from the CMS-ID webpage on the NPC website (NPC, n.d.-b). The first step in the process is for the Sailor to verify whether career waypoints (C-WAY) approval is required to negotiate orders. C-WAY is the application process used for a Sailor to request and receive approval to reenlist.

C-WAY should automatically initiate an application if the Sailor has 18 months or less time from his or her soft expiration of active obligated service (SEAOS). A Sailor has up to eight opportunities to seek C-WAY approval for reenlistment starting 16 months prior to the Sailor's projected rotation date (PRD). The Sailor can submit a C-WAY application every month from 16 months prior until 9 months prior to his or her PRD.

Starting 12 months from the Sailor's PRD, he or she can begin negotiating for orders through the CMS-ID system. A Sailor will have three opportunities to negotiate his or her orders; these opportunities are known as the negotiation windows. The Sailor will have a negotiation window 12 months prior, 10 months prior, and 8 months prior to his or her PRD. If a Sailor has not successfully negotiated for orders by 6 months prior to PRD, he or she will be assigned based on the needs of the Navy.

1. Needs of the Navy

The "Needs of the Navy" is a well-known concept amongst Sailors. The Navy has certain job requirements that must be met in order to successfully meet a mission area. When a Sailor is assigned to a command, he or she is given a billet, which identifies his or her job function and duties. Each billet meets one or several job requirements that must be met by the Navy. Some billets can be more challenging than others, and some are in less desirable locations than others. Many times, detailers have difficulty in finding Sailors who possess the right qualifications and want to fill these more challenging and less desirable billets; however, every billet must be filled. When this occurs, detailers may place a Sailor in one of these challenging and less desirable billets even though the Sailor may have no interest in going there. This concept is known as "Needs of the Navy" because every billet must be filled for the Navy to meet its many different mission areas.

2. Professional Development of Individual

Every enlisted Sailor beyond E-3 must have a rating. A rating is simply a job identification, such as Culinary Specialist, Machinist Mate, Yeoman, and Electrician. Different ratings require different training as well as different amounts of training. Additionally, a Sailor does not receive job training only during the first part of his or her career. Job training is spread out over the entire course of a Sailor's career. As the Sailor

progresses up through the ranks, he or she is required to know more about his or her rating and be more proficient in the execution of his or her job.

Another aspect of a Sailor's rating proficiency is met through experience. Different positions along a Sailor's career each require a certain level of experience. Sailors also gain experience and grow professionally within their specific rating as they take on different billets and positions. This is the idea behind professional development of the individual. The Navy does not want an individual to become stagnant in his or her job and never grow in his or her rating.

Professional development is beneficial for both the individual and the Navy as a whole. It is beneficial to the individual for promotion and movement up the ranks. It is beneficial to the Navy in order to fill higher up positions that become vacant due to retirements and attrition. Overall, it is of the utmost importance to both the individual Sailor as well as the Navy for professional development to occur.

3. Individual Desires

Sailors have many different reasons for joining the Navy, and they all have many different expectations for their career path and accomplishments along the way. Some Sailors want to make the Navy a career. Some want to travel the world. Some just want to get some money for college. Often times along the way circumstances change. At some points along one's career, a Sailor may want a stable billet in order to start a family. Alternatively, maybe he or she wants a hard-working billet in order to have better chances for promotion. These different desires are what motivates each Sailor along their professional lives. It is very important for detailers to elicit input from individual Sailors because it could be the difference between keeping or losing a hardworking Sailor. It is for these reasons that the detailing process allows for individual Sailors to provide inputs into the system and to their detailers.

B. RECORDS MANAGEMENT

All official Navy personnel records are managed by and maintained at BUPERS. These records include Sailor evaluations, individual awards, educational degrees earned,

Navy enlisted classification (NEC) codes earned, and additional qualification designators (AQDs) earned. BUPERS will also maintain any other records that are pertinent to Sailor advancements, promotion and selection boards, and detailing of Sailors to billets. Some personnel information can be found on various databases as well to include but not limited to Physical Readiness Information Management System (PRIMS), Navy Standard Integrated Personnel System (NSIPS), Navy Family Accountability and Assessment System (NFAAS), and Fleet Management and Planning System (FLTMPS).

Evaluations are used in the Navy's evaluation process. Enlisted Sailors receive annual Evaluation Reports. In addition to annual reports, they are also given when Sailors depart a command, when a reporting senior departs a command, and when necessary to document a special evaluation. These evaluations are reviewed extensively for advancements and on promotion and selection boards.

Sailors also periodically receive awards for exceptional performance. These awards are traditionally given at the end of a Sailor's tour of duty or when a Sailor is instrumental in helping the command succeed in an exercise or mission. These awards can be beneficial for advancements and promotion boards.

In addition to using evaluations to review past performance and qualifications, detailers also look in a Sailor's record for education, military schooling, and training. NEC codes provide information on specific job qualifications for enlisted Sailors. AQDs provide additional qualification information, which may not be specific to a Sailor's rating, but may be necessary for a specific job. These codes along with educational background and any military schooling and specialized training can be documented in a Sailor's record at BUPERS. This information becomes necessary for a detailer to assign the right Sailor to the right job.

All of these records must be sent to BUPERS in order to be placed in a Sailor's official record. Even if a Sailor has a specific qualification or experience for a job, it cannot be used in the detailing process if it is not sent to BUPERS and scanned into the Sailor's official record. Therefore, Sailors must be very proactive in ensuring their records are always up-to-date. If a Sailor's record is not up-to-date or is missing information, he or she

must work with his or her command and BUPERS to get the missing information placed in the official record.

C. CMS-ID

According to the CMS-ID webpage on the NPC website, detailers use CMS-ID as a tool to advertise all available billets and seek inputs from individual Sailors (NPC, n.d.-b). Once a Sailor reaches 18 months before his or her PRD, he or she has specific tasks to accomplish. This period is known as the "Detailing Countdown" (NPC, n.d.-b). Starting at the 18-month mark, the Sailor is to review his or her information and ensure it is all up-to-date. This is also the point at which he or she initiates the reenlistment process using C-WAY.

At the 14-month point, the Sailor needs to submit any requests for special circumstances, such as military spouse collocation, overseas tour extension, or a PRD extension at the current command (NPC, n.d.-b). Every Sailor should be preparing to enter his or her detailing window at this point. Sailors will be given three opportunities to submit inputs for future job postings. The first window of opportunity will be at 12 months prior. The second will be at 10 months prior. The third and final negotiating window opportunity will be at 8 months prior. During each negotiating window opportunity, the Sailor will be allowed to submit up to five requests for desired jobs (NPC, n.d.-b). Throughout this process, he or she should also be communicating with his or her Command Career Counselor and chain of command regarding career goals and the available billets.

Once the Sailor reaches the 6-month point, and he or she either has not submitted desired job requests or has not been selected for any requested billet, then he or she will be assigned to a billet as per the needs of the Navy (NPC, n.d.-b). This can happen if the Sailor had requested very high demanding jobs and was not selected for any of them or if the Sailor ignored submitting inputs or did not submit up to five inputs. A Sailor can submit up to five inputs during each negotiating window, but he or she does not have to submit five (NPC, n.d.-b). Finally, at the Sailors PRD, he or she will execute the orders given whether they are for a desired job or an assigned job based on needs of the Navy.

CMS-ID also uses an application known as billet based distribution (BBD) to better match job requirements to qualified Sailors. It provides near real-time manning data to allow detailers, placement officers, and command leadership better oversight of current manning shortfalls (NPC, n.d.-b). This allows Navy leadership to ensure necessary jobs are filled to meet fleet readiness requirements.

CMS-ID is not only used by Sailors to request desired jobs, but is also used by command leadership. Command representatives can provide comments on job advertisements, which provides the detailer with more amplifying information about the job requirements. Command representatives can also review and even rank applicants (NPC, n.d.-b). They can provide comments on individual applicants, which can be useful for the detailer in selecting the right Sailor for that billet. Ranking of Sailors is on a 1-to-5 scale based on job suitability with 5 being a "best fit" and 1 being a "least fit." (NPC, n.d.-b).

D. AIP

Assignment incentive pay (AIP), as described on the AIP webpage on the NPC website, is a special pay used to incentivize Sailors to volunteer for certain jobs, which are usually quite difficult to fill (NPC, n.d.-a). These particular jobs can be hard to fill at times for a variety of reasons, such as location of the job, type of job, or even the nature of the job requirements. AIP attempts to increase the volunteer rate for these jobs, as well as increase the morale of those Sailors filling those billets and ultimately increase retention and job satisfaction.

