BLUE HORIZONS FELLOWSHIP

AIR UNIVERSITY

BLOCKCHAINS IN NATIONAL DEFENSE:
TRUSTWORTHY SYSTEMS IN A TRUSTLESS WORLD

by

Neil B. Barnas, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor(s): Mr. Harry Foster

Maxwell Air Force Base, Alabama

June 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

ACKNOWLEDGEMENT

Thanks to my wife and children for their seemingly limitless patience and support.

ABSTRACT

The ability of the USAF to prevail in the highly contested environment of 2040 will be dictated by its ability to defend cyber-enabled systems, and the data within them, from compromise and manipulation. Yet contemporary cyber defense is faltering, and incremental improvements seem unlikely to overcome an exponentially growing cyber threat. Thus, an entirely new model for cyber defense strategy is needed. Blockchains are a new information technology that inverts the cyber security paradigm. First, blockchain networks are trustless; they assume compromise of the network by both insiders and outsiders. Second, blockchains are transparently secure; they do not rely on failure-prone secrets, but rather on a cryptographic data structure that makes tampering both exceptionally difficult and immediately obvious. Finally, blockchains networks are fault tolerant; they align the efforts of honest nodes to reject those that are dishonest. As a result, blockchain networks not only reduce the probability of compromise, but also impose significantly greater costs on an adversary to achieve it. The Air Force should research and develop blockchain technology and leverage it for national defense.

BIOGRAPHY

Major Neil B. Barnas is a US Air Force developmental engineer and acquisition manager. He holds a Bachelor of Science degree in Engineering Mechanics from the New Mexico Institute of Mining and Technology, Socorro, New Mexico and a Masters of Engineering in Systems Engineering from Pennsylvania State University, University Park, Pennsylvania. Major Barnas has served as a systems engineer or program manager for a variety of weapon systems, including the B-2, F-22, F-35, and other classified programs. Prior to the Blue Horizons Fellowship he was a branch chief in the Air Force Rapid Capabilities Office.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

I. INTRODUCTION

In 2015, the Chief of Staff of the Air Force tasked Air University's Blue Horizons Fellowship to explore "what competitive strategies and associated capabilities, capacities, technology investments, and integrating concepts the Air Force should pursue to prevail [in] highly contested environments in 2040." The Chief characterized the highly contested environment, in part, as three competitions: counter-electromagnetic spectrum (including cyber and EW), counter-sensor, and counter-decision.[1] Together, these three areas denote a broader strategic military competition characterized by the term "data-fighting." The concept of data-fighting does not have any formal definition, but it can be thought of as protecting one's ability to generate, store, disseminate, process, analyze, and exploit information while interfering with the adversary's ability to do the same. This paper is principally concerned with the defense aspects of data-fighting, or the ability to continue fighting despite adversary action.

The concept of data-fighting is not new. In *An Organic Design for Command and Control*, Boyd describes conflict as a competition of OODA loops, with victory favoring the actor that can execute OODA cycles faster and with less internal friction than an adversary.[2] While Boyd's model espouses the benefits of injecting friction into an adversary's decision process, it also promotes the benefit of making one's own process resilient to hostile action. The concept of data-fighting can also be related to the doctrine of counterair, which Air Force Doctrine Annex 3-01 defines as "the integration of offensive and defensive operations to attain and maintain a desired degree of control of the air and protection by neutralizing or destroying enemy aircraft and missiles." [3] Similarly, data-fighting could be described as the integration of offensive and defensive operations to attain and maintain a desired degree of control of the ability to generate, store, disseminate, process, analyze, and exploit information and protection by neutralizing the enemy's interfering action. Counterair's concept of *control*, which "describes a level of influence in [a] domain relative to that of an adversary," has important implications for data-fighting.[4] Control exists on a spectrum ranging from parity in the center to superiority and supremacy by either belligerent at the extreme. Thus, in data-fighting, until an adversary achieves supremacy an actor retains some ability to data-fight.

The principles inferred from Boyd and counterair doctrine show that active operations, both offensive and defense, are needed to prevail in data-fighting. Additionally, they show that one's ability to data-fight must be able to persist until the adversary achieves supremacy. Yet current cyber operations seems to hold the opposite view that a data-fighting network should be surrendered if one has anything less than supremacy over it. Joint Publication 3-12(R), *Cyberspace Operations*, states that if leaders suspect "that they cannot trust data on a network, or segment of the network, they should stop using the network/segment. In fact, the perception of data unreliability may unnecessarily extend beyond the specific degraded segment." [5] Given the DOD's increasing reliance not just on cyber systems specifically, but cyber-enabled systems generally, the prospect of surrendering a system or network despite one's near superiority over it is dismaying. It is the equivalent of surrendering control of the air over an entire country simply because an adversary can project force into it. If this notion is counter to airpower doctrine, then it should also be so in cyber.

To prevail in the highly contested environment of 2040, the USAF must be able to conduct data-fighting operations; not only offensive operations to impede an adversary, but also defensive operations that maintain the ability to data-fight despite some degree of adversary control within a broadly controlled USAF data-fighting battlespace. In a cyber context, this means: (1) preventing the intrusion of adversaries onto the data-fighting network; (2) if prevention fails, continuing data-fighting operations regardless of an adversary's presence on the network; and (3) using the data-fighting capability of the network to actively resist an adversary's efforts, even if those efforts are generated within from within one's one network.

In 2008, a new information technology called blockchain was introduced that enables defensive data-fighting. In simple terms, a blockchain is a shared, distributed, tamper-resistant database that every participant on a network can share, but that no one entity controls. Blockchain offer a paradigm shift in how data-fighting networks are designed, operated and defended. Blockchains are designed to operate in a highly contested environment against a determined adversary. They allow leaders and staffs to reliably command and control fielded forces despite adversary attempts to inject friction. Blockchains do this by always assuming the presence of an adversary on the network; by harnessing the numerical superiority of uncompromised nodes to neutralize the adversary's efforts; and by making information permanently resistant to manipulation or destruction. In sum, blockchains create trustworthy systems in a trustless world.[6]

The purpose of this paper is to explore blockchain technology for use in national defense. The paper begins with a discussion on the evolving cyber threat and the strategy of data manipulation. Next, it defines what a blockchain is, analyzes the elements that compose it, and then details its security attributes. This is followed by proposed uses of blockchain technology in defense-related applications. Finally, the paper concludes with closing thoughts and recommendations for implementation.

II. THE EVOLVING CYBER THREAT

As new technologies are developed, the DOD must continually re-evaluate the opportunities and threats these technologies create and adjust its strategy accordingly. Current trends in the development and democratization of digital technology call for such re-evaluation. This has been done, in part, by DOD's Third Offset, which will exploit the potential of learning machines to improve warfighting capability across the spectrum of military operations.[7] Recent developments in the field of machine learning and autonomy make this a prudent choice. However, the Third Offset does not address a probable adversary strategy against smart machines, which is to covertly manipulate the data these machine agents will use for analysis and decision making. Nor does the Third Offset address other significant technology trends that directly threaten not only smart machines, but also the cyber security strategy needed to protect them. These trends include the increase in nations with cyber forces, the exponential increase in the number and variety of malware, and the exponential increase in the number of personal computing devices throughout the world. In view of these trends, an analysis of cyber defense strategy is both timely and worthwhile.

The purpose of this section is to evaluate DOD cyber defense strategy in view of the threats highlighted above. It begins with a discussion on the evolution of weaponized information technology and the strategic calculus data manipulation. This is followed by a brief history and analysis of contemporary cyber defense strategy and a critique of why this strategy is inadequate to address future threats. This section closes with a strategy prescription for cyber defense.

