Report

POTENTIAL USES OF BLOCKCHAIN BY THE U.S. DEPARTMENT OF DEFENSE

March 2020

Value Technology Foundation

This paper was produced by the Value Technology Foundation, a 501 c (3) Think Tank, with:

Table of Contents

DARREN SOTO
9TH DISTRICT, FLORIDA

WASHINGTON OFFICE
1507 LONGWORTH HOB
WASHINGTON, DC 20515
(202) 225-9889

KISSIMMEE DISTRICT OFFICE
804 BRYAN STREET
KISSIMMEE, FL 34741
(407) 452-1171

Congress of the United States

House of Representatives

Washington, DC 20515

April 1, 2020

To the Value Technology Foundation:

To continue its standing as a world leader in technological innovation, the United States needs to engage with policymakers, the private sector, and academia to promote the research and development of blockchain technology. While China and Russia have invested millions of dollars worth of research and development (R&D) into the technology, the policymakers of our country are still trying to understand what the technology is, and our regulators are still trying to enforce old laws on the new technology.

Blockchain technology is not an easy concept to understand. Neither was the internet at first. However, this cannot stand in our way of overlooking the implications and opportunities this technology can provide us. As the Department of Defense led the way on leadership with the internet from which our economy and private sector still benefit from, I once again asked and got added to the National Defense Authorization Act a required briefing by the DoD to Congress on ways blockchain technology can be utilized. Furthermore, to build on this success, we submitted language in this year's appropriations process asking for a report that included key findings of this briefing, an outline of recommended activities the Department of Defense would like to engage with related to blockchain and the costs associated with this requests, as well as an analysis of the potential benefit(s) of consolidating blockchain related research and development in the Department within a center of excellence. I hope this report is codified in the upcoming NDAA for fiscal year 2021.

As with any effort or undertaking, the Government cannot go at this on our own and so I am grateful today to see how fierce competitors in the private sector have collaborated together to provide a roadmap for ways the DoD could apply blockchain technology. When I see the creativity of thought in ways of applying blockchain technology to support the Department of Defense in this paper, I am reminded of what a free and democratic society can do when called into action.

Sincerely,

Darren Soto

Darren Soto

Introduction

This paper highlights existing use cases of blockchain, or more broadly speaking, distributed ledger technologies (DLT), which the U.S. Department of Defense (DoD) can study to determine how to best implement its applications. Please note that for the purpose of this paper, the terms DLT and blockchain will be used interchangeably, even though not all DLTs are blockchain-based.

Digital technologies have transformed warfare. Beginning with the emergence of Network Centric Operations in the 1990s, digital technologies have become the basis for U.S. weapons, tactics, and strategy.[1] Today, warfighters use connected devices to coordinate air strikes on the battlefield. Drones are controlled from thousands of miles away. Commanders watch real-time video streams of the battle space. Logistics and the broader supply chain are regulated and managed by complex digital technologies.

The next generation of emerging technologies, which includes Artificial Intelligence, smart drones, robots, and additive manufacturing, will make the U.S. military even more dependent on digital technology. In this environment, the U.S. military has become critically dependent on secure, timely, accurate and trusted data. Yet, as data has grown in importance, cyber warfare has emerged to challenge the U.S. in the digital space. Today, key U.S. defense assets, ranging from communication systems to supply chains, can be disrupted by bad actors attempting to degrade U.S. capabilities.

Any physical or electronic asset that can be digitized can be tracked using DLT technology, which produce incorruptible, decentralized, and digitized ledgers of transactions that record the exchange of information. Blockchain has the potential to create instrumental advances in the DoD's capability, coordination, and certainty for foundational military technologies that enable strategic, operational, and tactical defense superiority for the warfighter. Built with cryptographic encryption, multi-node consensus enforcements, and distributed architecture, DLTs are well-suited for multi-tenant global organizations seeking to enhance their coordination of data and activity and provenance of authenticity of assets or action.

The DoD can leverage DLTs for multi-domain command and control, acceleration of procurement, management of mobile device assets, enhancement of supply chains, and additive manufacturing, including the manufacture of aircraft and other parts. These technologies can bring trust and transparency to the construction and maintenance of physical assets by tracking the origination and entire supply chain of each part. DLTs also provide cybersecurity solutions for access monitoring, authenticity, and provenance of data, and can be used to increase the speed, automation, and coordination of any activity across the Department, including automation of the chain of command for authorizing signatories for operational logistics and the onboarding and transfer of personnel. This paper will discuss these and additional use cases.

[1] https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619

Briefing Requirements

Briefing on the use of blockchain technology for defense purposes: The Conference Report accompanying the National Defense Authorization Act for FY2020 as passed into law on December 15, 2019, directs the Under Secretary of Defense for Research and Engineering to provide, not later than 180 days after the date of the enactment of this Act, to the congressional defense committees a briefing on the potential use of distributed ledger technology for defense purposes. This briefing shall include an explanation of how distributed ledger technology may be used by the Department of Defense to: (1) Improve cybersecurity, beginning at the hardware level, of vulnerable assets such as energy, water, and transport grids through distributed versus centralized computing; (2) Reduce single points of failure in emergency and catastrophe decision- making by subjecting decisions to consensus validation through distributed ledger technologies; (3) Improve the efficiency of defense logistics and supply chain operations; (4) Enhance the transparency of procurement auditing; and (5) Allow innovations to be adapted by the private sector for ancillary uses. The briefing shall also include any other information that the Under Secretary of Defense for Research and Engineering determines to be appropriate.

Report link:
https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf (p. 2793 of 3,488)

Blockchain's Global Impact

What Is Blockchain?

Through the use of decentralized distributed ledgers that are hosted among groups of participants, blockchain enables near real-time concurrent access, validation, and recording by multiple, decentralized participants of any given blockchain in a "write-once, read many" manner. State-of-the art cryptographic techniques generate digital fingerprints and signatures for the data transactions. Data integrity is ensured due to the use of hack-resistant consensus or protocols to ensure all nodes are synchronized, along with digital signatures that authenticate the content. Ledgers are immutable, meaning that they cannot be changed without proper consensus, or agreement, among network participants. Any attempts to alter any block will alert the participants of the tampering attempt. "Smart contracts" can be created to apply business rules automatically as contractual or business obligations are met. The "distributed" nature of the ledger ensures that all participants, across different geographies and environments, can transact with a shared common view.

Different blockchain network types, i.e., public or private, have rules for participants' access privileges. Public blockchain technologies are open and consequently allow all participants complete access, while a private network's permissioning enables participants to only perform certain actions and access critical information as appropriate. Blockchains can be used to provide high-quality, trusted data on a large scale to track any assets and transactions that can be digitized, ranging from cryptocurrency to tracking or audit data for physical or digital objects (e.g., aircraft parts and ocean freight). *For further information regarding these technologies, please see Appendix A: What is Blockchain and Distributed Ledger Technology?*

Blockchain's Value Proposition to the Department Of Defense

Blockchain technology has the potential to change countless industries: logistics, supply chain, identity, financial management, deployment, track and trace, banking (i.e., through currency trading and meeting Know Your Customer (KYC)/ Anti-Money Laundering (AML) requirements), additive manufacturing, and many others. The technology has proven itself disruptive to counterterrorism, cyber-intrusion, defense, intelligence, and global monetary policy, in addition to currency valuation and manipulation. The Department of Defense helped usher in the era of the internet that positioned the U.S. as a global leader in the financial space, increased gross domestic product (GDP), and developed advanced defense capabilities through significant investments.

Keeping the U.S. the de-facto location for capital investment, technological advancement, and defense leadership is predicated on control, security, and innovation continuing to occur within the U.S. As nations around the world look to the power of cryptocurrency and blockchain technologies to reduce the U.S.'s capacity to be the world's trusted broker, the U.S.'s position as a global economic leader is at risk. With cyber-intrusion on the rise, the U.S. needs to invest in this technology to increase security and transparency across all industries. Investing in blockchain for defense purposes enables the U.S. to continue its leadership and innovation in cyberspace, which has become one of the most hotly contested battlegrounds on the planet.

A global strategy is needed. As blockchain is a distributed system that fosters trust and value, it can be valuable among domestic entities. However, blockchain becomes even more powerful when it is built out and deployed amongst allies and strategic participants around the world. Permissioned and private blockchain networks can become mediums of data-sharing and coordination among world intelligence agencies or shared coalition defense initiatives. With the right tools, blockchain networks can be monitored for unusual or nefarious activity. As both crypto- and fiat- backed currencies move towards blockchain enablement, money movement by terrorist organizations, money launderers, and drug cartels may be reduced significantly while real-time visibility into global assets is established. By exchanging information on cryptographically secured, decentralized ledgers using DLT technology, global efforts by the U.S. and its allies can become tamper-evident, which lessens and exposes the impact of foreign sabotage efforts in cyberspace.