The Navy uses an open market bid process to find qualified Sailors for these arduous jobs while trying to minimize the amount of money it has to pay to incentivize and attract Sailors to these jobs. The Navy sets a maximum bid it will accept for these jobs and allows qualified Sailors to submit a bid for the amount of AIP he or she would desire to receive in order to accept the billet (NPC, n.d.-a). Once the bidding period closes, the Navy chooses the best Sailor for the job; usually this will be the lowest bid as long as the Sailor is qualified to fill the billet. Once selected and executing the orders for the job, a Sailor will receive the amount of AIP that he or she bid (NPC, n.d.-a).

The Navy uses the maximum bid as a way to control the amount of volunteers for these hard-to-fill jobs. If the Navy is not receiving sufficient bids, it will increase the maximum bid in order to attract more Sailors. Conversely, if it is receiving too many bids, it will lower the maximum bid to control the volunteer rate.

E. SUMMARY

Navy enlisted detailing has made process improvements in recent years. The implementation of BBD has helped ensure all required billets get filled by qualified Sailors. Before BBD, commands would submit an Enlisted Distribution Verification Report monthly to BUPERS in order to verify the command's current manning and future manning requirements. BBD implementation involved software upgrades to the enlisted manning process to provide near real-time manning data (Navy Personnel Command Public Affairs, 2014). This process improvement helps maximize fleet readiness by ensuring NEC "Fit" across the fleet (NPC, n.d.-b).

"Fit" is a measurement used by all commands. Certain billets require very specific qualifications, which must be filled by a Sailor with the proper NEC code. "Fit" measures the percentage of NEC coded billets at a command that are filled with Sailors currently holding the applicable NEC code.

Another improvement in recent years was the addition of the interactive portion of CMS-ID. This process improvement helped to match the right Sailor to the right job. Individual Sailors and command representatives now have the ability to provide inputs into CMS-ID. Sailors can rank jobs in order of preference, and command leadership can provide comments and even rank candidates based on qualifications needed for the jobs (NPC, n.d.-b). This helps ensure both Sailors and commands get matched according to their preferences and desires in addition to their qualifications.

These process improvements have helped focus fleet readiness and manning efforts between fleet readiness managers, detailers, placement officers, and command leadership. However, the enlisted detailing process as well as records management is still centrally controlled at BUPERS, which requires lots of manpower to manage the fleet's manning status. According to the Enlisted Detailing website's detailer point of contact listing, most

Navy enlisted ratings have 1–5 detailers per rating (NPC, n.d.-c). This shows the detailing process as being very manpower intensive.

III. BLOCKCHAIN TECHNOLOGY

A. HOW DID IT GET STARTED?

In 2008, an individual or entity under the pseudonym "Satoshi Nakamoto" published a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." The purpose of this new technology, as the title implies, is a means of electronic cash transfer between two parties without an intermediary. Bitcoin, also referred to as a "crypto-currency," uses an underlying decentralized and distributed ledger technology known as blockchain in order to operate. The terms Bitcoin and blockchain are sometimes used interchangeably, but in reality blockchain is a general term for the underlying technology that allows Bitcoin to work. Although some of the different aspects of blockchain technology have been around for decades, (namely a peer-to-peer network, cryptographic hashing, and an incentive structure), Nakamoto was the first one to combine them in a meaningful way to achieve a means of value transfer based on code instead of trust. Essentially, the Bitcoin blockchain is an ever-expanding database containing all of the transactions that have ever occurred on the network as well as an account of how many Bitcoins each public address or "wallet" owns. Although the "traditional" internet has become increasingly centralized by tech behemoths like Google, Amazon, and Facebook with warehouses of servers, Bitcoin works on the premise of decentralized nodes (computers) running computations to verify and store transactions on its ledger. (See Figure 1.) Because there is no centralized authority with an incentive to keep their database up to date and collect profit from customers, individuals who devote computing power to the blockchain are incentivized to do so by receiving newly created Bitcoins each time a new block is added to the chain (Nakamoto, 2008). Decentralization also allows nodes to join or leave the blockchain at will, with little to no effect on the network execution. While theoretically, Google's data can be lost by eliminating its servers, the Bitcoin blockchain cannot be eliminated unless the entire internet itself is shut down.

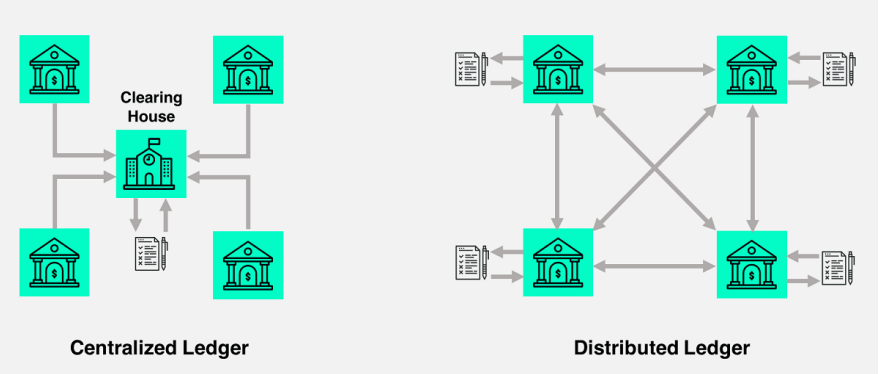

Figure 1. Centralized versus Distributed Ledger. Source: Belin (n.d.).

B. HOW IS IT USED TODAY?

The first and arguably only prominent use case of this technology so far is that of transferring value between two parties without a financial institution to verify the transaction. In this way, it is a "trustless" system. The recipient of a transaction does not need to place trust in the sender or in an intermediary to ensure the sender actually has them. Currently, the trust-based model used by most financial institutions to transfer funds requires that a third party, such as a bank, mediate a transaction between two parties in order to resolve disputes and reverse transactions if the need arises. To accomplish this, banks must gather personally identifiable information (PII) from their customers, who in turn must rely on the banks to secure said information. The bank will also prevent the payer from double spending the funds by combing through each transaction to ensure that not more money is spent than the person actually has on hand. Banks spend time and resources doing this accounting because it is profitable; they make money on transaction fees and on deploying their customer's capital to other parties as loans or investments (Nakamoto, 2008). Additionally, the customer must trust that the bank actually has the funds on hand, should he want to withdraw them. Most banks practice fractional reserve banking, in which they are allowed to lend a multiple of the funds that are held in reserve. For example, banks with accounts of over $124.2 million are required to hold ten percent of deposits as cash on hand meaning they can lend out the other ninety percent (Board of Governors of the Federal Reserve System, n.d.). In essence, these funds are created out of thin air and a bank run could quickly escalate into a catastrophe. In contrast, the Bitcoin blockchain is

immutable, meaning it is unchangeable and only a certain amount of coins will ever be "minted." The blockchain also prevents the double-spending problem by cryptographically proving that the payer has the funds for the payment, based upon the longest available ledger that is agreed upon by the majority of participating nodes. The Bitcoin blockchain is public and transparent so that every node can see every transaction. In this way, nodes can verify the earliest transaction of a particular payer to verify the funds available to that account. Instead of a central authority verifying which transaction came first, the blockchain uses a timestamp server and a "proof of work" algorithm.

C. HOW DOES IT WORK?

Blockchain technology involves a concept called proof of work in which transactions can be validated in a decentralized network. The technology is based on mining (to be explained in Section 3) to build the blockchain.

1. Proof of Work

Proof of work is a consensus mechanism that ensures that all of the participating nodes on the blockchain agree on the validity of the transactions in each block. In order to propagate the network and keep it secure, an incentive structure was put in place to ensure that computers or "miners" (computers solving complex algorithms; to be explained in Section 3) would use the electricity and computing power to do so. The reward for mining is paid out in the form of newly created Bitcoins (Frankenfield, 2018). The blockchain is an ever-expanding ledger in which new blocks are created by a process known as cryptographic hashing (to be explained in Section 2). The "block" is created approximately every ten minutes and contains transactions from the network that are stored in a transaction pool or "mempool," while waiting to be added to a block. Each block is mathematically linked to the one before and after it creating a chain, hence the name. For Bitcoin, cryptographic hashing serves two functions:

- To consolidate all of the data from a block including transactions into one hash function output known as a Merkle Root (to be explained in Section

4) which is then included in the next block to link the two. (This also provides security, which will be discussed in Section 2.)