A Growing and Evolving Cyber Threat

The cyber threat is not just growing; it is growing in three distinct ways. In the future, the US military will face an array of cyber forces that are more numerous, more capable, and better resourced than those it faces today. The number of devices projected to become part of the "internet of things" (IoT) is staggering. In 2006, there were two billion internet-enabled devices in use, or 0.3 devices for every person on Earth. By 2020, Cisco and Intel project that number could grow to 50-200 billion devices, respectively, or 6.5-26 devices per person.[8] [9] [10] [11] As digital innovation continues, even low cost consumer devices will have considerable computing power. In a recent interview with Time Magazine, Tim Cook, the president of Apple Computers, stated that even a device as common as the iPhone could be used to disable an electrical grid.[12] As of November 2015, Apple has sold more than 850 million iPhones.[13] The generation of malware exhibits a similar trend to computing devices. The number of distinct malware signatures increased from 7 million in 2007 to 100 million in 2012, with 200,000 more being registered each day with the US Cyber Emergency Repose Team (US-CERT).[14] Finally, state sponsorship of cyber activities will continue to grow. Today, 29 countries have acknowledged having offensive cyber forces, and 49 have procured software for hacking.[15] Given the relatively low cost of entry into the cyber competition, more countries will follow. These three trends – computing devices, malware generation, and state sponsorship – will have a force multiplying effect, creating a far more pervasive and effective cyber threat than what is seen today.

This force multiplying effect can already be seen in the increasing number of successful cyberattacks against highly resourced public and private entities. From August 2014 to October 2015, nine large US companies and 11 federal agencies were hacked, with the most notable being Sony, Target, JP Morgan, the Office of Personnel Management, the Joint Staff, and the

White House.[16] [17] Analysis of these types of attacks show that the intruders are able to persist within the network for an average of 200 days without being detected, providing ample time to locate valuable information caches and exfiltrate the data.[18] A meta-survey of media reports on successful cyberattacks provides a conservative estimate that in 2015 at least 290,000,000 records were leaked in the United States alone.[19] Cyberattacks like these are costly to the victims – they can lead to identity theft, loss of intellectual property, or damage to national security.[20] But just as new technologies evolve and become common in advanced societies, cyberattacks will evolve as well.

In the future, malicious cyber forces will move beyond just data theft to a far more dangerous tactic: data manipulation. This type of attack seeks to compromise the integrity, or truthfulness, of data. Militarily, such an attack is far more dangerous than data theft for two reasons. First, data manipulation affects every aspect of decision making. Using Boyd's OODA loop (Figure 1) as a model, one can quickly conclude that simply manipulating observations will have an effect down the decision chain. It influences what we see, which influences what we think, which influences how we act. In comparison, data theft simply allows an adversary to know what we know; it does not diminish or alter the victim's own thinking. The second reason data manipulation is more dangerous is that it can be more difficult to detect. Attackers can exploit natural variations and errors in data, or simply delete information all together. For instance, in a logistics management system, time-critical components could be redirected to other locations or the order deleted. In a joint targeting cell, weapons coordinates could be offset 30 meters by changing one digit by one increment. Such subtle manipulations not only yield significant results, but also reduce the likelihood of detecting the intrusion. Thus, the attacker is able to maintain persistence and continue operating. The advantages that integrity attacks provide to an adversary are now being highlighted by the nation's leading intelligence and security figures.

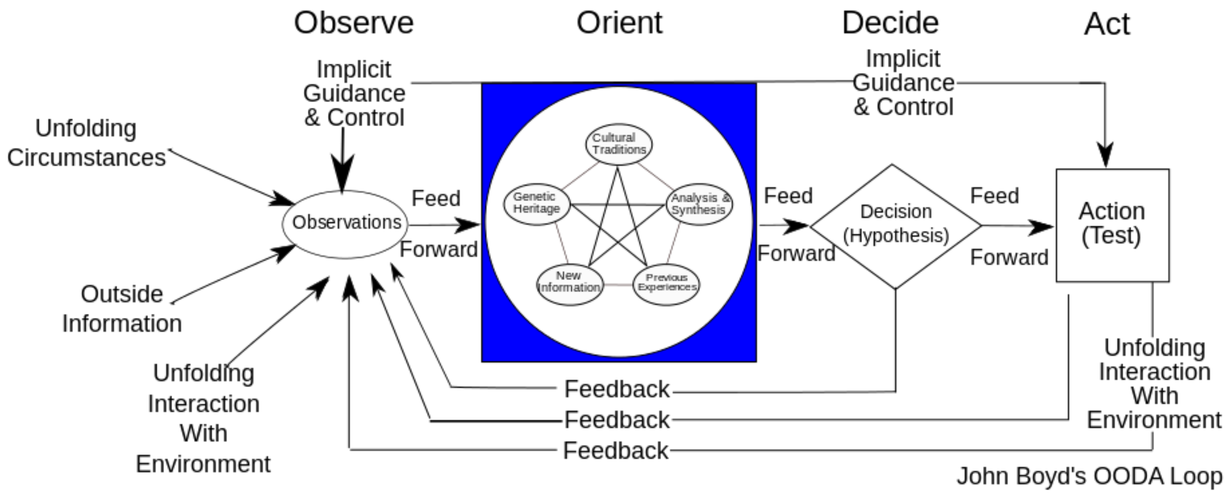

Figure 1: John Boyd's OODA loop decision model

In testimonies to congress, both James Clapper, Director of National Intelligence, and Navy Admiral Michael Rogers, Commander of US Cyber Command and Director of the National Security Agency, have expressed grave concern about the potential impacts of data manipulation.[21] [22] In 2013, Clapper rated the threat of cyberattack above terrorism as the greatest strategic threat to the United States, something that had not changed since 2001.[23] He described the most worrying element of this threat as "cyber operations that will change or manipulate electronic information in order to compromise its integrity." [24] Admiral Rogers related the consequence of this kind of attack to his time as a field commander, when he routinely relied on intelligence and information systems to help make quick, informed tactical decisions. "What happens if what I'm looking at does not reflect reality […] [and] it leads me to make decisions that exacerbate the problem I'm trying to deal with [or] make it worse?" [25] This question is applicable to decision making at every level of conflict, from pilots of advanced fighters engaging threats beyond visual range, to the President considering a nuclear response to a ballistic missile launch detection. How will operators, commanders, and government officials respond if the data and systems they rely on for decision making become suspect and cannot be trusted? [26]

The paradox of trusted information systems – that is, their ability to expand human agency while simultaneously creating dependence and, therefore, vulnerability – highlights the need for their assurance. Yet the analysis presented in this section indicates that assurance will become more difficult to attain, even as the need for it increases. Developing a strategy to close this gap, or at least halt its continued growth, starts with understanding the foundation of cyber defense strategy

The Fallacy of Cyber Defense

The story of cyber defense is a tragic tale that begins in 1988 with the ARPANET, the precursor to the modern internet. It is tragic because many of the flawed assumptions and philosophical leaps that underpinned cyber defense then still apply today. Understanding the architecture and governance structure from ARPANET can help to illuminate shortfalls in modern cyber defense, and provide a guiding policy for creating a new defense strategy based on modern technology.

In 1962, engineers from the Defense Department's Advanced Research Projects Agency (ARPA) began work on the precursor to the modern internet: the ARPANET.[27] ARPANET was envisioned to allow universities to more easily share the limited computing resources that existed across the country.[28] From 1969 to 1988, ARPANET spread from four nodes (or sites) at western universities to more than 10,000 nodes across the world.[29] The network architecture that connected the sites was decentralized. No single computer, server, or router was hierarchically superior to the others. This design was chosen to increase the network's overall resilience so that the loss any particular network nodes would not affect the network as a whole. The only rules that governed the network were embedded in the communication protocols that allowed the various nodes to communicate. Governance of the network, however, was centralized through DARPA and a number of formal working groups that oversaw ARPANET's technical development and implementation.[30] In other words, ARPANET used the principle of centralized control and decentralized execution.