Adversary Activity In Blockchain Technology: China & Russia

Our peer and potential adversary, China, has been extremely active in blockchain. In October of 2019, China's President Xi Jinping called for greater levels of research and investment into blockchain during a meeting with Communist Party officials. President Jinping noted blockchain would serve "an important role in the next round of technological innovation and industrial transformation," and that China wanted to gain an "edge" over other major countries in terms of blockchain research and development.[2]

China has issued the most web 3.0 patents, which use a decentralized internet model, i.e., through blockchain. Moreover, most of the biggest and most innovative web 3.0 firms are located in China. The Chinese Government is already rolling out coordinated blockchain development programs aimed at putting their country in the forefront. In March 2018 at a meeting of the Chinese Academy of Sciences and the Chinese Academy of Engineering, President Xi Jinping stated that, "ever since the start of the 21st century, a new generation of industrial revolution is substantially reshaping the global economic structure … with Artificial Intelligence, Internet of Things, and blockchain constantly making application breakthroughs."[3]

China sees cryptocurrency and blockchain as a means of controlling processes such as financial settlement across the world, and as a way to erode the U.S. Government's position as a provider of trust systems and banking for transactions. In addition, China has recognized the utility of DLT technology in other areas, as the Chinese Government has sanctioned and invested in over 500 blockchain projects across many sectors, including finance, industry, defense, currency, manufacturing, and logistics.

There has been substantial interest in blockchain within the Chinese military. An article in a People's Liberation Army (PLA) journal in 2018 argued that China's Defense and Security Agencies should leverage blockchain to manage the distribution of funds for intelligence operations, protect personnel and weapons life-cycle data from cyber-attacks, and make logistics

[2] https://www.businessinsider.com/china-bullish-on-blockchain-xi-jinping-2019-10
[3] https://www.ccn.com/chinese-president-xi-blockchain-breakthrough-is-reshaping-global-economic-structure/

operations safer. Overall, the Chinese Government is estimated to have spent $300 million in FY19 and an additional $1 billion in FY20 on blockchain-related initiatives.[4]

China's central bank also plans to put a digitized version of the renminbi, currently referred to as the Digital Currency Electronic Payment (DCEP)[5] into circulation by using blockchain before the end of 2020. It is reported that China's central bank is working on a pilot program with state-owned banks and telecom companies. DCEP will allow China to monitor anyone who uses DCEP as well as erode the role of the U.S. dollar as a global reserve currency where economic sanctions can be used in lieu of military actions.

Russia is also keen to adopt this new technology. In 2018, the Russian Ministry of Defense announced it was launching a research lab to analyze how blockchain technology can be used to mitigate cybersecurity attacks and to support military operations.[6] One of the priorities of the lab is the development of an intelligent system to detect and prevent cyber-attacks on important databases and weapons systems. The Ministry states that it hopes to build secure blockchain-based platforms that make it more difficult to hide traces of cyber-attacks while making it easier to track online intruders in their systems. Overall, Russia is investing heavily in the build out of elliptic-curve cryptography and digital signatures to be used only in Russian platforms to ensure that the next generation of cryptographic applications, including blockchain, are secured and address known vulnerability vectors.

Whether it is China establishing an offensive position for economic warfare and surveillance on the U.S. or Russia creating a defensive position with DLT technology that will make critical information-gathering on Russia's communications and systems, the two superpowers that pose the greatest threat to the U.S. are both heavily investing in both the research and development of blockchain technology.

Consequences Of Falling Behind On Blockchain Technology

By not strategically positioning the U.S. as a leader in DLT, the U.S. will lose its position as the top currency provider, source of safe, transparent capital investment, and leader in internet and technology. On the cusp of a large shift in technology, stemming from the advent of Artificial Intelligence, the Internet of Things, blockchain, quantum computing, and cyber-warfare, the U.S. cannot fall behind in its investment into the technological infrastructure that will power a new era. The need for trusted infrastructure, financial systems, currency, and general value exchange is crucial as digital asset movement becomes more prolific. As cyber-warfare replaces physical warfare, redundant, immutable, and tamper-evident infrastructure like blockchain becomes crucial to protecting our country and our allies. Investment and the development and execution of both a domestic and global strategy by the U.S. Government is critical. As blockchain is a technology based on its distributed properties, investing in its use and distribution to our

4 www.coindesk.com/from-banking-giants-to-tech-darlings-china-reveals-over-500-enterprise-blockchain-projects?utm_source=&utm_medium=&utm_campaign=
5 https://www.cnbc.com/2019/11/12/china-could-launch-digital-currency-in-next-2-3-months-investor-says.html
6 https://www.coindesk.com/the-russian-military-is-building-a-blockchain-research-lab

industries, defense agencies, and allies will strengthen the U.S. as a trusted provider of information, services, and assets across the world.

If the U.S. fails to act, key elements of our national security may be critically impaired. It is thus imperative for the future integrity of our national security assets that we act now rather than waiting for a crisis to emerge. In 1987, the U.S. Army War College introduced the concept of VUCA (**volatility**, **uncertainty**, **complexity**, and **ambiguity**) to describe the precarious world that has emerged in this post-Cold War era.[7] Such a metric seems more than appropriate in today's ever-changing world of technology. DLTs, leveraged appropriately, can handle the **speed of change** in a multilateral, **volatile**, and changing environment, to address **uncertainty** in data or coordination of actions, reconcile **complexity** that exists in a multi-tenant global organization with dynamic inputs, and handle the **ambiguity** that exists across the operational environment. As such, the DOD should not underestimate the instrumental advancement in capability DLT technologies enable or the threats that the DoD will face from countries and militaries that employ such capabilities. Fortunately, our allies in the UK, Australia, and elsewhere have also seriously begun to explore the use of blockchain for defense, just as the U.S. DoD should continue to do so.

[7] https://www.vuca-world.org/

Topic A: Improving Cybersecurity

Existing enterprise information systems are widely acknowledged to be vulnerable to many forms of cybersecurity attacks. Such vulnerabilities are particularly dangerous when compromised networks and user accounts are used to issue commands that would be difficult or impossible to roll back. Obvious examples include permanent erasure of data, control of critical infrastructure, large monetary transfers, or weapons release. At the same time, the integration of space-based communications infrastructure within 5G networks presents new, specific challenges for spacecraft, or more specifically, a necessary rationalization of currently patchy communications security and the assurance of identity when conducting high-level spacecraft tasking and control operations, particularly as it applies to the new U.S. Space Force.

DLTs present a unique way to address these issues. As already described, blockchains are distributed, append-only databases of transactions, and are considered a strict subset of distributed ledgers. Administrative responsibility and trust are typically shared among the operators of blockchain nodes. Blockchain allows a balance of the need for all constituents in the supply chain to have visibility into the flow of goods with the need for security of data in the supply chain ecosystem. Certain participants in the supply chain can have limited access to transactions which enhances security. The tamper-evident nature of blockchain makes them difficult to compromise because a successful attack requires the attacker to be able to successfully gain control of many participants. These characteristics make DLT generally applicable to many enterprise scenarios, such as eliminating the permanent erasure of data, control of critical infrastructure, large monetary transfers, command and control, and/or weapons release.

Use Case 1: Multi-Factor and Multi-Party Authentication

Multi-factor authentication is used to ensure that a user is who they say they are. For example, one may provide credentials to log onto a bank's IT systems, and then subsequently be asked to confirm this login request via an email, message to a registered mobile phone, or use of a separate hardware token. The second, hopefully independent, confirmation of the user's identity significantly increases the challenges facing a remote attacker attempting to gain unauthorized access. Similarly, multi-party authorization requires a separate party to validate an operation one wishes to perform before being allowed to proceed. In the case of a banking system, a bank may wish to confirm an attempt to close a joint account with other account holders before acting.

The use of a blockchain as a confirmation system allows for some interesting and useful concepts to be employed. A blockchain is a naturally distributed system that must come to consensus on new information in order to operate. The addition of arbitrary smart contract execution allows users of a blockchain to encode whatever business logic is appropriate for a given use case. A smart contract may be written to require actions taken by blockchain users, off-blockchain processes, other smart contracts, or any combination thereof. There is no theoretical limit to the business logic that may be so encoded, although implementations clearly have many practical limitations, such as the inability of hardware or operating system to execute business logic with high algorithmic complexity.