- To facilitate proof of work by incentivizing miners to solve a mathematically difficult problem and thus receive the "block reward," a predetermined number of Bitcoins. Both are accomplished using the Secure Hash Algorithm or SHA-256 (Tech Terms, n.d.).

2. Hashing

Hashing is a function that takes an input of any length and produces an output of a fixed length. It is a common cryptography tool that has several properties that are useful in blockchain:

- The input of a hash can be any length from a single character to all of the information on the internet, (Lisk Academy, n.d.) and the output of the hash will always be a fixed length string of characters (64 characters in the case of SHA-256) unique to that input.

- The "non-collision" property of SHA-256 means that no two input values will produce the same output value hash. Even changing one character of the input will completely change the output (Learningspot, 2016). (See Table 1.)

Table 1. SHA-256 Hash Function. Source: Passwords Generator (n.d.).

Input	Hash
hello	2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
Hello	185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

This property provides security to the network because any malicious actor wishing to change information in a block would change the Merkle Root or hash header of that block which would change the linked subsequent blocks in the chain. This change would be rejected by the miners.

- The pre-image resistance property of hashing means that knowing the hash output will not let you identify the input, however once an output is achieved it is simple to determine if it is correct. This feature is important when discussing mining.

3. Mining

As mentioned in Section 1, the Bitcoin network is propagated and secured through a process colloquially known as mining. Mining takes the same cryptographic hashing technique used to consolidate transactions into a single hash output and instead directs it towards solving a target value set by the Bitcoin network with a difficulty ensuring that the target is achieved approximately every 10 minutes thus creating a new block (Hong, 2019). This is done through brute force by the computers attempting to find a target hash output by systematically adding an integer known as a "nonce" to the input string. Recall that the pre-image resistance property of hashing means that given an output it is infeasible to determine the input. This means to get the target hash output the miners have to check each input one by one until they come up with the correct one. The target value is an output hash with a pre-determined leading number of zeros (Hong, 2019). The miners will start by attaching the number one to the input string and then check to see if the resultant output hash has the correct number of leading zeros. If it does not, then the number two will be attached and tried again until the correct number of leading zeros is hit on the output hash. Figure 2 illustrates this concept.

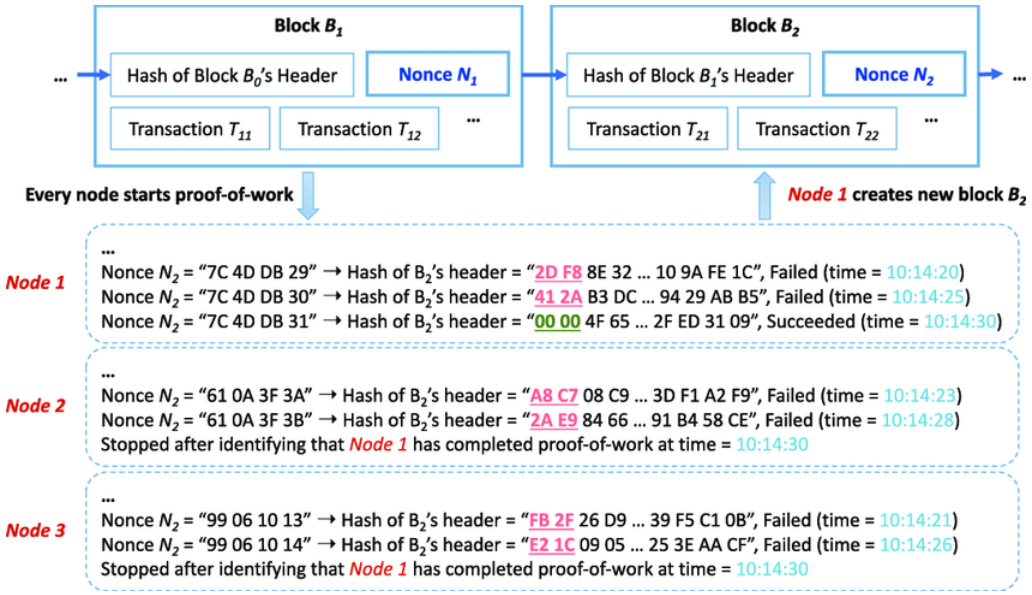

Figure 2. An Example of the Nonce Mechanism. Source: Kim, Kuo, & Ohno-Machado (2017).

Each zero added to the target output hash exponentially increases the difficulty of the problem. For example, if the leading number of zeros on the target output hash is too low meaning a new block is found in less than ten minutes, the network will increase the difficulty by increasing the leading number of zeros on the target. The more computing power added to the network, the quicker it takes to find the target and subsequently the higher the difficulty threshold is set to achieve the target time of ten minutes. Miners are incentivized to spend the computational power and electricity needed to complete the hashes by getting rewarded Bitcoins when solving a block. The reward for solving a block is decreased on a set schedule according to a "halving" process every 210,000 blocks. The reward started at 50 Bitcoins per block and is currently 12.5 Bitcoins per block (Hong, 2019). Due to the incredibly high hash rate and the improbability of a single, discrete computer solving the hash, rewards are usually split among "mining pools," that is many computers splitting the computational workload with the promise of gaining a fraction of the rewarded Bitcoins.

4. Merkle Trees

Merkle Trees are used within the Bitcoin Network in order to decrease the data size of the blocks. Patented by Ralph Merkle, the tree is a way to compress the data so that the leaves of the tree are hashed to become the branches, which are subsequently hashed to become the trunk (Merkle, 1988). Figure 3 is a visual representation of the concept.

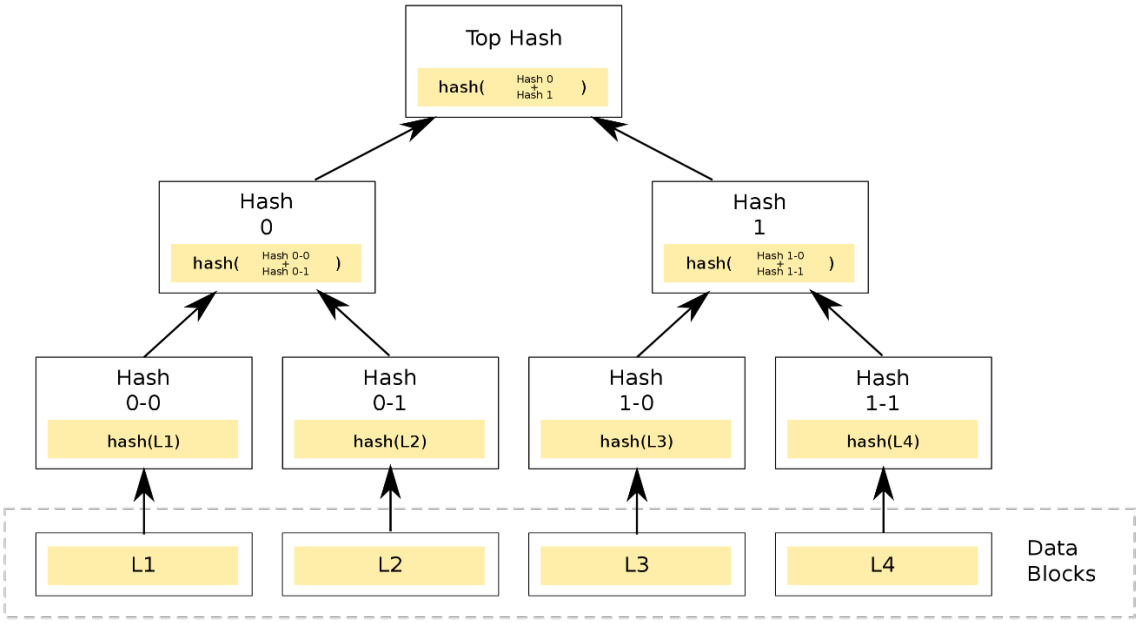

Figure 3. Example Merkle Tree. Source: Curran (2018).

The top hash in the diagram is called the "Merkle Root" and is the hash of all of the data in that block. Changing even one character in the data of a block would change its Merkle Root hash and subsequently the header hash in that block which is further discussed under hash pointers.