ARPANET's security model was based on confidentiality and trust. It assumed that "outsiders" could easily be excluded and that "insiders" could be trusted to not undermine the network intentionally.[31] That model was challenged, however, by divergent interests of its growing user base.[32] As its popularity expanded, anyone that could "borrow" a username and password from a colleague or friend could access the network.[33] This led to calls for greater vigilance in 1973 following two suspicious system crashes that were attributed to unauthorized users.[34] The first large-scale "insider attack" was executed in 1988 by Robert Morris, a graduate student at Cornell. Morris' purpose was not malicious; he was investigating machine-to-machine techniques for mapping ARPANET's true size and shape. His solution, however, turned out to be a type of malware known as a worm – a self-replicating application that propagates itself onto any computer it connects with. To make the software work, Morris took advantage of an operating system vulnerability that had been known about since the 1960s.[35] It is this event that launched computer defense into a full-fledged discipline.[36]

Surprisingly, despite nearly three decades and billions of dollars of public and private investment, cyber defense is still grounded in the same assumptions as ARPANET. This is typified by standard security architectures used in nearly all cyber systems: centrally controlled, fortress-like structures that can be likened to the layers of an onion. In these layered structures, authority is concentrated at the center and falls off rapidly away from it.[37] Similarly, access to the center is very limited, and access increases as one moves closer to the edge. Such nested, hierarchical structures have a logical consistency that, much like a fortress, espouses security. Yet for all their complexity and hierarchy, the security of these structures is still based on two assumptions; both of which have repeatedly been proven false. Those assumptions are secrets and trust.

Secrets are credentials, such as passwords or cryptographic keys, that help segregate insiders from outsiders. But secrets must remain secrets to be effective. The contradiction of secrets is that they must be shared with those that need them. This requires trust. In systems thinking, trust is not qualitative (e.g., a judgment of trustworthiness), but quantitative; it is derived from the trust of progressively higher authorities until one reaches the so-called "trust anchor" – the entity in which trust is assumed and not derived.[38] Thus, neither secrets nor trust can be assured – "secrets can be exposed and people can be compromised." [39] This lack of assurance has enabled some of the most notable hacks in the past two years. Edward Snowden, for example, exploited the trust of his insider position to not only copy thousands of highly classified files, but also to tamper with the audit logs that would have exposed his actions.[40] In the Target store hack, the attackers intercepted the username and password of a HVAC subcontractor with a network trust relationship with Target's business server.[41] In other words, they exploited a secret to exploit trust. This pattern is widely used in offensive cyber operations, including by the NSA's Tailored Access Office.[42] Thus, secrets and trust are an insufficient foundation for a cyber security strategy.

Ultimately, no matter how many echelons of trust and secrets exist, the networks owners are taking a leap of faith that neither will be compromised. The examples in this section show that such leaps are unwarranted. In place of faith and assumptions modern cyber defense should rely on tools that do not require secrets and trust, but rather on mathematically verifiable, unalterable truth.

III. BLOCKCHAIN TECHNOLOGY

What is a Blockchain?

A blockchain is a shared, distributed, tamper-resistant database that every participant on a network can share, but that no one entity control. In other words, a blockchain is a database that stores digital records. The database is shared by group of network participants, all of whom can submit new records for inclusion. However, those records are only added to the database based on the agreement, or consensus, of a majority of the group. Additionally, once the records are entered, they can never be changed or erased.[43] In sum, blockchains record and secure digital information in such a way that is becomes the group's agreed-upon record of the past.

Blockchain: A Brief History

The blockchain was first proposed in 2008 by Satoshi Nakamoto (a pseudonym) in conjunction with the cryptocurrency Bitcoin. Nakamoto's vision was to “allow online payments to be sent directly from one party to another without going through a financial institution.” [44] However, without a trusted central authority to oversee accounts and transactions there would be no way to prevent a dishonest actors from spending a single Bitcoin twice. Nakamoto's solution was a distributed database of time-stamped, consensus-based, cryptographically tagged transactions that form a record that cannot be changed – a blockchain.[45] Bitcoin became a reality in 2009 and since then its market capitalization has gone from zero to more than $6.3 billion, as of April 2016. Each day some of Bitcoin's 6.6 million users exchange more than $75 million in 120,000 transaction across the network.[46]

Bitcoin offers a noteworthy example of blockchain's potential. Every piece of Bitcoin currency, every Bitcoin transaction, and every Bitcoin account that has ever existed is recorded in a blockchain database that lives on the open internet. It is fully exposed to the hostile efforts of governments, criminal organization, and hackers. Yet the Bitcoin blockchain has never been hacked.[47] Clearly, this technology deserves study.

While "the blockchain" was virtually pseudonymous with Bitcoin for several years, it should be made clear that they are two separate technologies. Bitcoin is just the first popular application of blockchain, just as email was the first popular application of the internet.[48] Its potential is so vast, in fact, that advocates compare the maturity and innovative potential of blockchain technology today to that of the internet in 1992, an internet before the world wide web.[49] However, because blockchain technology simply rides on the existing internet infrastructure, the maturity of blockchain technology is likely to progress three times faster than the internet, with mainstream use expected within the next eight years.[50]

Industry has recognized the potential of blockchain technology. Since 2013, more than $1 billion of venture capital has been invested into 120 blockchain start-ups.[51] Their aims are diverse, ranging from finance, to the tracking and trade of indivisible assets, such as like diamonds and art, to digital notary services that can serve as evidence in a court of law. Interest has expanded beyond just start ups, however. Large, mature companies such as Lockheed Martin, IBM, and Goldman Sachs have also begun investigating potential blockchain applications in their respective sectors.[52]

Why Do Blockchains Matter?

Blockchains solve a challenging problem in data science of reliably exchanging information over an unreliable network on which some of the participants cannot be trusted.[53] The blockchain security model inherently assumes that these dishonest participants will attempt to create friction by not only generating false data, but also by attempting to manipulate valid data passed from honest participants.[54] By using a variety of messaging and consensus techniques, blockchains ensures data integrity by both rejecting invalid data and preventing valid data from being secretly modified or deleted.

Blockchain technology is worthy of examination because it offers three significant advantages over traditional cyber defense strategies. First, rather than trying to defend boundaries from compromise, blockchains assume compromise by both adversaries and trusted insiders. They are designed to defend data in a contested cyber environment. Second, blockchain networks harness the aggregate power of the network to actively resist the efforts of malicious actors. That is, blockchains take advantage of the asymmetry of many against few. Finally, the security that blockchains provide is not dependent on secrets or trust. There are no passwords to be exposed, cryptographic keys to be protected, or administrators to be trusted.[55] Blockchains provide an inherent security function on which additional security functions can be added, depending on the application. As result of these advantages, blockchains are capable of operating successfully and securely on the open internet, without a trusted central authority, and while fully exposed to hostile actors. Given their ability to protect the integrity of data in spite of adversary actions, blockchains offer significant military utility to the USAF to prevail in the highly contested environment of 2040.

Elements of Blockchain Technology

Like most technologies, blockchains combine other nascent technologies to provide a new, unique function or capability. This section explains some of technologies and functions they provide.

Hashing: the Digital Fingerprint

Blockchains employ a form of cryptography known as secure hash algorithms (SHA), or hashing.[56] Unlike encryption, secure hash algorithms do not use secrets, such as passwords or keys. Instead, hashing specifications are developed by the National Institute of Standards and Technology (NIST) and made publically available for use by both government and private entities. Hashing is used to convert any piece of digital information (i.e., text, images, videos, etc) to a string of bits with a prescribed length. For instance, digital information processed through the SHA-256 algorithm will output as a 256-bit string, equivalent to a 32-character string of alpha-numeric text. Secure hashes have two important properties. First, the algorithm only works in one direction. That is, the input cannot be derived from the output. Second, the output string is universally unique to any universally unique input.[57] Processing the same piece of information through the same hash algorithm will always return the same result, and no other input will produce the same output. Changing any portion of an input – even one character – will significantly alter the output.[58] Table 1 illustrates this point. The geographic coordinates of the Washington Monument were processed through the SHA-1 hash algorithm, resulting in the first string of 40 alphanumeric characters. The location was processed again after changing the longitude's fourth decimal place by one increment, resulting in an offset of 8.5 meters. Notice that the resulting hash differs from the original almost completely. A similar change could be expected from changing one pixel in an image or one letter of the US Constitution. Thus, hashing is an effective tool for verifying the integrity of a piece of data without having to inspect the data directly.