For example, a smart contract may be written so a command destined for an edge device[8] will not be validated by the contract until an authenticated user confirms their identity via a separate communications path (i.e., through multi-factor authentication and/or multiple authenticated users confirm the command's validity through multi-party authorization). Commands may also be checked for correctness of form (syntax), usefulness in an operational context, or any other automated checks that may be encoded in a smart contract. Adjusting edge device software to read from a remote system prior to command execution should require minimal changes for those systems that allow for remote software updates. The bulk of the work to implement multi-factor authentication and/or multi-party authorization would fall to a blockchain, where it can be more easily reached, extended, maintained, and managed.

Implementation of additional computation or communication protocols for the purpose of improving cybersecurity is often a significant cost. It is therefore important to note that a spectrum of options exist to improve the security of edge device call-backs so that the level of protection is proportional to the perceived risk. Reading a command verification from a blockchain may be itself enough to protect against a single account disclosure, but only if the communication channel is secure and the blockchain node returning the information is not itself compromised. Security could be improved by having an edge device query that different nodes are connected to the blockchain by using a so-called trusted oracle to cryptographically sign a command verification on the smart contract or some other verifiable computing scheme. It would also be possible in cases where enough computing power exists on an edge device to run a

[8] I.e., a device which provides an entry point into enterprise or service provider core networks, such as a router.

"light" blockchain client. A light client would allow an edge device to directly verify the Merkle path (i.e., hash tree) to command verification.[9]

Use Case 2: Securing Spacecraft Tasking and Control

Communication security for existing spacecraft has been incompletely implemented, leaving significant attack vectors related to spacecraft control.[10] Protecting this type of communication is paramount with the standing up of the new U.S. Space Force. Communications security has been widely deployed for military satellites, newer telecommunications satellites in geosynchronous orbit, and newer deep space probes. Relatively few of the new breed of CubeSats and other small satellites in low Earth orbit have launched with fully encrypted communications, including on channels used for spacecraft control.[11] Practical exploitation of such lax security measures thus far has been limited due to the relative complexity and cost of satellite ground stations. However, the recent implementations of ground-station-as-a-service offerings from Amazon and other vendors have slashed the costs of ground station access and exposed such communications vulnerabilities.

Motivations to close security vulnerabilities on satellites are generally synonymous with motivations for securing services on the public Internet. Attacks may be conveniently separated into two types: attempts to gain unauthorized control (i.e., "hacking") and attempts to deny service (i.e., "jamming" of radio communications). Spacecraft and ground-based systems that control them are at risk of such attacks. Although few spacecraft operators publicly acknowledge cybersecurity incidents, governmental transparency regulations in the United States have revealed some incidents. Examples include attacks by Chinese state actors that led to unauthorized access to "networks that control spacecraft" at the NASA Jet Propulsion Laboratory[12] and acknowledgement that U.S. Air Force satellites have been "jammed by commercial equipment easily acquired by state and nonstate actors."[13] One can reasonably assume that commercial satellite operators and space assets controlled by other governments have had and continue to face similar challenges.

The use of an enterprise blockchain as a confirmation system allows for some interesting and useful concepts to be employed to address these concerns. A blockchain is a naturally distributed system that must come to consensus on new information in order to operate. The addition of arbitrary smart contract execution allows users of a blockchain to encode whatever business logic is appropriate for a given use case. A smart contract may be written to require actions by blockchain users, off-blockchain processes, other smart contracts, or any combination thereof to occur. There is no theoretical limit to the business logic that may be encoded in smart contracts, although implementations clearly have many practical limitations.[14]

9 A hash tree or Merkle tree is a list of hash lists and chains that can be used to verify any kind of data stored, handled, and transferred in and between computers. They ensure that data blocks in a peer-to-peer network are received undamaged and unaltered.

10 https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf

11 https://www.space.com/34324-cubesats.html

12 https://oig.nasa.gov/docs/IG-19-022.pdf

13 https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf

14 E.g., the inability of hardware or operating system to execute business logic with high algorithmic complexity.

For example, a smart contract may be written so a command destined for a spacecraft will not be echoed to the blockchain until an authenticated user confirms the validity of a command issued to a satellite through multi-factor authentication or multiple authenticated users confirm the command's validity through multi-party authorization. Commands may also be checked for correctness of form, usefulness in an operational context, or any other automated checks that may be encoded in a smart contract. This is demonstrated via the following diagram.

Spacecraft Communication Secured By Blockchain Technology

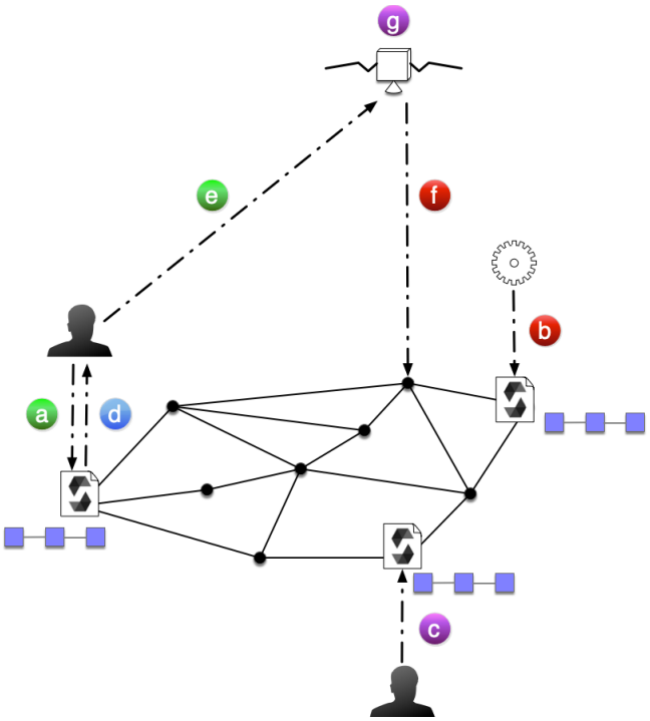

Figure 1: Multi-factor authentication and multi-party authorization example:

A. *An operator proposes a command to be sent to a spacecraft.*
B. *Some number of automated processes (zero or more) confirm command syntax and perhaps applicability in the operational context.*
C. *Some number of humans (zero or more) confirm the command should proceed.*
D. *The smart contract sets the entry of the command approval table associated with the hash of the command to the Boolean Value True.*
E. *The operator sends the command to the spacecraft. Where verifiable computing is used, the operator also sends a proof of what the entry of the command approval table has been set to.*
F. *Where the satellite runs a light client, the operator also sends the Merkle path to the contract state for the approval table.*

G. *The spacecraft executes the command if and only if the command verification was successful.* [15]

It is important to keep in mind that the various parties are making calls to the same smart contract even though the figure shows the parties interacting with different copies of the smart contract stored on different nodes. The blockchain, as a distributed system, is required to come to consensus between its nodes each time a write operation results in an addition of information to the blockchain. Smart contracts in this scenario would maintain a command approval table, indexed by the cryptographic hash of the command, which maps to a Boolean value that indicates whether a command has been approved.

Overall the key benefit of this approach is to provide a much higher level of authentication and/or authorization security. An attacker would need to gain control over an arbitrary number of user accounts and be able to use those accounts to perform actions on the blockchain in order to confirm an inappropriate command.

[15] https://www.researchgate.net/publication/337033747_Methods_for_Securing_Spacecraft_Tasking_and_Control_via_an_Enterprise_Ethereum_Blockchain

Topic B: Reducing Single Points of Failure in Emergency Decision Making

A single point of failure in technology is a part of a system that, if it fails, will stop the entire system from working. Blockchain provides opportunities and challenges when applied to reducing single points of failure in emergency decision making. In emergency or catastrophic decision making, the practice of effectively dealing with emergency situations by alleviating the losses of properties and lives caused by these events is one that is not new in the theater of battlefields. In recent times and with the invention of nuclear weapons, faster decisions made by fewer individuals have impacts at levels of magnitude that could change the world's population overnight. Blockchain technology enables efficacy attestation for high confidence decision making. DLT employs cryptographic proof of identification and remediation of single point of failures where centralized and traditional IT data architecture remains exposed to these weaknesses. Additionally, blockchain can make the networks used during emergency decision making have significant antifragile[16] properties, which is highly desirable.

When it comes to the decision-making process during emergency and catastrophic events, it is critical that the state and effectiveness of large operational networks and ecosystems remain functional, which DLT can help to ensure. Many factors must be considered in emergency decision making environments, especially when multiple actors are involved in the maintenance, orchestration, provisioning, and usage of these systems. In particular, and seemingly lacking in modern network IT architecture schemes, is the notion of continuous automated accountability – or the idea that a self-defending network may also be a self-interrogating network. Blockchain technologies can be programmed to root out, isolate, and mitigate against compromises that seek

[16] https://fs.blog/2014/04/antifragile-a-definition/

to exploit single points of failure in any networked system. The net result is a command and control hierarchy that can facilitate high confidence in decision making based on the efficacy of data generated from the systems being relied upon. By leveraging DLT, it may be possible to develop a framework around continuous cryptographic compliance that is based on decentralization that is underpinned by traditional best practices for complex IT systems and network designs.