Figure 4 shows how the above Merkle Tree gets incorporated into a block. All of the transactions that were sourced from the mempool at the bottom of the diagram are hashed and then re-hashed multiple times until a single hash output, the Merkle Root is created and added to the block header. The block header also contains the software version,

the previous block's hash (as mentioned in Section 1), the timestamp of the block, the difficulty target (mentioned in Section 3), and the nonce (also, mentioned in Section 3).

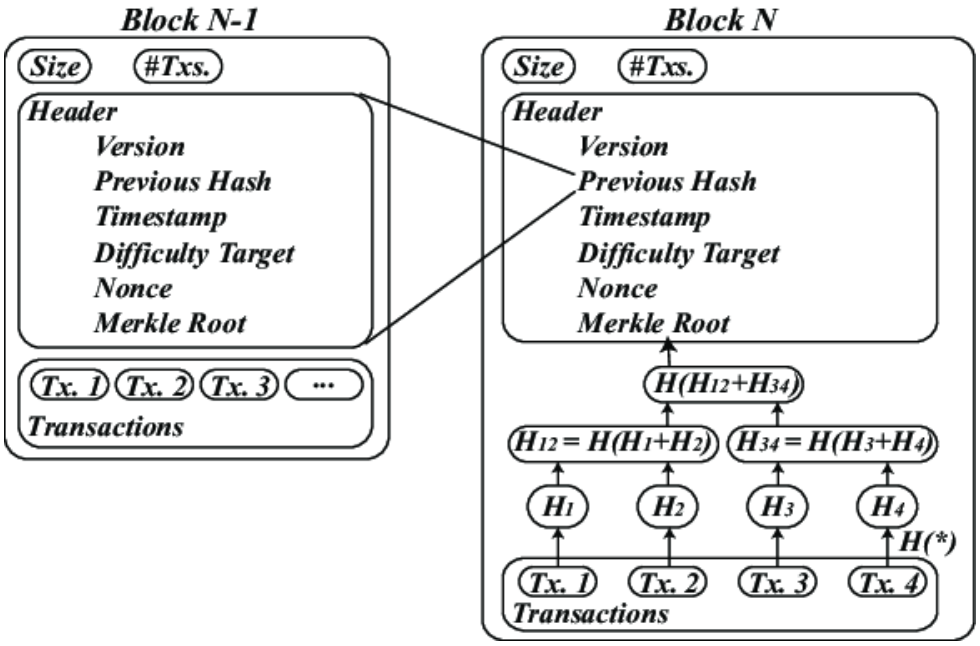

Figure 4. Structure of a Traditional Blockchain. Source: Cao, He, Jiang, Ma, Wu, & Yang (2018).

5. Network

When running the network, the processes outlined above are completed in the following order from the Bitcoin white paper:

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.

6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash. (Nakamoto, 2008, p. 3)

The longest chain will be considered the correct one and if a node receives two chains simultaneously it will begin working on the longest one while saving the other in case it becomes longer. The node will then switch to the other node on the next proof-of-work if it becomes longer (Nakamoto, 2008). Each block in the chain contains a timestamped pointer to the subsequent block therefore linking all of the blocks, as shown in Figure 5.

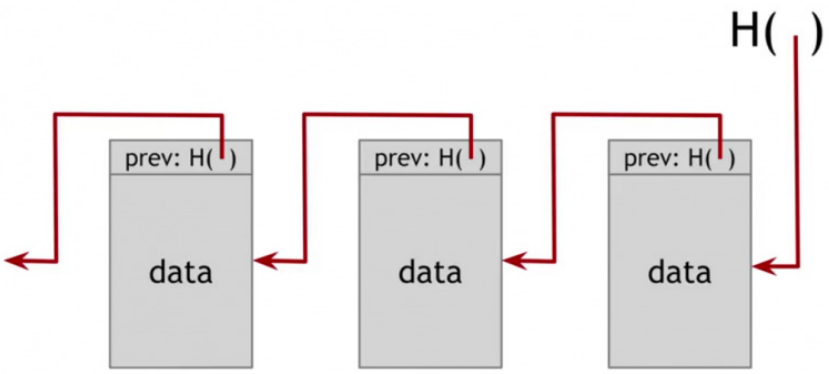

Figure 5. Example Hash Pointer. Source: Learningspot (2016).

As opposed to a normal pointer that only allows retrieval of information, a hash pointer allows retrieval of information and verification that it has not changed (Learningspot, 2016). One of the main advantages of this technology is immutability. The hash pointer at the head of the block indicates what the contents of the following block are since it is a discrete value. For example, in Figure 6, an adversary tries to change the content of the data in the block with the lightning bolt:

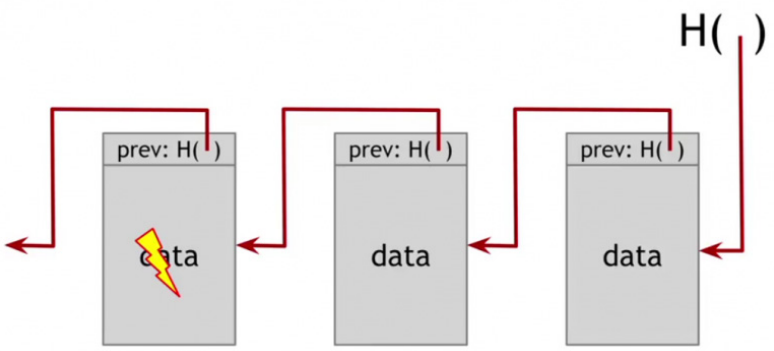

Figure 6. Example Adversary Attack. Source: Learningspot (2016).

Because this block is linked to the following block through a hash pointer, tampering with the data in this block will change the Merkle Root and subsequently the header of the next block, as illustrated in Figure 7.

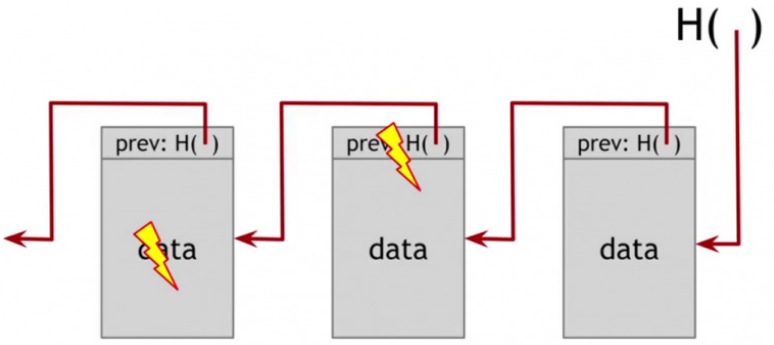

Figure 7. Example Header Change From Attack. Source: Learningspot (2016).

In essence, because each block is inextricably linked with the one before and after it, any inconsistency would be immediately broadcast to all of the nodes and rejected. Even if the attacker changed the header for each block until finally arriving at the last block in the blockchain, the nodes would pick up on the change and reject it. This linkage is what makes the blockchain immutable or tamper proof.

6. Example Bitcoin Transaction

In order to tie all of the concepts of Section C: "How Does It Work" together, it is useful to consider an example. Suppose Alice wants to pay Bob two Bitcoins for a good. Below are the steps that will occur.

- Alice will send her two Bitcoins to Bob's public address, digitally signing the transaction by inputting her private key. (Every Bitcoin user is assigned a public and private key. The only way to prove ownership of one's Bitcoins is to hold and then use the private key associated with one's account. This key should never be revealed to anyone else. The public key is just one's account address for receiving funds and like the name implies can be published without fear of funds being compromised.)

- The transaction is then added to the mempool along with all other transactions during that period and subsequently picked by the miners, who are incentivized not only by the block reward, but also by a transaction fee associated with the transaction. (Every transaction on the Bitcoin network is assigned a fee, though very small when compared with fees charged by financial institutions.) The miners will also ensure that Alice has enough funds in her account (Two Bitcoin plus a small fraction of a Bitcoin for the transaction fee).

- Once the miners have a compiled list of transactions roughly equal to one megabyte (the standard size of a Bitcoin block), they will compete to solve the target hash value. When the target is hit, the winning node will broadcast the hash output to all other nodes for confirmation. Upon accepting confirmation, all other nodes will begin working on the next block and the transaction will be sealed in the ledger. Figure 8 is a simplified infographic showing this transaction.