Input	Output of Secure Hash Function (SHA-1)
38.8895° N, 77.0353° W	7D08E44FC738843F23A73CDDAEB7964A0BE0CF0D
38.8895° N, 77.0354° W	56B7C2499D243F971595E367E458BE0694250D88

Table 1: Example input and output of secure hash function

Database Structure and Its Contents

A blockchain is a database composed of "blocks" (e.g., a group) of records, with each block containing a cryptographic link to the previous block, forming a chain. A blockchain begins as a single block, sometimes called the *genesis block*.[59] As new blocks are added they are "stacked" on top of the previous block. A visualization of a blockchain can be seen in Figure 2. Blockchains can be compared to pages in a book.[60] Each block, or page, has a header (e.g., identifying information at the top of the page) and contents (e.g., text).[61] The header of each block contains several pieces of information, but only three are highlighted here. First, and most importantly, is the digital fingerprint, or hash, of the previous block. Next is a timestamp that denotes when the block was created. Finally, there is the hash of the block's contents.[62]

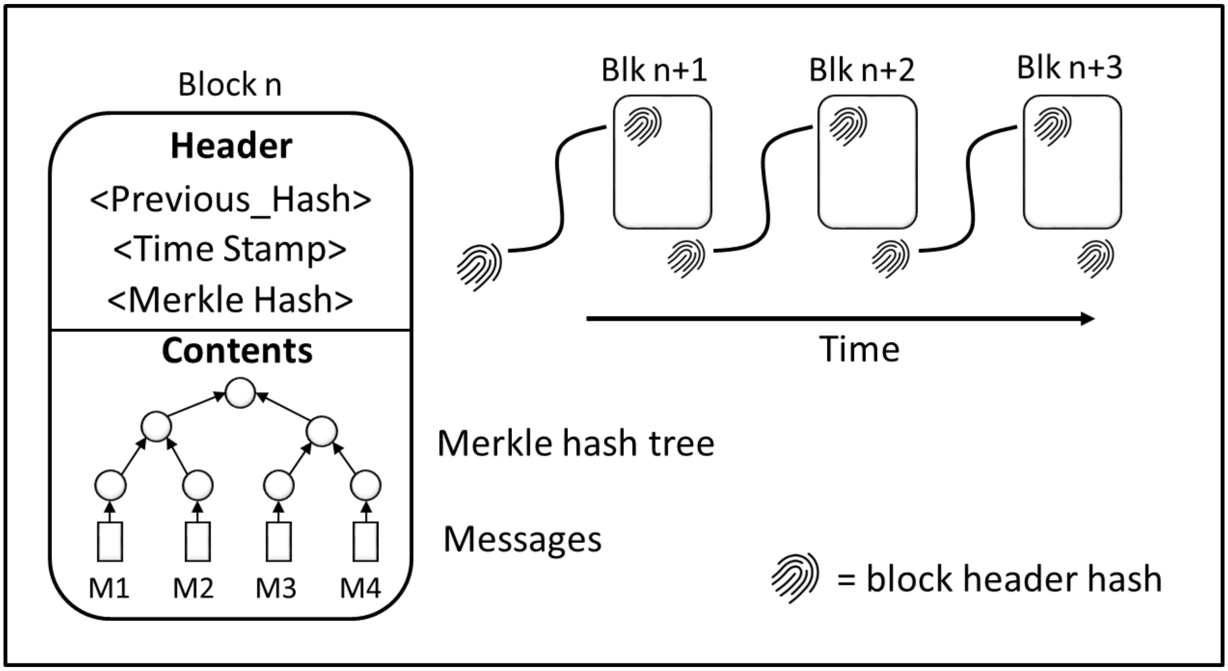

Figure 2: Visualization of blockchain data structure

This content hash is also known as a Merkle hash, which is the highest value of a Merkle hash tree. The Merkle hash tree is a cryptographic data structure that mathematically links the entirety of a block's contents to a single hash value. This allows any user to rapidly reconstruct any block to quickly confirm the integrity of its contents using the least amount of information. By linking each block to the one before it, the blockchain has an internal consistency that can be verified without ever inspecting the contents of any block, just as one can verify the presence of every page in a book without reading it.[63] This paper's section on blockchain security will illuminate the importance of this data structure.

The collection of information stored in each block can be any digital content, including simple text, structured messages, images, and videos. Any information stored in the blockchain is permanently secured – a historical record that can never be changed.

There are two fundamental trade-off to consider in determining a blockchain's contents: confidentiality and file size. Anything stored in the blockchain can be viewed by all network participants. This has obvious advantages (e.g., the ability to easily authenticated information across the network) and disadvantages (e.g., cannot control who in the network can see the information). Further discussion on confidentiality is addressed in this paper's section on security. File size is important because a complete blockchain contains every data record that has ever been added to it. If the data records are large and added frequently, then the blockchain will become enormous, a problem known as *bloat*.[64] Bloat becomes more problematic in decentralized blockchain networks, where multiple network nodes will independently construct the database.

Consensus mechanism

Consensus is a process that enables "a set of distributed processes [to] achieve agreement on a value or an action despite a number of faulty processes." [65] This is formally known as the Byzantine General's Problem.[66] One of the best known consensus algorithms, known as practical Byzantine fault tolerance (PBFT), is used pervasively in safety critical systems, such as quad-redundant navigation systems aboard aircraft.[67] In a blockchain network, consensus is used to prevent dishonest actors from writing potentially invalid information to the database.[68] The specific consensus mechanism used for any given blockchain depends on a number of assumptions, including the amount of trust between parties and the alignment of their interests, as well as factors concerning the shape and synchronization of the network.[69] The Bitcoin consensus model, for example, is decentralized and without trust. As a result, each node independently verifies each transaction; independently verifies new blocks; and, in case of "forks" in the blockchain, independently chooses the branch with the most cumulative computation.[70] Militarily, the consensus mechanism creates asymmetric advantage over an adversary by aligning the preponderance of honest nodes against a smaller number of dishonest nodes. Consequently, the blockchain becomes increasingly difficult to compromise as the network size increases.

Network architecture

Blockchains can be established on a variety of network architectures ranging from completely centralized to completely distributed, as illustrated in Figure 3.[71] It is important to note, however, that each of these network architectures represent trade-offs in security and efficiency. For instance, in a centralized network, all the outer nodes are reliant on the center node for network functionality. Thus, if the center node becomes compromised then the network

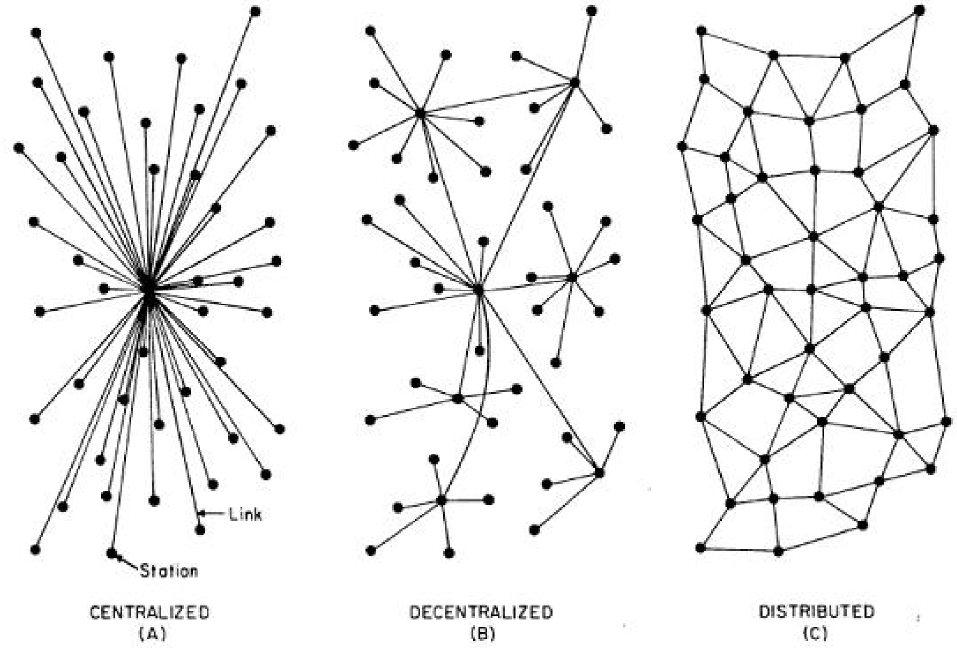

Figure 3: Diagram of generic network topologies[72]

as a whole is subject to compromise. At the other end of the spectrum is the distributed network, where each node is functionally independent from any other node. As a result, the compromise of individual distributed nodes does not necessarily compromise of network as a whole.[73]

Access control

Access control of blockchains can be accomplished in two ways: permissioned and unpermissioned. Unpermissioned, or public, blockchains operate without access control. Anyone with the appropriate software and connectivity can join the network and interface with the blockchain without permission from a central authority. Conversely, a permissioned, or private blockchain provides allows administrators to control the participants on the network, the portions of the blockchain that can be viewed, who can write to the blockchain, and even who composes the consensus group.[74]

Network Nodes Types

Network nodes serve as both the users and defenders of the blockchain. As users, they both generate new records to be included in the blockchain and reference the blockchain for historical information. Network nodes defend the blockchain by participating in the consensus mechanism, although not all nodes need participate in every aspect of consensus, depending on access control, for instance. The types of nodes in any blockchain network will vary depending on the network's purpose.