Prior to implementation of any blockchain technology, many organizations have already moved to distributing their workloads across multiple environments and networks in an effort to increase resiliency and to minimize single points of failure. While these efforts are in large part beginning to pay off, questions remain regarding the efficiency of metrics available to provide a level of confidence that an end-to-end workflow is being executed correctly. Simply put, if there is a fault in one or more of the network resources utilized, how is it captured, analyzed, communicated and mitigated in real-time or near real-time? More importantly, what was the level of exposure? Ultimately, blockchain technology presents both a challenge and an opportunity in this space as the benefits and costs of a centralized IT system architecture design must be measured against the implementation of a distributed network architecture.

In any modern blockchain operating environment, credentialed participants are part of a self-managed ecosystem facilitating the movement and validation of high value transactions. Providing operational integrity transparency across an entire DoD ecosystem could be a daunting task. However, therein lies the opportunity, as other agencies globally have discovered: blockchain technology can be utilized to facilitate distributing monitoring and compliance verification capabilities across multiple administrative domains. It is commonly understood but hardly realized or practiced at this nascent stage that IT or network-centric blockchain solutions must be implemented with detection, protection, and enforcement mechanisms that should be unified with the underlying communications infrastructure so that a near real-time or wire rate response can be generated across a multi-stakeholder operational environment. Without the ability of multiple participants able to confirm and agree upon transactions across the IT ecosystem, the new system lacks the essential aspect of a communications network that provides the benefit of transparency from blockchain technology.

Once a robust, decentralized framework is established, the network should have the ability to identify and quarantine resources that may be deemed as single points of failure and be able to verify the automation of the corresponding remediation. The blockchain network will then generate actionable insights to further enhance robustness and resiliency in the decentralized critical infrastructure systems. This leads to critical systems becoming self-interrogating and self-verifying, and therefore is of significant importance in the command and control decision making process.

Antifragility In A Blockchain Environment

When discussing network management through decentralized architecture and other means, the concept of antifragility, or increasingly improving resilience or robustness, is important to consider.[17] Decentralized antifragile systems – whether these systems are energy networks, applications or critical infrastructure – become stronger the more people or machines try to break them. Blockchain technology extends this capability by enabling one single version of the truth, data immutability, and automated processes. Combining blockchain technology with machine learning algorithms would allow multi-stakeholder systems to continually improve themselves, better react to challenges in the future, and perhaps even anticipate potential problems. Setting up machine learning algorithms to constantly measure specific parameters and adjust themselves accordingly could allow those systems to learn new solutions to preserve their operational levels.

While data is shared in a blockchain network, there are a minimum of three states that data can be in – public, shareable, or private. Confidentiality and privacy of data are understandably very important to enterprise ecosystems as well as for large DoD systems. Sustaining these states can be accomplished using mechanisms of selective disclosure on the ledger. Users define access rights upon committing data to a blockchain network. Policies should be set up in the network so data being posted is always compliant with the governance models all parties have agreed upon. Decentralized architecture maintains the systematic metrics and measures to govern this. A user's roles and responsibilities within the network will grant them the according degrees of access to information.

[17] See Nassim Nicholas Taleb's book *Antifragile: Things That Gain from Disorder* (Penguin Random House, 2012)

For example, a General could be granted access to all information, but a Data Entry Specialist would have only access to certain areas. Again, adhering to decentralized principles as described earlier ensures unassailable efficacy of data management, delivery, and automation through smart contracts. The smart contracts ensure policy enforcement and yield a clear, concise picture of knowledge that is shared across an ecosystem of partners to ensure that the decisions are of high quality. The single source of truth created by blockchain technology reinforces the confidence and accuracy of a decision in a catastrophic scenario. Smart contracts programmed to allow those who 'need to know' the access or origin of data allows for the appropriate functioning and interface with the hierarchical community of human decision makers in command and control environments with the decentralized system architecture of blockchain technology.

The next level would be creating a data overlay specifically for the purpose of providing algorithms access to ecosystem-attested data, or data that is compliant, shared correctly, and of high value to the considerations in catastrophic decision-making. In theory, machine-learning algorithms may produce higher quality insights for antifragility as ecosystem-wide observations are shared. The complex network infrastructure of many DoD systems used in catastrophic decision-making scenarios is a perfect example of how a complicated system with many stakeholders provides massive amounts of high-quality data for a machine-learning algorithm to use. Adding blockchain in between the infrastructure and machine learning would potentially increase the quality of information that is analyzed for all users while maintaining control of data access and preventing tampering.

Topic C: Blockchain for Improving the Efficiency of Defense Logistics and Supply Chain Operations

"You will not find it difficult to prove that battles, campaigns, and even wars have been won or lost primarily because of logistics." ~**Dwight D. Eisenhower**

Overwhelming power is an essential element of military success, and few foes are equipped to defeat a U.S. military unit head-on. Our warfighters are equipped with the world's most advanced weapons systems and defensive measures, ranging from the flying firepower of an Air Force jet to the Near Infrared Signature Management Technology[18] in the Army Combat Uniform. However, U.S. adversaries understand that these systems are the final stage in an unimaginably vast production and supply network. They understand that it is far safer to surreptitiously alter the design of a rotor blade than to confront an attack helicopter. They understand that infecting the meals ready to eat (MRE) supply chain is infinitely more disruptive than surrounding an infantry squad. The most advanced enemies are skilled at sowing doubt in their adversaries and know that an untrusted supply line is effectively sabotaged.

In recent years, the risk of counterfeit or non-conforming components making it into the DoD supply chain has increased dramatically. The Senate Armed Services Committee and Government Accountability Office (GAO) have both published reports[19] within the decade

[18] https://www.revolvy.com/page/Near%252Dinfrared-signature-management-technology

[19] https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts

detailing the proliferation of counterfeit threats, particularly as they pertain to the manipulation of components by foreign adversaries.[20] Counterfeit risk is a concern for most supply chains; however, compounding factors such as cheap overseas labor and materials, a reduction in the number of domestic manufacturers, and proliferation of U.S. resellers have resulted in substandard acquisition conditions. The DoD requires increased oversight and greater collaboration with trusted manufacturers to help secure the supply chains of mission-critical components.

Blockchain technology acts as a trust enabler within procurement ecosystems by allowing greater visibility and collaboration between origination and destination. Across the world, companies that depend on their supply chains are turning to blockchain technologies. Manufacturers, retailers, and the transoceanic shipping companies are implementing blockchain-based "track and trace" systems which provide visibility and trust of food and product components from their origins to the end consumer. These systems provide use cases for potential DoD supply chain usage of blockchain.

Defense Supply Chain Challenges

Until 2019, the GAO High-Risk List Report has included the management of the defense supply chain as a high-risk program since 1990. The GAO studies identified vulnerabilities to fraud, waste, and abuse, and recommended better acquisition practices and inventory management in past reports. In 2019, the GAO removed the DoD supply chain risk management from the high-risk list because it had made progress in asset visibility and material distribution by addressing several actions identified in the 2017 report. The initiatives undertaken by the DoD include creating a single portal system providing 7,500 users access to supply and transportation data, and the use of RFID technology to identify, track, and store information. The commitment of senior DoD leadership to make progress in modernizing the defense supply chain and improving the management of its assets is commendable. However, it is imperative that senior leaders continue their efforts to implement technologies and initiatives to improve the visibility of supplies, delivery standards, acquisition-methods, asset management, anti-counterfeit efforts, and data-driven decision making.

Lack of collaboration and trust are at the core of the defense supply chain management challenges for the U.S. Army and other branches of the DoD as well. Naturally, challenges arise when dealing with a global network of suppliers and sub-suppliers, many of whom are small and financially unable to invest in digital technology to support their businesses. Many of the challenges created by this complex ecosystem include:

- **No single source of truth** – Record-keeping and reporting managed by many entities lead to incomplete and unreliable data across disparate systems. This causes significant difficulty in tracking and routing, inventory management, and asset readiness.
- **Lack of trust and collaboration** – The defense supply chain procures a wide-spectrum of goods and products to support the warfighter, ranging from food to high-end weapons system components. Procuring these goods from a few trusted sources is nearly

[20] https://www.gao.gov/assets/590/588736.pdf

impossible at the scale required by the defense supply chain; thus, the DoD must procure from thousands of sub-suppliers. At such a large scale, trust and collaboration are nearly impossible in comparison to the closed supply chain common in private industries.