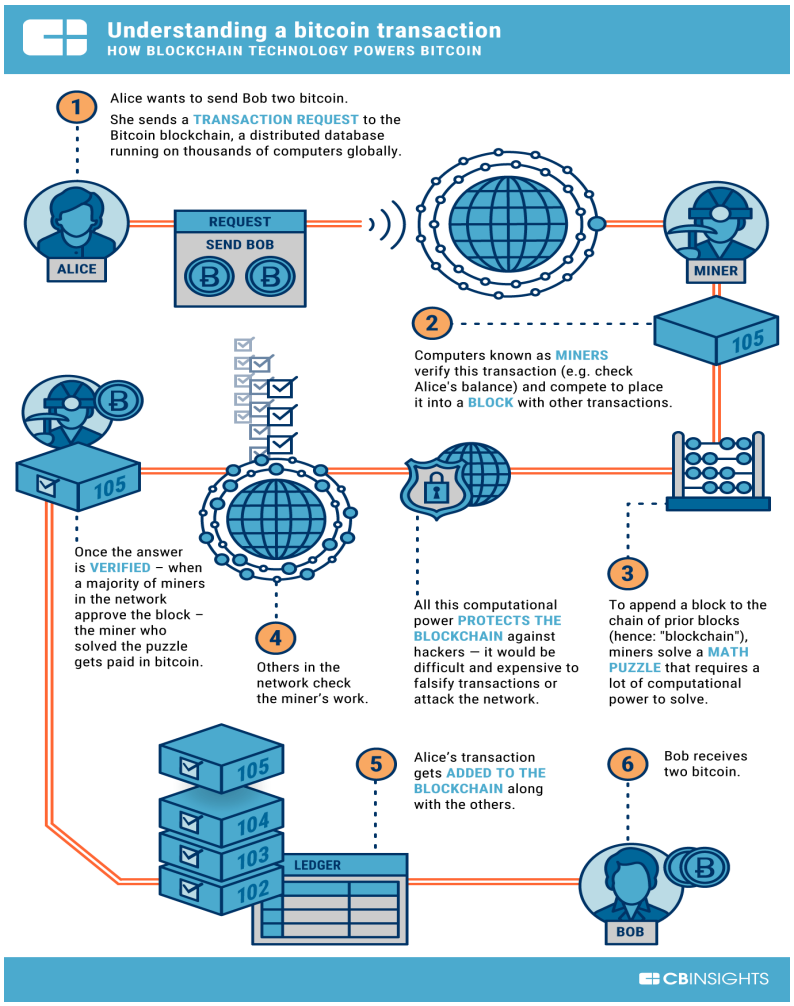

Figure 8. Understanding a Bitcoin Transaction. Source: CBInsights (2018).

7. Types of Blockchains

Although many different types of blockchains exist, most are beyond the scope of this paper. This report will address the two broad categories of blockchains that the Navy will have to consider as a potential records management solution: public (or permission-less) and private (or permissioned). Almost all blockchains fit in to these two broad categories with the exception of some hybrids that cross between the two. A useful analogy is that a public blockchain is similar to the internet, while a private blockchain is similar to an intranet.

Bitcoin runs on a public blockchain meaning that anyone can access and transact on the system. This was the original intent behind Bitcoin, which was created in the wake of the 2008 financial crisis. Financial freedom could be had by not placing trust in any human governed authority, but in an objective network based on code. The potential ramifications for this technology are truly groundbreaking: near-instant cross border payments, banking the unbanked, and a store of value during economic turmoil being a few. However, the most prominent use case in the early years of Bitcoin's existence was buying and selling illicit goods, mostly drugs. The open-ness of a public blockchain brought with it the ability for entrepreneurs to fill a void in the market; the relatively easy exchange of contraband for an anonymous payment system. This was possible because even though a public blockchain is transparent (everyone is able to see every transaction) the public address provided a level of anonymity to users of the blockchain. Recall that a public address is a random 64-character string of letters and numbers. Any user could create a public address without tying any PII to it. However, this protection has been clearly eroded by software that uses website cookies and on-chain transaction analysis to tie a Bitcoin address to an individual (Emerging Technology from the arXiv, 2017). The Federal Bureau of Investigation (FBI) used this and other techniques to bring down the dark web drug exchange site "The Silk Road" and its founder Ross Ulbricht in 2013 (Hume, 2013).

One significant disadvantage of a public blockchain is the amount of computational power that must be used to keep the network running. Although the proof of work algorithm keeps the network secure by ensuring that no malicious actor(s) can modify the ledger without controlling at least fifty-one percent of the hashing power (known as a 51% attack) it is extremely energy intensive. This point is evidenced in the Bitcoin blockchain, which has grown exponentially over the past decade. Not only does the ledger itself grow, but also as the price of Bitcoin grows, so does the hashing difficulty, requiring more computing power. The current power draw is estimated to be twenty-two terawatt-hours per year, which is about the same consumption as the country of Ireland (G. F., 2018). Another disadvantage of a public blockchain, with regard to housing sensitive data like official military records, is that as mentioned above, all of the data stored can be viewed by anyone.

While this transparency is lauded as one of the main value propositions in a new digital payment system, it is not a feasible solution when privacy must be maintained.

A private blockchain, on the other hand, requires that a user is sent an invitation and subsequently must be validated on the network (Jayachandran, 2017). This could be accomplished several ways including current participants deciding on future participant entry or a regulatory authority giving license to a would-be participant (Jayachandran, 2017). In addition to maintaining privacy, a permissioned blockchain can be faster and more scalable than a permission-less one due to the relative size of data throughput. Any real consideration of using a blockchain solution for sensitive records should be centered on using a permissioned blockchain due to the aforementioned concerns of maintaining privacy, as well as the fact that a public blockchain would be unwieldly an overkill for that purpose.

Additionally, a permissioned blockchain uses a different consensus mechanism than a permission-less one. Because of the inherent increase in level of trust in a permissioned blockchain, using a proof of work algorithm would also be overkill. Instead, permissioned blockchains, like the Linux Foundation's hyperledger fabric, use a Practical Byzantine Fault Tolerance (PBFT) Algorithm (Baliga, 2017). PBFT works on the premise that given enough "honest nodes," this complex algorithm can still achieve consensus. This algorithm would not work on a public blockchain, which is an untrusted environment, i.e., nodes are presumed to be malicious. However, in the semi-trusted environment of a permissioned blockchain, a PBFT algorithm accounts for a limited number of failing nodes (Baliga, 2017).

D. BENEFITS

There are several advantages that blockchain technology has over a traditional centralized ledger. The first concerns the issue of trust. Within a centralized server, trust must be placed with the entity in charge of running that server. Due to the cryptography associated with blockchain, trust is instead placed in the mathematical functions that run the network. There is no one "in charge" of the Bitcoin blockchain. Instead, all transactions are verified and trusted through the aforementioned process of hashing and consensus.

Because tampering with the blockchain is so difficult, the user can trust that the ledger is immutable.

The second advantage blockchain has is redundancy. Because of the decentralized network, given enough nodes, a blockchain is mostly impervious to deletion. There is no central point of failure because each node will have a copy of the ledger stored and if one drops offline, the rest can continue running seamlessly. A deletion of the Bitcoin blockchain, for example, would require deletion of the internet itself.

Transparency and completeness are additional advantages that blockchain has over a central repository. Because the blockchain ledger is an ever-increasing distributed database, every transaction that occurs within its network is saved. In a public blockchain, any user will be able to see every recorded piece of the blockchain. In this way, the blockchain is an "append only" database. The only way to reverse a transaction is for the recipient to send the funds or the data back to the sender.