In an Air Force context, nodes could be envisioned in three categories, depending on their relative capability (e.g., processing, storage, communication, etc). These categories include Full Nodes, Partial Nodes, and Simple Nodes. Examples and responsibilities of each node type are summarized in Table 2. Full Nodes serve as the backbone of the blockchain network. Their most important function is to build and maintain a complete, up-to-date copy of the blockchain database. Another important function performed by full nodes is generating new blocks, which are then distributed to other nodes. Next, full nodes will verify new transactions or blocks received from other nodes, ensuring they are in accordance with the consensus rules and maintain the database's internal consistency. Finally, like all other nodes, Full Nodes generate and transmit new records for inclusion in the database.

Type	Example	Responsibilities (rank ordered)
Full	Server / Desktop AOC AWACS Tactical platform GEO satellite	• Independently constructs complete copy of blockchain • Generates blocks • Verifies blocks • Verifies all records • Generates and transmits new records
Partial	Laptop LEO Satellite Small UAV	• Constructs "headers-only" copy of blockchain • Verify new blocks • Verify new records • Verify old records with peer support • Generate and transmit new records
Simple	Cell phone Attritable UAV	• Verify new records • Generates and transmits new records

Table 2: Example of blockchain node types in an Air Force network

The next category type is a Partial Node. Due to platform design constraints, partial nodes lack sufficient capability to maintain a complete copy of the blockchain database. Instead, a Partial Node retains a "headers-only" version of the blockchain containing just the headers of every block. Recall that the block headers contain the previous block’s header hash, a timestamp, and the hash of the current block's contents. This allows the Partial Node to not only verify the consistency of the blockchain, but also to completely verify every new block. Once verified, only the block's header data in retained. In Bitcoin, this limited blockchain model reduces the database's size from 45 gigabytes to just 45 megabytes, a factor of 1,000. However, because the block's contents are discarded, a Partial Node requires the support of full nodes to verify any previous transaction.

The final category type is a Simple Node. As can be seen in Table 2, Simple Nodes only generate, transmit and verify new records. Simple nodes are, by design, low-cost commoditized items with limited capability. However, the presence on the network could still serve a valuable role in the consensus mechanism.

Security and Attack Vectors

The strength of blockchain security is attributable to its core elements: secure hashing, the back-linked data structure, and the consensus mechanism. First, the hash is not secured by a secret key; it is simply a universally unique cryptographic representation of a piece of data – a digital fingerprint. Recall that the hash of the previous block is embedded in the header of the current block, which directly affects the current block's own hash. Thus, if the previous block changes in *any way*, its hash will change, which will affect the hash of the current block and every block thereafter.[75] As a result, making changes to the data in a blockchain becomes more difficult the farther back the change is implemented; an attacker must re-compute not only the target block, but every block after it as well, which is both time and resource intensive. As a general rule, any block with six additional blocks on top of it is considered irrevocable.[76] Finally, the rules of the consensus mechanism control which new data entries are transmitted, verified, and ultimately appended to the blockchain. Consensus makes use of the blockchain's internal consistency, which any node can easily verify. Any data entry or block that breaks that consistency is immediately obvious to honest observers and is ignored. Together, these three elements build a database of historical records that is considered *immutable*, or unable to change.[77]

Confidentiality is an important issue for blockchain security. Anything in the blockchain can be viewed by all permissioned users in the network. However, additional security measures can be added to blockchain network. One example is traditional public key infrastructure, which is used DOD common access cards and network tokens. This approach allows a data owner to encrypt a record, store it in the blockchain, and subsequently maintain control access to it.. This approach has been adopted in Estonia, which now protects every citizen's healthcare record inside a blockchain. The patient (i.e., the data owner) can now control which healthcare providers have access to her healthcare record, inspect the changes that have been made to the record, and revoke access when it is no longer necessary.[78]

Because records become extremely difficult to alter once secured in the blockchain, the target for attackers becomes new records, both valid or invalid.[79] The vector for executing attacks on a blockchain is through the consensus mechanism. By controlling a majority of the consensus nodes, attackers could control the content added to the blockchain in two ways. First, attackers could independently generate, transmit, verify, and secure invalid transactions that would normally be rejected by honest nodes. Second, attackers can conduct a denial of service attack against honest nodes by simply ignoring any messages the attackers did not generate themselves.[80] While certainly possible, the chance of a consensus attack succeeding is mitigated by three factors: network size, identity management, and access controls. As the number of consensus nodes increases, so too does the effort required for an attacker to control its majority. Thus, larger networks provide greater security. Additionally, identify management and access controls prevent the so-called "Sybil attack," wherein individual attackers create multiple identities to control a disproportionate number of consensus nodes.[81]

IV. APPLICATIONS IN NATIONAL DEFENSE

Blockchain technology has utility in national defense applications. This section describes three specific, near-term use cases where blockchains offer utility in both operational and support roles.

Cyber Defense: Data integrity

Cyber defense is the most near-term, low-cost, high-payoff application of blockchain technology. As discussed earlier, cyber security relies on secrets and trust to maintain security, but neither can be assured. Blockchains operate independent of secrets and trust. Edward Snowden abused the trust of his administrator role to copy privileged files and then tampered with the audit logs that monitored his actions. He deleted a truth.

Blockchains preserve truths in two ways. First, they ensure digital events are widely witnessed by transmitting them to other nodes on the blockchain network. Then, using consensus, those events are secured in a database that can never be altered by a single adversary.

Blockchains also enhance cyber defense's perimeter security strategy, not by helping to hold up the walls, but by monitoring the walls and everything within them. The growing complexity of modern systems, including weapon systems, make vulnerabilities both more likely and less detectable. "Instead of searching for vulnerabilities, equivalent to searching for a needle in a haystack, you can [monitor] every stalk of hay, every digital asset that constitutes the system you want to protect."[82] Malware attacks against systems are integrity attacks against their configurations. Using blockchain, the configurations of every component in the system can be imaged, hashed, secured in the database, and continually monitored. Any unscheduled change to any configuration, no matter how small, can be detected almost instantly.

Supply chain management

There is growing anxiety about supply chain management for defense systems, which increasingly use commercial-off-the-shelf components for embedded software systems. The concern is that these components may contain deliberate vulnerabilities that could be exploited by an adversary at the time of his choosing. This threat was sensationalized in the novel *Ghost Fleet,* in which China disabled the entire fleet of F-35 aircraft using an intentionally embedded flaw in a commodity circuit card. Thus, this issue is one of *provenance,* or the ability to establish the origin and traceable ownership of an asset.

Blockchains offer a solution that could establish the provenance of every circuit board, processor, and software component from "cradle to cockpit." The card design firm could use blockchains to log every design iteration of a circuit. Manufacturers could log every model and serial number of every card it produced. Finally, distributors could log the sale of batches of circuits to system integrators, who could log the allocation of circuits to specific aircraft assemblies, and so on. In this context, blockchains create a permanent records for the transfer of *assets* between *owners,* thereby establishing provenance.