- **Real-time management and decision making** – All supply chains are challenged by unforeseen circumstances such as natural disasters, weather delays, labor disputes, or resource shortages. Inherent in military supply chains are the added threats of intentional sabotage, political instability, and, of course, combat disruptions. Agility is required in these circumstances to avoid crises, especially in the effort of supporting the safety and readiness of the warfighter. The lack of collaboration and data transparency issues are exacerbated in critical scenarios where real-time information of goods within the supply chain and inventory are unavailable. This hinders efforts to ensure that the warfighter is prepared for any and all threats, and results in high costs associated with procuring additional goods rather than redirecting existing supplies.

Characteristics of a Blockchain Supply Chain

Defense leadership has made significant progress in improving supply chain management through strategic initiatives and the introduction of new technologies to its ecosystem. The result of modernizing the defense supply chain is already being realized with billions of dollars in savings according to the GAO's 2019 report.[21] However, blockchain technology can bring the defense supply chain into the future by bridging the gap between the physical and digital world and developing a logistics ecosystem that is fueled by collaboration and trust. Among the challenges that blockchain can address for defense organizations are:

- **Traceability** – On-demand verification of the source, provenance, and identity of the software, hardware, and supporting documentation for components and systems.
- **Assurance** – Greater adherence to product quality and specifications as well as compliance with industry and regulatory standards.
- **Transparency** – The ability to share, with specific permissions, permanent and verified records of transactions and transfers across an ecosystem of suppliers, partners, and customers.
- **Fast Settlement** – The ability to implement smart contracts for ownership transfers and automated distribution of funds based on agreed business rules.
- **Simplicity** – Streamlined reconciliation, elimination of exceptions, improvement of audibility, reduction of paperwork, and increased collaboration with ecosystem partners.
- **Secure Trading** – Securing the buying and selling of components and products across the supply chain through improved understanding of supply chain partners' credentials and practices.

The characteristics of a blockchain-powered supply chain unlocks the value trapped in traditional supply chain ecosystems. The introduction of connected devices and software allows participants to gather more data efficiently, with improved data integrity and reduced data reconciliation costs. The availability of high integrity data allows participants to increase their business

[21] https://www.gao.gov/assets/700/697245.pdf

intelligence through advanced analytics and data science solutions which were previously not possible due to non-standard data practices. The integration of blockchain technology introduces new opportunities for the DoD such as procurement efficiency, improved logistics, and inventory management, and improved supply chain security.

Supply Chain Use Cases

Supply chain use cases of DLT include:

- **Provenance of Goods**: For origin of goods, assured identity tied to a physical object, recall management, and certified products. The provenance of a good refers to its origin as well as a chronological record of its ownership, location, and other important information as it moves along a supply and distribution network. Blockchain combined with Internet of Things technology (GPS, RFID sensors, etc.) can enable a deeper understanding of the components and goods the DoD is acquiring than previously feasible. The DoD requires detailed information about the materials and components that their manufacturers are sourcing from a variety of suppliers. In addition, blockchain technology can bridge the gap of trust within its supply chain and ensure the entire process has been ethical and maintains the appropriate standards of care.
- **Counterfeit Protection**: For unassigned suppliers' warranty, manufacturing (physical) identity, tamper detection (fraud), and track and trace. Today, we are surrounded by counterfeit goods that range from retail products to software, electronics, digital media, piracy, deep fakes, and intellectual property. Counterfeit goods entering the defense supply chain could have disastrous consequences at the moment a defense system is needed most. The DoD supply chain ecosystem depends on certifications and collaboration between procurement teams to ensure the validity of the goods being acquired. Increasing transparency and data sharing between these entities enables better anti-counterfeit protection.
- **Food Supply**: For safety recalls, food fraud, and food traceability. In addition to arming the warfighter, the U.S. defense supply chain also has the duty to feed soldiers, sailors, airmen, and marines around the world. Safe food supply is essential to readiness. One of the early private sector large-scale uses of blockchain is tracking the food products from origin through domestic and international supply chains. This same technology that ensures the health and safety of the American consumer must also be extended to deployed personnel.
- **Commodity Sourcing**: Verification of Mass-produced Goods. Many products procured for defense purposes are common mass-produced items not made specifically for military use. U.S. Defense Procurement Agencies do not buy these directly from the manufacturer, and so have little or no visibility into their production. A hostile actor, knowing that a portion of a facility's output will be eventually purchased for inclusion in U.S. Defense systems, could contaminate or weaken that one facility's products. By the time the contamination is detected, there may be no way to know where the products are now in the supply chain, and whether any were used in U.S. Defense systems. Product recalls on a massive scale could result, affecting unit readiness as systems are taken offline while their integrity is assured.

- **Asset Readiness & Advanced Analytics:** Data-Driven Planning & Decision. Advanced data science solutions and analytics are transforming decision making, allowing executives to make data-driven decisions informed by data in real-time. Integrating blockchain into the defense supply chain would standardize data collection and storage and increase the amount of data available for analysis. Data science solutions such as machine learning and Artificial Intelligence enable analysis on a scale unmatched by humans, providing insights that may have never been identified. The combination of Artificial Intelligence and Blockchain could revolutionize the defense supply chain from procurement, logistics routing, inventory management, and managing the lifecycle and maintenance of equipment.

Examples of Blockchain for Defense Supply Chain

Blockchain is already being used within the defense supply chain as follows:

- **International Naval Engineering Contracts:** A naval program needed to cut supply chain costs away from inefficient third parties and wanted to lessen the logistical burden. Using blockchain and automated smart contract agreements, the naval program was able to cut the internal order intake process by 45% by taking out manual entering and requiring fewer people to verify yes or no decision making in their logistics process, saving international partners 30% in supply chain exchange fees without having to use a third-party system to create the payment.
- **Defense Aerospace:** An Armed Services Agency estimated that 15% of the components in their machinery were counterfeited or fraudulent. Recognizing the need for product assurance they created a process to certify products at each stage of the value chain using electronic component fingerprinting technology.
- **Civil Aerospace:** An Aerospace Department needed to track engines and service activity while also expecting an increase in engine production of 25%. With blockchain technology they created a risk management assessment tool, verified by a distributed ledger to alert authorities when and where an aircraft was going, tracking manufacturing quality across international partners.
- **Additive Manufacturing (AM):** For 3D parts manufacturing, prototyping products/machinery, and replacement parts, AM technology allows the construction of 3D objects by adding layer upon layer of material regardless of whether that material is plastic, metal, concrete, or even human tissue. AM allows just-in-time manufacturing close to the need, which reduces cost and time to deliver. AM depends on digital design files distributed to manufacturers. Blockchain technologies can indicate when files have been tampered with or corrupted. To guarantee the integrity of those design files, ensure their secure delivery, and prevent alteration or unauthorized reproduction, AM designers protect their design files with blockchain technology. This use case will be further expanded upon in the following section, given the current importance of it to the DoD.

Aircraft Parts Made Through Additive Manufacturing (AM)

SIMBA Chain, a company that was formed in 2017 from a grant awarded by the Defense Advanced Research Projects Agency (DARPA), has a pilot demonstrator that is designed to protect the integrity of AM data and acquisition during the transmission on the supply chain. This enables a tracking system on the AM data and physical flows for the Air Force that can identify counterfeits or compromised components in the field and also prevent malicious intrusions during manufacturing. The main goals for the demonstrator are to ensure the verifiability of the design file during the manufacturing process and to be able to track the part from manufacturing to installation.[22] SIMBA Chain's platform, which is run on the Microsoft Azure Government Cloud, has a zero-code graphical interface for the development of smart contracts and automated generation tools that create application programming interfaces (APIs) for smart contracts using simple Representational State Transfers (REST)-based endpoints. To use this tool, a user simply conceptualizes their application into entities to be tracked, along with the circumstances of how they should be tracked, and then defines the data to be collected at each step. This model is based on "assets", being the nouns and "transactions", being the verbs of the defined business process. In the AM scenario, assets are used to represent the design file and the AM component that is printed, and transactions are used to define how these are tracked. For AM components for example, transactions were used to track and trace the manufacture, delivery and installation of each AM component. Optionally, each asset or transaction can include a hashcode to uniquely represent any files that are stored elsewhere (off-chained), e.g., the design file and a photo of the manufactured AM component. This model is converted into smart contract code and deployment onto the Blockchain (Ethereum in this case) and a REST API is exposed for application integration. The resulting pilot provided a complete chain of blockchain transactions that allowed a component to be printed from a verified design file and tracked from production to installation.

[22] https://www.ledgerinsights.com/us-navy-blockchain-aircraft-supply-chain/

Topic D: Enhance the Transparency of Procurement Auditing

As has been already noted, since the early 1990s, the contract management by the DoD has been on the GAO's high risk list because of its deficiencies in many areas, including service acquisitions.[23] Since 2017, this remains unchanged.[24] The following section will highlight how blockchain can assist the DoD in service acquisition, specifically the enhancement of transparency through procurement and auditing.