One huge obstacle facing the United States Navy is that an individual's data is stored across many separate silos that do not communicate with each other. This inefficiency directly increases the workload of administrators who must find data about a particular individual across disparate databases. A blockchain solution could improve efficiency. Estonia, (as discussed later in Section F) has largely solved this problem by implementing a digital infrastructure called X-Road that houses its citizens' information in databases that communicate with each other, but also maintain privacy, through public and private key cryptography. Figure 9 is a diagram of the X-Road architecture that Estonia has in place (Heller, 2017). In a McKinsey and Co. article, the authors make the case that certain data can be accessed by authorized government agencies to streamline processes, but only the data that is needed:

> In certain situations, smart contracts could expose certain information to designated agencies if predefined conditions are met. If recipients of unemployment benefits are imprisoned, for instance, that information could be transmitted to the labor agency so payments can be stopped for the duration of the sentence. Agencies would be able to use a specific piece of information for the purpose at hand but would not have unlimited access to all of an end user's data. The use of blockchain ledgers would reduce the risk of unauthorized access (through strong encryption) and data

manipulation (through tamperproof audit trails). Indeed, public services could become truly networked, without infringing unduly on privacy rights. Individuals and companies would no longer need to spend a lot of time filling in forms with information they had already provided to the government. And agencies could tailor their services to meet individuals' needs, rather than deploying a one-size-fits-all approach. (Cheng, Daub, Domeyer, & Lundqvist, 2017, para. 16)

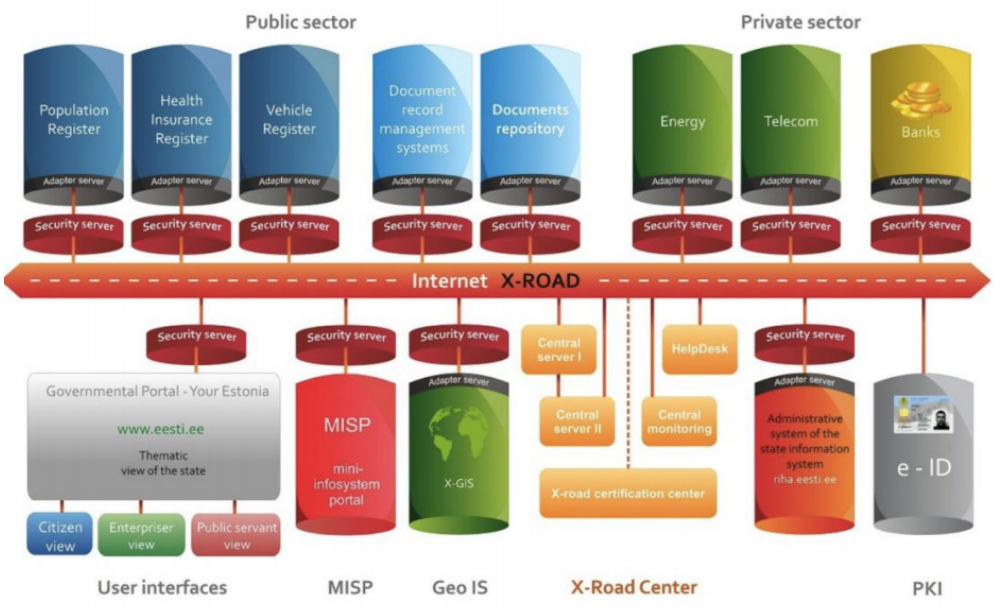

Figure 9. X-Road Data Exchange Schematic. Source: Jaffe (2016).

Blockchain technology can also be used to streamline processes such as land transfer. Sweden and the Republic of Georgia are researching the use of a mobile application to record each step in a land sale transaction on a blockchain theoretically reducing the time needed to complete a sale from three to six months to just days (Cheng et al., 2017).

E. DISADVANTAGES

Although blockchain technology contains some inherent benefits, it also brings with it disadvantages that must be recognized. In addition to the immense computational power that must be used to keep the Bitcoin blockchain running and the totally transparent nature of the network, it is generally much slower than a database. The time required to

verify and gain consensus on the new information in the blocks, means that unlike a database that can be updated near instantaneously, a blockchain solution may possibly take minutes to even hours depending on the amount of transactions and the speed at which consensus is achieved. For example, the Bitcoin blockchain is limited to the creation of one megabyte sized blocks every ten minutes. If the volume of transactions greatly exceeds this throughput, then lower priority transactions, i.e., those with lower transaction fees, will take longer to be verified by the network.

On the other hand, the issues of computation power and latency are largely resolved with a permissioned blockchain. The main disadvantage to implementing a blockchain over a Standard Query Language (SQL) database is that of complexity and cost. As a fledgling technology, the start-up costs to build and implement a permissioned blockchain would undoubtedly be substantial. So why replace a functioning database? The primary reason is security. According to Collin Thompson in an article for *Blockchain Daily News*, a permissioned blockchain still takes advantage of the security features of a permission-less one while disregarding the complex mathematical functions to achieve consensus:

> Private blockchains mimic the security process utilized by public blockchains like Bitcoin, but do not involve mathematical guarantees at the validation level or with respect to irreversibility. However, they still make use of cryptography and data structures like Merkle trees to ensure non-valid transactions aren't added to the blockchain. At the end of the day, private blockchains provide higher levels of error checking and transaction validity than regular shared databases. (Thompson, 2018, para. 11)

F. CURRENT APPLICATIONS

There are many applications of blockchain technology in use today within industries both private and public to include financing, healthcare, and supply chain management.

1. Bitcoin/Crypto-Currencies

The most prominent current use of blockchain technology is the aforementioned digital currency Bitcoin. Crypto-currencies are an inherently good fit for blockchain because of the solution to the "double spend" problem and the fact that the underlying blockchain solves multiple issues with our legacy banking system, including need for a

trusted third party, cross border remittance payments, susceptibility to hacking, fractional reserve banking, and a fluctuating interest rate. A new technology called "smart contracts" popularized by the crypto-currency Ethereum allow for cryptographic execution of a transaction given that certain requirements are met, without the need for an escrow service. Use cases for smart contracts include land transfer, supply chain management, and insurance (Coleman, 2016).

Even Wall Street is recognizing the benefits of this fledgling technology. JP Morgan Chase has announced that it will be using its own crypto-currency backed by the U.S. dollar. As of this writing, it is a closed loop system within JP Morgan Chase banks and it is not available to clients yet. However, it is hoped to be used to increase speed of wire transactions, which currently take hours or even days, to near instantaneous (Merced & Popper, 2019).

2. Supply Chain Management

Next to crypto-currencies, supply chain management is one of the most promising fields in which blockchain technology can be put to use. Walmart has partnered with IBM to use "hyperledger fabric" which is a blockchain solution built by the Linux Foundation to track its produce. In a *Fortune* article, Walmart under the leadership of Frank Yiannas, vice president of Food Safety, was able to reduce the time needed to determine the origin of mangos it was selling from over 6 days to just seconds (Hackett, 2017). Hyperledger was used not only to ascertain the origin of the fruit, but also to ascertain intermediate stops along the way to its final destination, including passage through customs, processing, and storage (Hackett, 2017). Walmart is not the only company interested in blockchain solutions to increase supply chain efficiency. Maersk, Airbus, and Daimler are also actively testing or researching their own use cases.

Naval aviation has collaborated with Indiana Technology and Manufacturing Company (ITAMCO) to develop a solution for aircraft parts tracking using a product called "Simba Chain." Simba Chain is a Defense Advanced Research Projects Agency (DARPA) led product that the Navy hopes to use to "rapidly determine the origin and lineage of flight-critical aircraft parts" (The Cube, 2019). The Navy currently uses pen and paper to track

aircraft parts via a Scheduled Removal Component Card (SRCC) that is then manually entered into a database (The Cube, 2019). Much like Walmart drastically reducing the time needed to trace its fruit, Naval Air Systems Command (NAVAIR) hopes to be able to track aircraft parts much quicker and more efficiently.