Such a system also has clear benefits for both DOD and industry beyond a system's production phase. Many weapon systems are designed with service lives of 30 years or more. However, the computing technologies these systems use are rarely produced for more than a decade. As a result, replacing obsolete parts becomes more difficult with time. Additionally, federal law prevents DOD from using any component whose provenance cannot be established; any discontinuity in ownership renders some parts unusable even though they are functional and in high demand. In addition to helping DOD to support legacy systems, resellers would have an economic incentive to track specifically identified COTS components in a blockchain to maintain their provenance, which in turn increases their value.

Resilient Communications

Blockchain technology can provide resilient communications in a highly contested environment. In a high-end conflict, DOD should be prepared for the adversary to contest the electromagnetic spectrum, particularly against critical communication systems such as satellites, undersea cables, and tactical datalinks. Additionally, adversaries will attempt to manipulate the data used to complete the kill chain. Countering this threat will require the capability to securely generate, protect, and share data that is impervious to these adversary actions. Blockchain networks are uniquely able to provide these capabilities.

The Bitcoin network demonstrates these capabilities. Bitcoin is relatively immune to suppression due to the mutually reinforcing nature of its security protocols, which include its messaging system, the adaptability of its protocol to various communication mediums, the distributed blockchain database, and the consensus mechanism.[83] Bitcoin uses a peer-to-peer messaging model that propagates every message to every active node across the world within seconds. Every node on the Bitcoin network contributes to this service, including smartphones. If a node's terrestrial, wireless, or satellite internet service is disrupted, a bitcoin message can be sent through alternate channels, such as high-frequency radio, fax or even transcribed into a barcode and hand-carried.[84] However it is received, the servicing node will verify the message, then retransmit it to every connected peer. Some of those peers are the 7,000 full nodes that are can independently aggregating messages into new blocks.[85] Because there is no "master" centralized node to disrupt, the network will continue to operate even if large portions become disconnected. Finally, the consensus mechanism ensures that invalid messages and blocks, generated by dishonest actors, are ignored. Together, these protocols ensure that verified message traffic is reliably transmitted across the world, despite malicious attacks against communication paths, individual nodes, or the blockchain itself.

V. CONCLUSIONS AND RECOMMENDATIONS

The ability of the USAF to prevail in the highly contested environment of 2040 will be dictated by its ability to successfully conduct data-fighting operations. That is, protecting one's ability to generate, store, disseminate, process, analyze, and exploit information while interfering with the adversary's ability to do the same. Clearly, this requires a means of defending cyber-enabled systems from compromise. Yet contemporary cyber defense is faltering and is unlikely to improve given the evolving cyber threat. This threat includes not only a growing array of malware and embedded computing devices, but also an adversary strategy that favors data manipulation over simple data theft. Thus, for the USAF to prevail in data-fighting it needs to develop a model of cyber defense that addresses the failings of today’s strategy and the future threat.

Blockchain technology offers such a model. Blockchains break with many of the flawed assumptions of traditional network security. First, blockchains are trustless; they assume compromise by both insiders and outsider. Second, blockchains are transparently secure; they do not rely on failure-prone secrets, but rather on a cryptographic data structure that provides a secure foundation on which to add additional security protocols. Finally, blockchains are fault tolerant; they use algorithmic consensus mechanisms to align the efforts of honest nodes to reject those that are dishonest. Together, these properties allow system designers to rethink the fundamental architectures of cyber systems and networks.

The USAF should continue to explore blockchain technology for use in national defense applications. The following recommendations represent a path for this exploration.

Recommendation #1: Develop organic government expertise in blockchain technology. There is currently limited awareness or knowledge of blockchain technology within the USAF. To combat this, the USAF should establish a line of research within AFRL to explore the potential blockchain technology. Research is needed to ensure that blockchains are sufficiently scalable, adaptable, and secure to support the USAF's broad array of missions in the air, space, and cyber domains. AFRL's research should specifically be conducted in conjunction with AFIT and USAFA research projects to not only harness the innovative spirit of the USAF's brightest junior officers, but also to grow a cadre of scientists and engineers familiar with blockchain technology.

Recommendation #2: Partner with industry. The USAF should seek partnering opportunities with industry to cooperatively and collaborative develop blockchain-based technologies for mutual benefit. The USAF and industry share many common challenges, including the scourge of cybercrime and industrial espionage. Blockchain technology offers a new model of security and trust that could significantly mitigate a growing cyber threat. Silicon Valley, large technology firms, and the defense sector have demonstrated their interest and intent to develop new applications; the USAF should harness that momentum.

VI. BIBLIOGRAPHY

"A History of the ARPANET: The First Decade." Defense Advanced Research Projects Agency, April 1, 1981.

"Advanced Threat Analytics | Microsoft." Accessed March 17, 2016. https://www.microsoft.com/en-us/server-cloud/products/advanced-threat-analytics/overview.aspx.

Anthony Lewis. "A Gentle Introduction to Blockchain Technology." *Bits on Blocks*, September 9, 2015. http://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/.

Antonopoulos, Andreas. *Banking, Issue 15, Evidence - October 8, 2014*, 2014. http://www.parl.gc.ca/content/sen/committee/412/BANC/15EV-51627-E.HTM.

Antonopoulos, Andreas M. *Mastering Bitcoin*. Oreilly & Associates Inc, 2014.

Baran, Paul. "On Distributed Communications." Product Page, 1964. http://www.rand.org/pubs/research_memoranda/RM3420.html.

"Beyond Distributed and Decentralized: What Is a Federated Network?" *Institute of Network Cultures*. Accessed March 30, 2016. http://networkcultures.org/unlikeus/resources/articles/what-is-a-federated-network/.

"Blockchain Implications for Trust in Cybersecurity." Guardtime Federal, February 17, 2016.

"Brief History of the Internet." Internet Society, October 15, 2012. http://www.internetsociety.org/brief-history-internet.

Bruce Schneier. "Crypto-Gram: February 15, 2016 - Schneier on Security," February 15, 2016. https://www.schneier.com/crypto-gram/archives/2016/0215.html#2.

CFA, Evan Niu. "How Many iPhones Has Apple Sold? -." *The Motley Fool*. Accessed May 27, 2016. http://www.fool.com/investing/general/2015/11/14/iphones-sold.aspx.

Cheryl Pellerin. "Rogers: Data Manipulation, Non-State Actor Intrusions Are Coming Cyber." *U.S. DEPARTMENT OF DEFENSE*. Accessed March 3, 2016. http://www.defense.gov/News-Article-View/Article/630495/rogers-data-manipulation-non-state-actor-intrusions-are-coming-cyber-threats.

Cisco. "The Internet of Things [INFOGRAPHIC]." *blogs@Cisco - Cisco Blogs*. Accessed March 17, 2016. http://blogs.cisco.com/diversity/the-internet-of-things-infographic.

Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-01 Counterair Operations." US Air Force, October 27, 2015. https://doctrine.af.mil/download.jsp?filename=3-01-ANNEX-COUNTERAIR.pdf.

Dang, Quynh H. "Secure Hash Standard." National Institute of Standards and Technology, July 2015. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

David Wessel. "Panel Discussion: Beyond Bitcoin: The Future of Blockchain and Disruptive Financial Technologies," January 14, 2016. http://www.brookings.edu/~/media/events/2016/01/14-bitcoin/20160114_blockchain_bitcoin_transcript.pdf.

Douceur, John R. "The Sybil Attack - Microsoft Research." *Proceedings of 1st International Workshop on Peer-to-Peer Systems*. Accessed April 4, 2016. http://research.microsoft.com/apps/pubs/default.aspx?id=74220.

Driscoll, Kevin, Brendan Hall, Håkan Sivencrona, and Phil Zumsteg. "Byzantine Fault Tolerance, from Theory to Reality." In *Computer Safety, Reliability, and Security*, edited by Stuart Anderson, Massimo Felici, and Bev Littlewood, 235–48. Lecture Notes in Computer Science 2788. Springer Berlin Heidelberg, 2003. http://link.springer.com/chapter/10.1007/978-3-540-39878-3_19.