Governments around the world are implementing various technologies to improve integrity, efficiency, and value-for-money in their procurement processes. Blockchain is amongst the technologies being tested, primarily as it is tamper-resistance, tamper-evident, and inherently generates a single source of truth that can be trusted and used as a benchmark to detect waste, fraud, and abuse.

The worth of including DLT into the architecture of an e-procurement system comes with the advantage of a ledger that is tamper resistant and capable of being updated and shared in real time amongst participants in a network to promote transparency. The unique ability of blockchain to validate and form consensus around the accuracy and completeness of data being shared on a common ledger amongst a group of semi- to non-trusting parties opens up many possibilities to improve e-procurement for the U.S. government, which will result in reduction, if not elimination of the major adverse findings in GAO and IG reports.

[23] https://www.gao.gov/key_issues/dod_contract_management/issue_summary
[24] https://www.gao.gov/highrisk/dod_contract_management/why_did_study

First, options for creating a blockchain network and its respective rules must be considered. Departments and agencies must decide on who the blockchain participants will be and how transactions are validated. If the network is open and anyone can join it, the blockchain would be considered a public chain (permissionless). If the network is more sensitive and the participants are known and invited to participate, the blockchain would be considered a private chain (permissioned). Within the context of DoD's structure, a permissioned private blockchain system is one that is set up for a semi-trusted environment with rules setup amongst members.

After making the decision on consensus, it is important to draft rules and decide how governance of the blockchain will work. An in-depth knowledge and understanding of existing businesses processes is essential for setting up a DLT system. Once the network is configured with all the rules and a governance model has been established, data can start to be shared amongst the participants in the network and members can start to analyze the various deficiencies that blockchain promises to correct. Integrating a blockchain ledger into existing data flows is a great way to expand the infrastructure and take advantage of the data that is already being produced and consumed in these networks.

It is important to consider how the DoD might design their blockchain network architecture to assist in their procurement process as it exists today. Department and agencies having the ability to integrate transactional level control over data and write that to a blockchain make it harder to alter and easier to share. Data can be stored off chain and a hash or pointer to the data can be saved on chain, making any alteration or access apparent and traceable. This increases the faith that the participants have in the network and its ability to protect data integrity by making use of a shared ledger.

Examples Of Blockchain Technology To Improve Procurement

Three specific GAO identified deficiencies related to DoD's service acquisition process will be used as example areas to highlight how blockchain technology might be used to increase efficiencies and to improve integrity while reducing costs and increasing value. The specific areas of deficiencies covered in the reports are DoD's lack of ability to assess contract award time frames,[25] improve upon tracking and management of budgets in contracted services,[26] and utilize inventory information in management decisions.[27]

These problems are normal for businesses the size of DoD. We will recommend ways DoD might apply blockchain technology to maximize efficiencies enabled by the technology while reducing deficiencies in the three areas.

The first of the GAO findings in the procurement process addresses an inability to track major system acquisition timelines. On a blockchain, the DoD, as a node owner with data rights to the departments' data, can start to analyze transactions as they occur in real time. The procurement process can be coded onto smart contracts that record on the blockchain ledger major decision

25 https://www.gao.gov/assets/700/693123.pdf
26 https://www.gao.gov/key_issues/dod_contract_management/issue_summary
27 https://www.gao.gov/assets/700/690954.pdf

milestones and activities in real time. These milestones can be shared with others based on the data owners sharing policies as has been decided upon when the governance was set up. The need for timely data calls can be reduced or eliminated. All transactions now have a date and time stamp, leaving records that provide an easier way to gain insights into the DoD's collective data.

The inability to share real time data pertaining to ongoing procurement makes it inefficient and costly to collect and analyze key procurement milestone events. Departments and agencies do not freely share data for many reasons, amongst them security. Recently, the Health and Human Services department (HHS) obtained the first Authority To Operate (ATO) approval for blockchain within the Government. Oki Mek, Chief Product Officer at the division of acquisition at HHS made some observations on how blockchain performs in procurement. "We had to meet the FISMA [Federal Information Security Management Act] requirement. Part of that requirement is that all federal funded systems have to be authorized to operate. Part of that process is a rigorous assessment process and authorization by the authority official. We have proven that blockchain can be authorized to operate in the Federal Government. Not only that, we found out that blockchain improves cybersecurity."[28]

The next issue raised by GAO that will be analyzed is the DoD's inability to sufficiently track and manage contracted service budgets. If blockchain allows for data sharing with semi-trusted parties, data that has not historically been shared can be shared by using rules setup amongst the participants in the network. The characteristics of blockchain help to assure others that there will be a recorded event of all transactions that will result in an audit trail that allows all rules and transactions to be audited.

It is best highlighted through real-world HHS blockchain implementation examples in the procurement process to illustrate ways in which budget issues can be addressed. Michael McFarland, director of the Office of Acquisition Business Systems at HHS, provided his observation on how prices and budget information can be shared across network participants. He noted that they will now have unprecedented access to prices paid, vendor data, and other acquisitions that have occurred as a result of the blockchain technology so that they will be able to make decisions with far more information than they have had available to them before.[29] The successful HHS use cases help to bolster the government's case for using blockchain, especially given the known challenges and deficiencies faced by departments and agencies as cited by oversight organizations.

Finally, the ability to have accurate, real-time inventory counts for precise procurement requests can be enabled through a distributed ledger that is shared throughout the chain of the procurement process and help avoid waste in decision making on the quantity of orders. Additional technologies such as Internet of Things (IoT) sensors and other passive or active tracking devices can also assist with and act as oracles for smart contracts that only trigger the need for new procurement requests at certain inventory levels to maximize efficiency.

[28] https://govmatters.tv/hhs-obtains-first-blockchain-ato-in-federal-government/
[29] https://fcw.com/blogs/lectern/2017/10/comment-kelman-gsa-blockchain.aspx

In conclusion, blockchain can be looked at as an enabling technology with a distributed ledger that allows for integration of technologies and workflows that have not been possible before. New ways of contract management and transparency in the procurement process on a real-time basis provide efficiencies for both the DoD contracting officers and the private sector contractors providing goods and services. Just as the DoD found a way to build new applications and make distributed systems possible on the Internet, blockchain enables new capabilities by offering a layer of trust that the DoD can apply to improve its procurement process.

Topic E: How Blockchain Disrupts People, Processes, and Industries, and Ancillary Private Sector Use Cases

The concurrency across multiple, diverse stakeholders using DLT provides the potential for highly optimized business processes across people, processes, and industries. More powerful, however, is the potential for entirely new business models than what exists today.

Central to the DLT's implementation is the stakeholder network that spans a diverse set of entities. No longer contained within the control of one entity, the created network bears the responsibility for the operational success of the platform. But what does that mean? Generally, users are all familiar with centralized systems owned and managed by their organizations. Even in a software-as-a-service (SaaS) model, there is clear line of sight to the application, its functions and features, its data, and a single entity, i.e., the SaaS provider, who is ultimately responsible if something should go wrong or new features or functions are needed.

In a DLT implementation for a streamlined supply chain, there is a manufacturer, a transportation company, a supplier, and the DoD intake depot. These four diverse stakeholders, who compromise the network, engage in commerce together to track the provenance of replacement parts for warfighter aircraft. With the DLT application, there is a unifying application built on the blockchain infrastructure that the network equally accesses, verifies transactions for, and records information to. It is a community product equally owned by all four stakeholders. Ideally, they have all agreed to the business rules and what constitutes a "valid" transaction. Alongside the co-owned DLT application, they all have their own systems that manage their business, such as enterprise resource planning and financial systems, that may integrate with the DLT application as well.

Whether the example above is viewed as an optimized business process that now facilitates automated, near real-time data sharing or a new business model that provides provenance and

traceability, it presents a unique situation because of the application and the accompanying data that is co-owned and co-operated. Formalization of this network, which is sometimes referred to as a consortium, is necessary to align incentives for participation, outline roles and responsibilities, and orchestrate and support the DLT-based application. Clear operating and governance models must be developed and agreed upon so that critical decisions such as funding, liability models, and regulatory oversight can be agreed upon across the network participants.

Too many recent DLT experiments or proofs of concept have focused solely on the technology. They have been conceived and developed by a single entity emulating a value chain across simulated network participants. These are great technology learning experiences and should not be undervalued as such. However, the technology is the easiest part of implementing these new business processes or models. The harder part is getting true networks to come together and develop workable and agreeable operating and governance structures. A network participant must perceive value in participation and believe that the policies, intellectual property, governance structures and business values embodied protect their mission or business model.