3. Records Management

Encoding personal data on a blockchain is of immense interest for many organizations including government offices and businesses. However, as opposed to the supply chain management use case, applying a blockchain solution to records management is not as cut and dry. For instance, one must ask, "What problem am I trying to solve by using a blockchain instead of a traditional database?" McKinsey and Co. illustrates the point that blockchain innovation may be stalling out due to lack of any tangible benefits over traditional servers and databases in an article titled "Blockchain's Occam Problem:"

> Certainly, there is a growing sense that blockchain is a poorly understood (and somewhat clunky) solution in search of a problem. The perspective is exacerbated by short-term expense pressures, cultural resistance in some quarters (blockchains may threaten jobs), and concern over disruption to healthy revenue streams. There are challenges in respect of governance—making decisions in a decentralized environment is never easy, especially when accountability is equally decentralized. And there are technical impediments, for example in respect to blockchains' data storage capacity. (Higginson, Nadeau, & Rajgopal, 2019, para. 26)

However, later in the article, the authors assert that although some use cases may be withering on the vine, there are still benefits to be gained in certain areas, particularly those of supply chain and records management:

> Recent experiments in supply chains, identity management, and sharing of public records have been positive…An emerging perspective is that the application of blockchain can be most valuable when it democratizes data access, enables collaboration, and solves specific pain points. (Higginson et al., 2019, para. 30)

4. Estonia

The country of Estonia has become an international testbed for a completely digital society. X-Road, the architecture behind Estonia's disparate databases, "links individual

servers through end-to-end encrypted pathways" (Heller, 2017, para. 17). This technology allows the average citizen to control their data almost entirely online and ensures privacy by allowing access to only authorized individuals. Instead of data being held in a centralized location, the X-Road system allows it to live locally, while at the same time connected to all of the other databases, painting a complete picture of a resident's online identity and still ensuring data privacy. This "silo-ing" of data allows a resident's doctor to access her medical file, but not her voting record. Furthermore, when that doctor looks at her record, it is recorded and reported. Anyone looking at another's medical record or any other data without authorization is punishable under Estonian law. Running behind X-Road is a blockchain called K.S.I. or Keyless Signature Infrastructure. Martin Ruubel, the president of Guardtime, the Estonian company that developed KSI, states immutability and timeliness of the discovery of attempted tampering as the reasons Estonia uses a blockchain to encode its resident's data. In a *New Yorker* article titled "Estonia, the Digital Republic," Ruubel and the author make this case:

> Popular anxiety tends to focus on data security—who can see my information?—but bits of personal information are rarely truly compromising. The larger threat is data integrity: whether what looks secure has been changed. (It doesn't really matter who knows what your blood type is, but if someone switches it in a confidential record your next trip to the emergency room could be lethal.) The average time until discovery of a data breach is two hundred and five days, which is a huge problem if there's no stable point of reference. "In the Estonian system, you don't have paper originals," Ruubel said. "The question is: Do I know about this problem, and how quickly can I react?" The blockchain makes every footprint immediately noticeable, regardless of the source. (Ruubel says that there is no possibility of a back door.) To guard secrets, K.S.I. is also able to protect information without "seeing" the information itself. (Heller, 2017, para. 69)

IV. APPLICATION

A. ADVANTAGES OVER CURRENT SYSTEM

Encoding Sailor's enlisted records on to a blockchain brings with it multiple advantages, several of which have been discussed in Chapter III, Section D under "Benefits." Although trust and immutability of the data on the blockchain are no doubt tremendous advantages, it is unlikely that a detailer or anyone else with write privileges to Navy Personnel Command databases would purposely alter a record for malicious purposes. However, if that detailer accidentally entered the wrong information, the blockchain would flag it immediately and ensure that every authorized user, including the Sailor in question would be able to ascertain the validity of the entry.

One of the main benefits of a blockchain solution for Sailor records would be housing all of the data from disparate Navy databases on to a single blockchain thereby streamlining the process to update a record. If a solution similar to X-Road were implemented, databases such as NFAAS, Navy Knowledge Online (NKO), PRIMS, and MYPAY could be connected with end-to-end encryption. The Estonian solution couples X-Road with KSI to add an extra layer of security.

B. IMPLEMENTATION

The Keyless Signature Infrastructure (KSI) that Guardtime uses is an interesting, potential fit for securing Sailor record data. KSI secures the data in a traditional public key infrastructure (PKI) served database by creating a mirror of the database comprised of only the hash values of the underlying data. Recall that hashing is a one-way function meaning that the original data that is hashed cannot be derived from the hash itself. When the hashes are collision free, no two pieces of data can have the same hash. This keeps the functions of signature identity and signature integrity separate. Signature identity can still be solved using PKI asymmetric cryptography, much like the current common access card (CAC) system. In order to keep the signatures secure and tamper-free, hashes of each document are aggregated, which are then hashed. In essence, what results is a Russian Nesting Doll of hash values, with the top value, or Merkle-Root comprised of all the previous hash

values before it. What follows are Guardtime's steps for signing many documents using KSI:

1. Hashing: The documents to be signed are hashed and the hash values are used to represent the documents in the rest of the process.

2. Aggregation: A global temporary per-round hash tree is created to represent all documents signed during the round. The duration of rounds may vary but is set to one second in the working solution.

3. Publication: The root hash values of the per-round aggregation trees are collected into a perpetual hash tree (so-called hash calendar) and the root hash value of that tree is published as a trust anchor. (Buldas, Kroonmaa, & Laanoja, 2013, p. 313)

Again, Estonia serves as a testbed and although it's a relatively small country with 1.3 million people (Worldometers, n.d.), its population is still approximately four times the size of current active duty Sailors in the Navy, so scaling is likely not a relevant consideration. Guardtime says as much on their website under "The Benefits of KSI:"

> Massive Scale. The KSI signatures can be generated at exabyte-scale. Even if an exabyte (1,000 petabytes) of data is generated around the planet every second, every data record (a trillion records assuming 1MB average size) can be signed using KSI with negligible computational, storage and network overhead. (Guardtime Federal, n.d., para. 9)

C. GUARDTIME'S CURRENT PARTNERSHIPS

Guardtime Federal, the U.S. arm of its parent company has already solidified partnerships with U.S. government agencies and defense contractors. In April of 2017, Lockheed Martin contracted Guardtime Federal to incorporate blockchain technology into its "system engineering process, supply chain risk management and software development efforts" (Vill, 2017, para. 2).

Guardtime Federal has also been hired by the U.S. Department of Energy to modernize the energy infrastructure. From Guardtime's press release:

As we modernize our energy infrastructure, the speed, size and complexity of energy data and transactions exchanged increases exponentially, noted Michael Mylrea, PNNL's primary investigator for the project. To help overcome these challenges, blockchain KSI technology provides a unique value proposition in its potential to help optimize and secure these critical data sets. The multi-million dollar award is designed to protect the Nation's energy infrastructure from emerging cyber threats and enhance the reliability and resilience of the Nation's critical energy infrastructure through innovative, scalable, and cost-effective research and development of cybersecurity solutions and operational capabilities. (Ruubel, 2017, para. 2)

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

When designed as a private or permissioned architecture, blockchain technology provides the necessary security to protect sensitive personal information with a decentralized system. With the proper design, it could be used to gather data from several personnel databases to support detailing and retention incentive decisions within the enlisted detailing marketplace. It has the potential to streamline the process, thereby lowering the amount of manpower required in the process.

A. AREAS FOR FUTURE RESEARCH

Although the use case for blockchain technology to house official Navy records shows promise, further research must be conducted, specifically in the form of a cost-benefit analysis (CBA). As previously stated, the main benefits blockchain provide over traditional databases are security and redundancy. If coupled with a software solution connecting common Navy websites with end-to-end encryption similar to X-Road, the resultant potential man-hours saved could have a tangible impact to the Navy's Operations and Maintenance (O&M) bottom line. However, does this potential benefit outweigh what would most probably be a significant financial cost of implementation?

If the answer to the above question is yes, then a decision still needs to be made on who should build out the architecture. There are several possible solutions. First, the Navy could try to build a solution in-house. Given that blockchain technology is extremely new and relatively untested as well as the fact that there is undoubtedly little corporate knowledge within the Navy to build a complex blockchain based records management solution, this option should be given the least consideration.

The next option is to outsource the job to a DoD agency outside of the military dedicated to researching cutting-edge technology like the Defense Advanced Research Projects Agency (DARPA.) DARPA has already begun research into use cases for blockchain technology within the DoD. In 2016, DARPA awarded Galois, a computer security firm, 1.8 million dollars to formally audit Guardtime's KSI blockchain (Richmond, 2017). Timothy Booher, DARPA's program manager for initiative, makes the

case that the technology could be used to sniff out malicious actors who manage to break into the system rather than continuing to attempt to keep them out altogether: "Instead of trying to make the walls of a castle as tall as possible to prevent an intruder from getting in, it's more important to know if anyone has been inside the castle, and what they're doing there" (para. 5). DARPA has the resources and the ability to outsource work to individuals with the skills needed to tackle the extensive coding required to complete such a project.

The last option the Navy has to implement a blockchain solution is to outsource it to a civilian technology company such as IBM. IBM has done extensive work in the past several years on its own blockchain solutions mainly in the field of supply chains as mentioned in Chapter III with hyperledger fabric. Although a company such as IBM undoubtedly has a vast amount of technical expertise, the company is currently focusing on three use cases: financial services, shipping, and healthcare (Garcia, 2018). The healthcare industry is likely the most comparable to naval records management as IBM is looking to streamline the process through blockchain based medical records. Disparate medical information is a similar problem to that of official Navy record information.