Eric Piscini, Joe Guastella, Alex Rozman, and Tom Nassim. "Blockchain: Democratized Trust: Distributed Ledgers and the Future of Value," February 24, 2016. http://dupress.com/articles/blockchain-applications-and-trust-in-a-global-economy/.

Finley, Klint. "How the Tech Behind Bitcoin Could Stop the Next Snowden." *WIRED*, June 2, 2015. http://www.wired.com/2015/06/tech-behind-bitcoin-stop-next-snowden/.

Gault, Mike. "Forget Bitcoin — What Is the Blockchain and Why Should You Care?" *Re/code*, July 5, 2015. http://recode.net/2015/07/05/forget-bitcoin-what-is-the-blockchain-and-why-should-you-care/.

Gibbs, Nancy, and Lev Grossman. "Here's the Full Transcript of TIME's Interview With Apple CEO Tim Cook." *Time*, March 17, 2016. http://time.com/4261796/tim-cook-transcript/.

Global Horizons: Final Report: United States Air Force Global Science and Technology Vision. AF/ST TR 13-01. Chief Scientist, United States Air Force, 2013.

Granville, Kevin. "9 Recent Cyberattacks Against Big Businesses." *The New York Times*, February 5, 2015. http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html.

Hammond, Grant. *The Mind of War: John Boyd and American Security*. Smithsonian Institution, 2012.

"'Information Integrity' among Top Cyber Priorities for U.S. Gov't, Clapper Says." *SC Magazine*, September 11, 2015. http://www.scmagazine.com/news/intelligence-committee-hosts-cybersecurity-hearing/article/438202/.

Intel. "A Guide to the Internet of Things Infographic." *Intel*. Accessed March 17, 2016. http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

Kaushal, Mohit, and Sheel Tyle. "The Blockchain: What It Is and Why It Matters." *The Brookings Institution*. Accessed February 25, 2016. http://www.brookings.edu/blogs/techtank/posts/2015/01/13-blockchain-innovation-kaushal.

Lamport, Leslie. "The Byzantine Generals Problem." *ACM Trans. Program. Lang. Syst.* 4 (1982): 382–401. doi:10.1145/357172.357176.

Johnson, Matt. "Matt Johnson's Keynote at Asia Cyber Liability Conference in Singapore — Guardtime." *Guardtime*, July 2, 2016. https://guardtime.com/blog/matt-johnsons-keynote-at-asia-cyber-liability-conference-in-singapore.

Miguel Correia, Giuliana Santos Veronese, Nuno Ferreira Neves, and Paulo Verissimo. "Byzantine Consensus in Asynchronous Message-Passing Systems: A Survey." *International Journal of Critical Computer-Based Systems* 2, no. 2 (2011): 141–61.

Morgan, Lewis. "List of Data Breaches and Cyber Attacks in 2015 – over 290 Million Leaked Records." *LinkedIn Pulse*, December 15, 2015. https://www.linkedin.com/pulse/list-data-breaches-cyber-attacks-2015-over-290-million-lewis-morgan.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

https://bitcoin.org/bitcoin.pdf.

Nils, Diewald. "Decentralized Online Social Networks." In *Handbook of Technical Communication*, 461–505. Berlin/Boston, 2012. http://www.nils-diewald.de/dsn-chapter.html.

Seltzer, Larry. "The Morris Worm: Internet Malware Turns 25." *ZDNet*. Accessed April 3, 2016. http://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/.

Swan, Melanie. *Blockchain : Blueprint for a New Economy*. Oreilly & Associates Inc, 2015.

Swanson, Tim. "Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems." Working paper, April 6, 2015. http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributedledgers.pdf.

"The DoD Cyber Strategy." Department of Defense, April 1, 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

"The Great Chain of Being Sure about Things." *The Economist*, October 31, 2015. http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

"The Trust Machine | The Economist." *The Economist*, October 31, 2015. http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

Timberg, Craig. "The Real Story of How the Internet Became so Vulnerable." *Washington Post*. Accessed March 23, 2016. http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

US Census Bureau, Demographic Internet Staff. "International Programs, International Data Base." Accessed March 17, 2016. https://www.census.gov/population/international/data/idb/worldpopgraph.php.

U.S. Joint Chiefs of Staff. "Joint Publication 3-12 (R), Cyberspace Operations." Accessed April 6, 2016. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Valentino-DeVries, Jennifer, and Danny Yadron. "Cataloging the World's Cyberforces." *Wall Street Journal*, October 12, 2015, sec. Tech. http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

Walters, Riley. "Continued Federal Cyber Breaches&#160;in 2015." *The Heritage Foundation*. Accessed March 17, 2016. http://www.heritage.org/research/reports/2015/11/continued-federal-cyber-breaches-in-2015.

Welsh, Mark A. "Selection as a Blue Horizons Fellow for Academic Year 2016," July 1, 2015.

Work, Robert O. "Reagan Defense Forum: The Third Offset Strategy." *U.S. DEPARTMENT OF DEFENSE*. Accessed March 17, 2016. http://www.defense.gov/News/Speeches/Speech-View/Article/628246/reagan-defense-forum-the-third-offset-strategy.

Zetter, Kim. "NSA Hacker Chief Explains How to Keep Him Out of Your System." *WIRED*, January 28, 2016. http://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/.

VII. NOTES

1. Gen Mark A. Welsh, "Selection as a Blue Horizons Fellow for Academic Year 2016," July 1, 2015.

2. Grant Hammond, *The Mind of War: John Boyd and American Security* (Smithsonian Institution, 2012).

3. Curtis E. LeMay Center for Doctrine Development and Education, "Annex 3-01 Counterair Operations" (US Air Force, October 27, 2015), https://doctrine.af.mil/download.jsp?filename=3-01-ANNEX-COUNTERAIR.pdf.

4. Ibid.

5. U.S. Joint Chiefs of Staff, "Joint Publication 3-12 (R), Cyberspace Operations," accessed April 6, 2016, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

6. Mohit Kaushal and Sheel Tyle, "The Blockchain: What It Is and Why It Matters," *The Brookings Institution*, accessed February 25, 2016, http://www.brookings.edu/blogs/techtank/posts/2015/01/13-blockchain-innovation-kaushal.

7. Work, "Reagan Defense Forum: The Third Offset Strategy," *U.S. DEPARTMENT OF DEFENSE*, accessed March 17, 2016, http://www.defense.gov/News/Speeches/Speech-View/Article/628246/reagan-defense-forum-the-third-offset-strategy.

8. Intel, "A Guide to the Internet of Things Infographic," *Intel*, accessed March 17, 2016, http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

9. Cisco, "The Internet of Things [INFOGRAPHIC]," *blogs@Cisco - Cisco Blogs*, accessed March 17, 2016, http://blogs.cisco.com/diversity/the-internet-of-things-infographic.

10. US population: 6.6 billion (2006) and 7.7 billion (2020). Demographic Internet Staff US Census Bureau, "International Programs, International Data Base," accessed March 17, 2016, https://www.census.gov/population/international/data/idb/worldpopgraph.php.

11. Given the uncertainty of the IoT projection in 2020, the author chose to not include a projection for 2040.

12. Nancy Gibbs and Lev Grossman, "Here's the Full Transcript of TIME's Interview With Apple CEO Tim Cook," *Time*, March 17, 2016, http://time.com/4261796/tim-cook-transcript/.

13. Evan Niu CFA, "How Many iPhones Has Apple Sold? -," *The Motley Fool*, accessed May 27, 2016, http://www.fool.com/investing/general/2015/11/14/iphones-sold.aspx.

14. *Global Horizons: Final Report: United States Air Force Global Science and Technology Vision*, AF/ST TR 13-01 (Chief Scientist, United States Air Force, 2013).

15. Jennifer Valentino-DeVries and Danny Yadron, "Cataloging the World's Cyberforces," *Wall Street Journal*, October 12, 2015, sec. Tech, http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

16. Kevin Granville, "9 Recent Cyberattacks Against Big Businesses," *The New York Times*, February 5, 2015, http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html.