A network framework that provides the necessary operational and governance structure with the network or consortium at its core also needs to cover five additional key factors, which each have their own unique considerations:

- **Operations** – designating day-to-day operations and maintenance responsibilities.
- **Business impacts** – understanding impacts to core business processes.
- **Compliance** – adapting to accommodate potentially varied rules and regulations.
- **Talent** – sourcing the right people to lead implementation and sustain the operations.
- **Technology** – navigating through rapid technological changes.

Defining the consortium membership is far from trivial. Collaboration amongst participants in DLT networks is necessary in order to set standards, develop infrastructure, and execute transactions. Consider also that members' roles may evolve as an application matures. It is important to include all participants necessary for success in a large enough group to eventually achieve a viable scale. To ensure its survival over time, a consortium should be adaptable and scalable, without being subject to unnecessary membership limits. Members, therefore, should design the network to allow for flexibility in both the number of participants and transaction volumes. Rules for changing rules should also be established. Varying levels of complexity may result depending on whether the consortium is limited to government or includes industry alongside government.

Another important question concerns the common goals of the consortium. If members cannot agree on clear, common goals and reasons for operations, the consortium could be set up for failure. If a member brings key resources but doesn't receive enough benefits to compensate for its contributions, the goals should be adjusted, or an additional payment or benefit agreement should be worked out.

This matters because in nearly every conversation with government leaders, the same basic questions tend to arise: who owns it and who pays for it? Models to accommodate this new structure need to be developed.
When considering operations, choices made in defining the application can potentially affect each member's day-to-day operations and the way in which they work together. The operating plan must address who is responsible for managing and maintaining the platform, as this is key to a successful interagency or cross-consortium operation. Attention to activities in areas including operations, production control, diagnostics and problem handling, maintenance, data administration, system security plans, and configuration management is critical.

In considering the business impact, it's important to understand that DLT protocols are processes accompanied and even driven by change. Critical to success is understanding the implications to all members' day-to-day operations, as well as the assumptions and understandings of each member prior to adoption. As noted earlier, blockchain can transform business models and processes. Failure to understand, anticipate, and plan for these changes not only risks missing out on performance improvement opportunities, but also can jeopardize implementation success. Central to a full understanding of the business impact is consideration of the impact on the people affected by the changes.

Compliance is a critical factor in the success of any DLT solution. In our fast-paced world and with interactions that can quickly become global in nature, consortium members should establish an operating model with current regulations in mind, while also ensuring that there is flexibility to adapt to future rules and regulations. Where multiple agencies may be involved, there may be conflicting standards and regulations. For example, if there are conflicting standards on the use of cloud computing or open source software, these risks will need to be identified and accommodated before implementation. On a global stage, new regulations like the European Union's General Data Protection Regulation and the California Consumer Privacy Act need to be considered as well.

Talent, or ensuring you have the right people with the right skills, is essential, especially since DLT talent is in short supply. Different talent models can be used to design and develop DLT applications. However, agencies should look to have talent knowledgeable in the value and future potential these solutions can drive. They should ensure that they have the talent and training needed to sustain the system. Understanding the depth of experience of any vendor the consortium will use is also essential to the sustained success of the application.

Finally, DLT technology, to include blockchain, is still viewed as an emerging technology that is evolving at a rapid pace. Often referred to as a protocol, choosing which DLT protocol most closely aligns to the requirements is essential. Not all DLT protocols are a right-fit for all business needs. Because the technology is rapidly evolving, it is critical that a loosely coupled architecture is used for the overall application build that allows for decisions to be made around upgrades and increased features and functions.

Formulating a holistic approach to incorporating DLT into current business processes to gain operational efficiencies or create new business opportunities will make the difference between building a proof of concept that demonstrates limited value and one that can be easily and

quickly scaled to deliver expected outcomes. A recommended approach to successfully deliver a holistic approach is to create a Blockchain Center of Excellence that can help navigate current policies and procedures across DoD's complex landscape. Evolving knowledge surrounding budget and funding, regulations, private / public partnership, etc., can be shared and developed enabling departments to know how best to proceed.

In the considerations of DLT technologies, the DoD will be able to provide an excellent roadmap on the effective deployment of a blockchain network that many in the private sector will be able to adapt in the process of deciding on and establishing a blockchain network. In the DoD's consideration in procurement and establishment of new blockchain systems, it is likely that the most important lesson will be in conducting an honest appraisal of whether blockchain technology is needed for the various processes across the enterprise of the DoD and how this system will integrate and work with the rest of the network architecture. Building blockchain technology in isolation is exactly what a Blockchain Center of Excellence will help the DoD avoid.

Ancillary Blockchain Use Cases For Government and the Private Sector

While this paper has mainly looked at DoD-focused use cases of blockchain, potential use cases developed by the DoD that could be exported to private enterprise include those related to:

- Supply Chain
- Parts
- Logistics
- Large, complex requirements tracking
- Vertical Lift
- Contracts Management
- Contracts
- Data exchange / Command and Control
- Additive Manufacturing
- Terrorist event data sharing
- Identity
- Individuals
- Devices
- Businesses
- Tokenization
- Digital assets
- Contract payments

In summary, there are many current DoD use cases that can be appropriated for private-sector use, making investment in blockchain research and development a worthwhile investment not only for the defense, but also commercial, benefits. These use cases will be further explored in future research by the Value Technology Foundation.

Conclusion

In conclusion, blockchain technology already has made a profound impact on economies and industries across the world and will continue to grow in influence. The impact of DLT on the world economy needs to be carefully studied, analyzed, understood, and invested in by the DoD. It is not enough for our private sector to be competitive in DLT; rather, the DoD and whole of U.S. government must become highly proficient in its use in order to ensure our country's military and economic superiority.

This paper has provided an overview of how DLT may be used in various specified areas, including improving cybersecurity, reducing single points of failure during emergency decision making, improving the efficiency of defense logistics and supply chain operations, and enhancing transparency in procurement auditing, as well as in how technology used by the military could be adopted by the private sector for ancillary uses.

Ultimately, there is tremendous potential within blockchain technology that our adversaries and allies alike see. As discussed, this has resulted in worldwide research and development efforts racing to create successful blockchain technology systems that will increase the influence and power of countries around the world. At a minimum, to understand what China and Russia are exploring with such vigor, it will be essential to have experts trained in blockchain within the DoD in order to avoid the U.S. falling behind in DLT technologies.

The many exciting ideas for blockchain technology presented in this white paper spring from fresh ideas of experts in top private sector companies and are a testament to the successes of technology allowed to innovate freely in a democracy. It is the goal of the Value Technology Foundation that the United States consider funding a dedicated Federally Funded Research and Development Center (FFRDC) for blockchain technology so that its tremendous potential is not overlooked and to ensure that our adversaries do not surpass us with technological superiority.

Appendix A: What is Blockchain and Distributed Ledger Technology (DLT)?

Today, blockchain has become a loaded word for a simple concept. Out of a handful of emerging DLTs, blockchain has become the most prolific, powering world-wide and world-changing distributed networks like Bitcoin, Ethereum, and many others as a medium for trusted value movement or exchange of assets and transactions. Since the launch of Bitcoin in 2009, blockchain technology has since seen many ebbs and flows in its adoption, value, prevalence, and feasibility. However, by 2020, the feasibility of blockchain has been proven through a variety of groundbreaking use cases and technologies.

Ledgers have been the centerpiece of commerce for millennia, being used as a record keeper for numerous assets, such as the exchange of goods, money and property. An extension of this concept, a distributed ledger, at its essence is an asset store that is shared across multiple sites, geographies, or institutions.[30] All network participants have their own identical copy and any changes need to be reflected across all entities. Distributed ledgers also have been around for thousands of years, with the first notable implementation being a banking system used by the Roman Empire that allowed people to participate in transactions across its regions. They also extended this concept to paper checks, which fed into the ledger to record transactions.[31]

Further extending these ideas into the digital domain began in the nineties. In 1991, at an ice creamery, the concept of using many dispersed but interconnected copies of a shared ledger, (versus trusting a central authority) was developed. Stornetta worked with Haberto develop a cryptographically secure archive that could verify records without revealing their contents.[32] Such mechanisms enabled the collaborative creation of digital distributed ledgers with capabilities that far surpass paper-based ledgers. This early work led to the concept of DLT, which has been described as a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. There is no central administrator or centralized data storage.

As the name suggests, each word contributes to the overall definition:

- **Distributed** reflects its decentralized nature rather than a centralized one.
- **Ledger** represents a database of records.
- **Technology** defines the protocol that synchronizes data so that the database can operate in a decentralized way without the need for a central authority to regulate it.

Consequently, a DLT facilitates the storage of information in a secure and accurate manner using cryptography. Once stored, it becomes immutable.