B. OTHER USE CASES

As was stated earlier in Chapter III, Estonia's X-Road system allows many kinds of personnel information to be stored on a blockchain type architecture known as KSI, to include medical records. Since a permissioned blockchain allows for a level of security as well as the ability to quickly identify any tampering of information, it could also potentially be used within the DoD healthcare industry to track a patient's medical history. Some DoD members see specialists outside of a Military Treatment Facility (MTF). A blockchain could allow medical records to be seen by any doctor providing care to a specific patient.

Another potential use case for blockchain is within the DoD's supply chain management system. As was previously stated, NAVAIR is already looking at the possibility of using blockchain technology to track aircraft parts. This technology could be used across the entire DoD to track parts. Supply chain management within the DoD involves many individuals and organizations, which can make tracking parts through the system difficult. The use of a decentralized ledger would allow anyone to see the exact

location of a part as well as track the movement of the part from its origin to its destination. It could cut down the number of hours spent locating a specific part.

There are certainly benefits to using such technology within the DoD, but a more in-depth analysis needs to be done on the costs to implement such a system. Each of these use cases, to include the use of blockchain technology on personnel records management and the enlisted detailing and retention process, must be evaluated further through a CBA or similar analysis. As was stated earlier, a CBA would help determine whether the benefits of using blockchain technology outweigh the costs of implementing such a system.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Baliga, A. (2017, April). *Understanding blockchain consensus models.* Retrieved from https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf

Belin, O. (n.d.). The difference between blockchain and distributed ledger technology. Retrieved May 1, 2019, from TradeIX website: https://tradeix.com/distributed-ledger-technology/

Board of Governors of the Federal Reserve System. (n.d.). Reserve Requirements. Retrieved April 30, 2019, from https://www.federalreserve.gov/monetarypolicy/reservereq.htm

Buldas, A., Kroonmaa, A., & Laanoja, R. (2013). Keyless signatures' infrastructure: how to build global distributed hash-trees. *Secure IT Systems, 8208*, 313–320. https://doi.org/10.1007/978-3-642-41488-6_21

Cao, J., He, J., Jiang, S., Ma, M., Wu, H., & Yang, Y. (2018). BlockHIE: a BLOCkchain-based platform for healthcare information exchange. Retrieved from ResearchGate website: https://www.researchgate.net/publication/324728250_BlockHIE_a_BLOCkchain-based_platform_for_Healthcare_Information_Exchange

CBInsights. (2018, September 11). What is blockchain technology? Retrieved from https://www.cbinsights.com/research/what-is-blockchain-technology/

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

Coleman, L. (2016, October 12). Smart contracts: 12 use cases for business and beyond. Retrieved from CCN website: https://www.ccn.com/smart-contracts-12-use-cases-for-business-and-beyond

Curran, B. (2018, July 9). What is a Merkle tree? Beginner's guide to this blockchain component. Retrieved from Blockonomi website: https://blockonomi.com/merkle-tree/

Emerging Technology from the arXiv. (2017, August 23). Bitcoin transactions aren't as anonymous as everyone hoped. *MIT Technology Review.* Retrieved from https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/

Frankenfield, J. (2018, July 30). Proof of work. Retrieved from https://www.investopedia.com/terms/p/proof-work.asp

Garcia, A. (2018, September 12). IBM is betting big on blockchain technology. Is it worth the risk? Retrieved from CNN website: https://money.cnn.com/2018/09/06/technology/ibm-blockchain-gamble/index.html

G. F. (2018, July 9). Why bitcoin uses so much energy. *The Economist.* Retrieved from https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy

Guardtime Federal. (n.d.). Keyless signature infrastructure. Retrieved April 16, 2019, from http://www.guardtime-federal.com/ksi/

Hackett, R. (2017, August 22). Why big business is racing to build blockchains. Retrieved from Fortune website: http://fortune.com/2017/08/22/bitcoin-ethereum-blockchain-cryptocurrency/

Heller, N. (2017, December 11). Estonia, the digital republic. *The New Yorker*. Retrieved from https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic

Higginson, M., Nadeau, M.-C., & Rajgopal, K. (2019, January). Blockchain's occam problem. Retrieved from McKinsey and Company website: https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem

Hong, E. (2019, April 29). How does Bitcoin mining work? Retrieved from https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

Hume, T. (2013, October 5). How FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road. Retrieved from https://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html

Jaffe, E. (2016, April 20). How Estonia became a global model for e-government. Retrieved from Sidewalk Talk website: https://medium.com/sidewalk-talk/how-estonia-became-a-global-model-for-e-government-c12e5002d818

Jayachandran, P. (2017, May 31). The difference between public and private blockchain [Blog post]. Retrieved from https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Kim, H., Kuo, T.-T., & Ohno-Machado, L. (2017, September 8). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

Learningspot. (2016, November 28). Hash pointers and data structures: definition and application to structures. Retrieved from http://learningspot.altervista.org/hash-pointers-and-data-structures/

Lisk Academy. (n.d.). What is hashing? Retrieved February 5, 2019, from https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-hashing

Merced, M. J. de la, & Popper, N. (2019, February 14). JPMorgan Chase moves to be first big U.S. bank with its own cryptocurrency. *The New York Times*. Retrieved from https://www.nytimes.com/2019/02/14/business/dealbook/jpmorgan-cryptocurrency-bitcoin.html

Merkle, R. (1988). A digital signature based on a conventional encryption function. *Advances in Cryptology—CRYPTO '87, 293*, 369–378. Retrieved from http://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkle.pdf

Nakamoto, S. (2008, October 31). Bitcoin: a peer-to-peer electronic cash system. Retrieved from Bitcoin Project website: https://bitcoin.org/bitcoin.pdf

Navy Personnel Command. (n.d.-a). Assignment Incentive Pay (AIP). Retrieved January 3, 2019, from NPC website: https://www.public.navy.mil/bupers-npc/career/payandbenefits/Pages/AIP.aspx

Navy Personnel Command. (n.d.-b). Career Management System Interactive Detailing (CMS-ID). Retrieved January 3, 2019, from NPC website: https://www.public.navy.mil/bupers-npc/enlisted/cmsid/Pages/default2.aspx

Navy Personnel Command. (n.d.-c). Enlisted detailing. Retrieved January 3, 2019, from NPC website: https://www.public.navy.mil/bupers-npc/enlisted/detailing/Pages/default2.aspx

Navy Personnel Command Public Affairs. (2014, November 13). 4 things you need to know: modernizing enlisted detailing. Retrieved from DoD Live website: http://navylive.dodlive.mil/2014/11/13/4-things-you-need-to-know-modernizing-enlisted-detailing/

Passwords Generator. (n.d.). SHA256 hash generator. Retrieved May 1, 2019, from https://passwordsgenerator.net/sha256-hash-generator/

Richmond, J. (2017, May 3). DARPA and advancing cybersecurity infrastructure with blockchain. Retrieved from https://www.nasdaq.com/article/darpa-and-advancing-cybersecurity-infrastructure-with-blockchain-cm783507

Ruubel, M. (2017, September 21). U.S. Department of Energy Contracts Guardtime, Siemens, and industry partners for blockchain cybersecurity solutions [Blog post]. Retrieved from Guardtime website: https://guardtime.com/blog/us-department-of-energy-contracts-guardtime-pnnl-siemens-and-industry-partners-to-develop-blockchain-cybersecurity-technology-for-distributed-energy-resources

Tech Terms. (n.d.). Hash definition. Retrieved January 29, 2019, from https://techterms.com/definition/hash

The Cube. (2019, January 30). *Cisco multicloud showcase* [Streaming video]. Retrieved from https://video.cube365.net/l/J3dKyfP4QDaYM-deYka7PA

Thompson, C. (2018, May 14). Private blockchain or database, what's the difference? *Blockchain Daily News.* Retrieved from https://www.blockchaindailynews.com/Private-Blockchain-or-Database-Whats-the-Difference_a24596.html

Vill, M. (2017, April 27). Lockheed Martin contracts Guardtime Federal for innovative cyber technology [Blog post]. Retrieved from Guardtime website: https://guardtime.com/blog/lockheed-martin-contracts-guardtime-for-innovative-cyber-technology

Worldometers. (n.d.). Estonia population—2019. Retrieved April 16, 2019, from http://www.worldometers.info/world-population/estonia-population/

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California