Notes

17. Riley Walters, "Continued Federal Cyber Breaches&#160;in 2015," *The Heritage Foundation*, accessed March 17, 2016, http://www.heritage.org/research/reports/2015/11/continued-federal-cyber-breaches-in-2015.

18. "Advanced Threat Analytics | Microsoft," accessed March 17, 2016, https://www.microsoft.com/en-us/server-cloud/products/advanced-threat-analytics/overview.aspx.

19. Lewis Morgan, "List of Data Breaches and Cyber Attacks in 2015 – over 290 Million Leaked Records," *LinkedIn Pulse*, December 15, 2015, https://www.linkedin.com/pulse/list-data-breaches-cyber-attacks-2015-over-290-million-lewis-morgan.

20. Bruce Schneier, "Crypto-Gram: February 15, 2016 - Schneier on Security," February 15, 2016, https://www.schneier.com/crypto-gram/archives/2016/0215.html#2.

21. Cheryl Pellerin, "Rogers: Data Manipulation, Non-State Actor Intrusions Are Coming Cyber," *U.S. DEPARTMENT OF DEFENSE*, accessed March 3, 2016, http://www.defense.gov/News-Article-View/Article/630495/rogers-data-manipulation-non-state-actor-intrusions-are-coming-cyber-threats.

22. "'Information Integrity' among Top Cyber Priorities for U.S. Gov't, Clapper Says," *SC Magazine*, September 11, 2015, http://www.scmagazine.com/news/intelligence-committee-hosts-cybersecurity-hearing/article/438202/.

23. "The DoD Cyber Strategy" (Department of Defense, April 1, 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

24. "'Information Integrity' among Top Cyber Priorities for U.S. Gov't, Clapper Says."

25. Cheryl Pellerin, "Rogers."

26. Ibid.

27. "Brief History of the Internet" (Internet Society, October 15, 2012), http://www.internetsociety.org/brief-history-internet.

28. "A History of the ARPANET: The First Decade" (Defense Advanced Research Projects Agency, April 1, 1981).

29. Ibid.

30. Ibid.

31. Craig Timberg, "The Real Story of How the Internet Became so Vulnerable," *Washington Post*, accessed March 23, 2016, http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

32. Ibid.

33. Ibid.

34. Ibid.

35. Ibid.

36. Larry Seltzer, "The Morris Worm: Internet Malware Turns 25," *ZDNet*, accessed April 3, 2016, http://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/.

Notes

37. Andreas Antonopoulos, *Banking, Issue 15, Evidence - October 8, 2014*, 2014, sec. Standing Senate Committee on Banking, Trade and Commerce, http://www.parl.gc.ca/content/sen/committee/412/BANC/15EV-51627-E.HTM.

38. Andreas M Antonopoulos, *Mastering Bitcoin* (Oreilly & Associates Inc, 2014), chap. 10.

39. Matt Johnson, "Matt Johnson's Keynote at Asia Cyber Liability Conference in Singapore — Guardtime," *Guardtime*, July 2, 2016, https://guardtime.com/blog/matt-johnsons-keynote-at-asia-cyber-liability-conference-in-singapore.

40. Klint Finley, "How the Tech Behind Bitcoin Could Stop the Next Snowden," *WIRED*, June 2, 2015, http://www.wired.com/2015/06/tech-behind-bitcoin-stop-next-snowden/.

41. Granville, "9 Recent Cyberattacks Against Big Businesses."

42. Kim Zetter, "NSA Hacker Chief Explains How to Keep Him Out of Your System," *WIRED*, January 28, 2016, http://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/.

43. Mike Gault, "Forget Bitcoin — What Is the Blockchain and Why Should You Care?," *Re/code*, July 5, 2015, http://recode.net/2015/07/05/forget-bitcoin-what-is-the-blockchain-and-why-should-you-care/.

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

45. Ibid.

46. "The Great Chain of Being Sure about Things," *The Economist*, October 31, 2015, http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

47. Antonopoulos, *Antonopolis Testimony*, sec. Standing Senate Committee on Banking, Trade and Commerce.

48. Melanie Swan, *Blockchain : Blueprint for a New Economy* (Oreilly & Associates Inc, 2015), chap. 2.

49. David Wessel, "Panel Discussion: Beyond Bitcoin: The Future of Blockchain and Disruptive Financial Technologies," January 14, 2016, http://www.brookings.edu/~/media/events/2016/01/14-bitcoin/20160114_blockchain_bitcoin_transcript.pdf.

50. Antonopoulos, *Antonopolis Testimony*, sec. Standing Senate Committee on Banking, Trade and Commerce.

51. Eric Piscini et al., "Blockchain: Democratized Trust: Distributed Ledgers and the Future of Value," February 24, 2016, 83, http://dupress.com/articles/blockchain-applications-and-trust-in-a-global-economy/.

52. "The Great Chain of Being Sure about Things."

53. Antonopoulos, *Mastering Bitcoin*, chap. 1.

54. Leslie Lamport, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.* 4 (1982): 382–401, doi:10.1145/357172.357176.

55. "Blockchain Implications for Trust in Cybersecurity" (Guardtime Federal, February 17, 2016).

Notes

56. "The Trust Machine | The Economist," *The Economist*, October 31, 2015, http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

57. Quynh H. Dang, "Secure Hash Standard" (National Institute of Standards and Technology, July 2015), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

58. "The Trust Machine | The Economist."

59. Antonopoulos, *Mastering Bitcoin*, chap. 7.

60. Anthony Lewis, "A Gentle Introduction to Blockchain Technology," *Bits on Blocks*, September 9, 2015, http://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/.

61. Ibid.

62. Antonopoulos, *Mastering Bitcoin*, chap. 7.

63. Anthony Lewis, "A Gentle Introduction to Blockchain Technology."

64. Swan, *Blockchain*, 6.

65. Miguel Correia et al., "Byzantine Consensus in Asynchronous Message-Passing Systems: A Survey.," *International Journal of Critical Computer-Based Systems* 2, no. 2 (2011): 141–61.

66. Lamport, "The Byzantine Generals Problem."

67. Kevin Driscoll et al., "Byzantine Fault Tolerance, from Theory to Reality," in *Computer Safety, Reliability, and Security*, ed. Stuart Anderson, Massimo Felici, and Bev Littlewood, Lecture Notes in Computer Science 2788 (Springer Berlin Heidelberg, 2003), 235–48, http://link.springer.com/chapter/10.1007/978-3-540-39878-3_19.

68. Tim Swanson, "Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems" (Working paper, April 6, 2015), http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributedledgers.pdf.

69. Miguel Correia et al., "Byzantine Consensus in Asynchronous Message-Passing Systems: A Survey."

70. Antonopoulos, *Mastering Bitcoin*, chap. 8.

71. Nils Diewald, "Decentralized Online Social Networks," in *Handbook of Technical Communication* (Berlin/Boston, 2012), 461–505, http://www.nils-diewald.de/dsn-chapter.html.

72. Paul Baran, "On Distributed Communications," Product Page, (1964), http://www.rand.org/pubs/research_memoranda/RM3420.html.

73. "Beyond Distributed and Decentralized: What Is a Federated Network?," *Institute of Network Cultures*, accessed March 30, 2016, http://networkcultures.org/unlikeus/resources/articles/what-is-a-federated-network/.

74. Anthony Lewis, "A Gentle Introduction to Blockchain Technology."

75. Antonopoulos, *Mastering Bitcoin*, chap. 7.

76. Ibid., chap. 2.

77. Eric Piscini et al., "Blockchain," 89.

78. Matt Johnson, "Johnson Keynote."

79. Antonopoulos, *Mastering Bitcoin*, chap. 8.

Notes

80. Ibid.

81. John R. Douceur, “The Sybil Attack - Microsoft Research,” *Proceedings of 1st International Workshop on Peer-to-Peer Systems*, accessed April 4, 2016, http://research.microsoft.com/apps/pubs/default.aspx?id=74220.

82. “Blockchain Implications for Trust.”

83. Antonopoulos, *Mastering Bitcoin*, chap. 5.

84. Ibid.

85. Swan, *Blockchain*, chap. 6.