Frequently, DLT and blockchain are used as synonyms, as they have been in this paper, but in fact, a Blockchain is a specific type of DLT that encompasses its own set of rules and features, including organizing transactions as a chain of blocks. Blockchains are far more opinionated than DLTs

30 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/ 492972/gs-16-1-distributed-ledger-technology.pdf
31 https://medium.com/blockstreethq/before-blockchain-there-was-distributed-ledger-technology-319d0295f011
32 https://doi.org/10.1007/BF00196791

because blockchain defines a specific way of implementing a DLT, whereas DLTs generally have a much broader scope and flexible structure.

Like a DLT, a Blockchain is a distributed ledger in which an immutable, non-repudiable record of transactions are stored permanently and verifiably, without the need for a central authority. The difference is how a Blockchain achieves this technically using a specific set of features. Blockchain algorithms allow transactions to be grouped into a block and each block is added to existing blocks to, as the name indicates, form a chain. As opposed to traditional database architectures, blockchains require consensus to be formed among participants for information to be added. Information is collected into blocks which are cryptographically linked to preceding blocks. These features combine to make the blockchain tamper evident. The blocks are chained together using a cryptographic signature called a hash, which is stored at the beginning of the block, and represents all previous transactions that have taken place. This process ensures it can be verified because the information cannot be manipulated without changing the hash, and each hash forms part of that information, like a kind of wax seal. A hash can be thought of as a digital fingerprint that uniquely represents the content of the data.

Each node on the network maintains a shared copy of the ledger, and for its synchronization, a peer-to-peer network is needed as well as a consensus algorithm to ensure addition and replication of blocks across its nodes. One such consensus algorithm is called Proof of Work (PoW)[33] and the participants that take part are special nodes known as miners, using a process called mining. In PoW, miners compete with each other by solving a complicated mathematical puzzle where the solution can be easily proven, and the first one to solve it is the winning miner. Miners validate new transactions, record them on the blockchain, and get rewarded for this task in digital tokens. In this way, a public network can be self-sustaining because it can reward its participants for taking part. However, the recording of transactions is slow, often taking several seconds for a block to be added. Bitcoin uses PoW. While Blockchain owes its fame as being the technology behind Bitcoin, there are now several hundred different blockchains which offer a variety of features that extend way beyond cryptocurrency.[34]

Furthermore, PoW is designed for open, public networks and therefore it is generally not suitable for most enterprise applications. For the DoD specifically, networks are private, permissioned, and secured, and other more efficient consensus algorithms than PoW can be used that do not require the use of cryptocurrency or tokens. For example, Proof of Authority, Byzantine Fault Tolerance, or Raft-based consensus is used in the popular Quorum enterprise blockchain,[35] which can achieve several thousands of transactions per second.

Permissioned or Permissionless?

A Blockchain can be either public or private, or, alternatively, permissionless or permissioned. A permissionless blockchain, as its name suggests, offers no permission requirements for access, so the network is completely public, like Bitcoin. Permissionless networks tend to be far more decentralized and slower than permissioned alternatives.

[33] https://cointelegraph.com/explained/proof-of-work-explained
[34] https://blog.bitdegree.org/did-you-know-there-are-861-blockchains-c60e1720fad5
[35] https://www.goquorum.com

Permissioned blockchains, on the other hand, originally had an open, free, and public ideology, but the majority of permissioned blockchains now are private blockchains that require access permissions to participate at various levels, typically focusing on two main aspects: who can join the network and who has access to which transactions. As a result, an owner of a permissioned blockchain can define who can participate in the network, and also define who has access to what within the network. Information on permissioned blockchains is typically validated only by its approved members.

For permissioned Blockchains, there are a number of different approaches to how one can define who has access to what. At the higher levels, existing authentication and authorization mechanisms could be used to decide who has access to the network and which aspects of the network each user has access too. However, far finer levels of granularity can be built into the network itself. For example, Quorum defines permissioning at the node level and transaction level. It uses network permissioning, which can define which nodes can connect to a given node and also to which nodes the given node can connect out to. This ensures that only the nodes that are listed become part of the network. Second, Quorum's so-called enclave encryption encrypts payloads/transactions to make them private to only a subset of the network.

Wallets and Cryptographic Signatures

Most Blockchains use the concept of a wallet, which originally was named that way because it stored a special key that provided access to your Cryptocurrency. However, even on networks that do not use cryptocurrency, a wallet is still used, and this wallet contains cryptographic credentials that identify a user/wallet on the network, and it allows a user to sign transactions, making each transaction identifiable. A simple wallet can be generated using an asymmetric cryptosystem, also known as public key cryptography. These systems have two keys: a public key that can be shared and a private key that is kept secret. Simply put, if you encrypt with one key, you can decrypt with another. Public key encryption is used in every aspect of our on-line experience. For Blockchain, they form the basis of a wallet, which uses these two keys and a derived key, the address. It contains:

- **The private key** – the private key that is kept secret.
- **The public key** – which can be made public.[36]
- **An address on the network** – which is typically generated by taking a hashcode of the public key. Given a hashcode is a one-way function, it is impossible to derive the public key from the address.

Every blockchain transaction has one owner, which is identified through the use of a digital signature that is created using the private key from the wallet and the contents of the transaction. More technically, a digital signature is the encryption of the hashcode of the transaction's content with the user's private key. This provides a mechanism to both identify the creator of the

[36] However, it is not recommended to make a public key public for a cryptocurrency wallet because, although it is not possible now, in the future e.g. using Quantum computing, it could be possible to derive your private key from it.

transaction and to verify that the contents of the transaction have not been changed. In fact, in Blockchain, this hashcode verification is done twice, once per transaction and once per block.

Storing Large Data on the Blockchain?

As discussed, the storing of data on a blockchain ensures its integrity and non-repudiability. However, what if the data is large? Large data will quickly bloat a Blockchain, making it expensive and inefficient to scale. The answer to this problem is to use so-called *off-chained* data. Off-chaining data allows the data to be stored in an external data store but bound on the blockchain, by storing its fingerprint, or hashcode, on chain. A hashcode is a cryptographic mechanism that can generate a small fixed sized fingerprint for any size file, in such a way, that it is virtually guaranteed two files will never generate the same fingerprint. This means that a hashcode uniquely represents the content of a file.

Consequently, if we store the hashcode of a file on the blockchain, and the file in another store, we guarantee two things:

- That the contents of the file have not been changed since it was stored – because otherwise the hashcode would not match the file stored externally.
- And, that the user that stored the external file is identified – because each transaction is signed by the user, using their wallet.

Off-chaining an excellent strategy for tracking external files or datasets on the blockchain because it minimizes the storage on-chain while providing a non-repudiable audit trail for externally generated data. This means it is possible to seamlessly use blockchain with existing data and systems, vastly improve the tracking of data, guarantee the integrity of data, and aggregate multiple copies of data across disparate data systems and applications.

DLT is furthering Web 3.0, or a movement towards decentralized networking technologies using peer-to-peer (p2p) technology to protect individual property and privacy.

Just a few years ago, the idea that we could unseat the Web 2.0 powers (i.e., “Big Tech” companies such as Google and Facebook) was all but implausible. But the advent of distributed consensus protocols has enabled trustless peer-to-peer transactions in places we have previously had to rely on central authorities to hold or transmit data or value. Bitcoin and Ethereum proved the concept and ignited a belief in many of us that we now have the tools to create digital banking, court systems, and other institutions without having to trust that our data won’t be hacked or misused.

Appendix B: Contributors

The Value Technology Foundation would like to thank the following individuals and their organizations for their support in writing this paper.

Co-authors: Dr. Victoria Adams (Value Technology Foundation), Mike Alonso (ConsenSys), Wendy Henry (Deloitte), Dr. David Hyland-Wood (ConsenSys), Walter "Chip" Jansen (ConsenSys), Venkat Kodumudi (CGI Federal), Anoop Nannra (Amazon Web Services), Joel Neidig (SIMBA Chain), Matt Nelson (IBM), Nikhil Shenoy (Colvin Run), John Stevens (Accenture Federal Services), William "Hudson" Sutherland (CGI Federal), Dr. Ian Taylor (SIMBA Chain), and Jeff Tennenbaum (IBM).

Editors: Dr. Victoria Adams, Jason Brett, Frederic De Vaulx, and Whitney Kalmbach (Value Technology Foundation), in addition to Michelle Gitlitz (Crowell and Moring LLP), Dr. Hilary Kalmbach (University of Sussex), and Dr. Ian Taylor (SIMBA Chain).

Additional thanks to: Sherri Sokol (Defense Information Systems Agency), Christopher Hare, Dr. Sandra Johnson, Peter Robinson, and Robert Saltini (ConsenSys), and Caitlin Eckvahl and David Wachsman (Wachsman).