Calhoun
Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

DSpace Repository

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

2022-09

TACTICAL BLOCKCHAIN TO PROVIDE DATA PROVENANCE IN SUPPORT OF INTERNET OF BATTLEFIELD THINGS AND BIG DATA ANALYTICS

Dogum, Gregory; Jones Maia, Kristin L.; Meszaros, Michele I.; Novoa, Jonathan; Villarreal, Rene A.

Monterey, CA; Naval Postgraduate School

http://hdl.handle.net/10945/71131

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

Downloaded from NPS Archive: Calhoun

DUDLEY KNOX LIBRARY

http://www.nps.edu/library

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

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

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SYSTEMS ENGINEERING CAPSTONE REPORT

TACTICAL BLOCKCHAIN TO PROVIDE DATA PROVENANCE IN SUPPORT OF INTERNET OF BATTLEFIELD THINGS AND BIG DATA ANALYTICS

by

Gregory Dogum, Kristin L. Jones Maia, Michele I. Meszaros,
Jonathan Novoa, and Rene A. Villarreal

September 2022

Advisor:	Bonnie W. Johnson
Co-Advisor:	John M. Green

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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

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

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2022	**3. REPORT TYPE AND DATES COVERED** Systems Engineering Capstone Report

4. TITLE AND SUBTITLE
TACTICAL BLOCKCHAIN TO PROVIDE DATA PROVENANCE IN SUPPORT OF INTERNET OF BATTLEFIELD THINGS AND BIG DATA ANALYTICS

5. FUNDING NUMBERS

6. AUTHOR(S) Gregory Dogum, Kristin L. Jones Maia, Michele I. Meszaros, Jonathan Novoa, and Rene A. Villarreal

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

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

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

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This capstone project evaluated the use of blockchain technology to address a number of challenges with increasing amounts of disparate sensor data and an information-rich landscape that can quickly overwhelm effective decision-making processes. The team explored how blockchain can be used in a variety of defense applications to verify users, validate sensor data fed into artificial intelligence models, limit access to data, and provide an audit trail across the data life cycle. The team developed a conceptual design for implementing blockchain for tactical data, artificial intelligence, and machine learning applications; identified challenges and limitations involved in implementing blockchain for the tactical domain; described the benefits of blockchain for these various applications; and evaluated this project's findings to propose future research into a wider set of blockchain applications. The team did this through the development of three use cases. One use case demonstrated the use of blockchain at the tactical edge in a "data light" information environment. The second use case explored the use of blockchain in securing medical information in the electronic health record. The third use case studied blockchain's application in the use of multiple sensors collecting data for chemical weapons defense to support measurement and signature intelligence analysis using artificial intelligence and machine learning.

14. SUBJECT TERMS
blockchain, data provenance, artificial intelligence, machine learning, internet of battle things, data fabric, systems engineering, model-based systems engineering, data architecture, sensors, Internet of Things, Internet of Battlefield Things, data life cycle

15. NUMBER OF PAGES
93

16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

TACTICAL BLOCKCHAIN TO PROVIDE DATA PROVENANCE IN SUPPORT OF INTERNET OF BATTLEFIELD THINGS AND BIG DATA ANALYTICS

Gregory Dogum, Kristin L. Jones Maia, Michele I. Meszaros,
Jonathan Novoa, and Rene A. Villarreal

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2022

Lead Editor: Kristin L. Jones Maia

Reviewed by:	
Bonnie W. Johnson	John M. Green
Advisor	Co-Advisor

Accepted by:
Oleg A. Yakimenko
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This capstone project evaluated the use of blockchain technology to address a number of challenges with increasing amounts of disparate sensor data and an information-rich landscape that can quickly overwhelm effective decision-making processes. The team explored how blockchain can be used in a variety of defense applications to verify users, validate sensor data fed into artificial intelligence models, limit access to data, and provide an audit trail across the data life cycle. The team developed a conceptual design for implementing blockchain for tactical data, artificial intelligence, and machine learning applications; identified challenges and limitations involved in implementing blockchain for the tactical domain; described the benefits of blockchain for these various applications; and evaluated this project's findings to propose future research into a wider set of blockchain applications. The team did this through the development of three use cases. One use case demonstrated the use of blockchain at the tactical edge in a "data light" information environment. The second use case explored the use of blockchain in securing medical information in the electronic health record. The third use case studied blockchain's application in the use of multiple sensors collecting data for chemical weapons defense to support measurement and signature intelligence analysis using artificial intelligence and machine learning.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABMS	Advanced Battle Management System
AI	artificial intelligence
CONUS	Continental United States
CS	chemical sensor
DDIL	disrupted, disconnected, intermittent and low-bandwidth
DOD	Department of Defense
FM	field manual
EHR	electronic health record
HIPAA	Health Insurance Portability and Accountability Act
HLF	Hyperledger Fabric
ICAM	identity, credential, and access management
IoBT	Internet of Battefield (or Battle) Things
IoT	Internet of Things
ISR	intelligence, surveillance and reconnaissance
JAIC	Joint Artificial Intelligence Center
LRF	long-range fires
MAS	multi-agent system
MASINT	measurement and signature intelligence
MBSE	model-based systems engineering
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, civil considerations
MHS	Military Health System
ML	machine learning
NAWC/WD	Naval Air Warfare Command Weapons Division
NPS	Naval Postgraduate School
ONR	Office of Naval Research
OODA	observe, orient, decide, act
SE	systems engineering

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Future large-scale combat operations against a peer or near-peer adversary will involve a cyberspace domain in addition to the more traditional physical domains of air, land, sea, and space. The role that data and information play at every point in this continuum cannot be understated. Moreover, the ability to communicate effectively and coordinate across multiple domains simultaneously—to have the necessary command and control—is dependent upon accessible and reliable information. The U.S. Army is drafting a new Army Doctrine Publication 3-13, titled *Information,* that "links the military applications of information to all warfighting functions, branches, and forms of warfare" (U.S. Army Combined Arms Center 2022, 2). These shifts in how the Army will maintain an advantage on the battlefield underscore the critical role that data and information play as a tool of war.

The primary objective of this capstone project was to explore the use of blockchain in a variety of contexts that are relevant to the DOD. First, the team researched the current body of work on blockchain and adjacent topics, such as the Internet of Things (IoT), big data, artificial intelligence (AI) and machine learning (ML). The research revealed an emerging concept called the "Internet of Battlefield Things" (IoBT). Tosh et al. (2018) write about how the IoBT could fulfill a "strong need of decentralized framework…to serve the purpose of the battlefield environment" (2). Kott, Ananthram, and West (2016) highlight several cybersecurity challenges associated with IoBT availability, confidentiality, and integrity, whereas Tosh et al. (2018) discuss how blockchain technology could benefit the IoBT architecture.

In addition to the myriad devices on the network (e.g., IoBT), data storage is another critical aspect of managing data, both now and in a future environment marked by decentralized information. Blockchain, when combined with the use of a data storage mechanism, could aid in the availability, confidentiality, and integrity of IoBT devices and their data. The team looked at the potential to use a tactical data fabric as an "off chain" data storage mechanism. Data fabrics automate the discovery, governance, and consumption of data that enables users to access data when and where they need it, without

requiring any knowledge of where the data resides. A data fabric is a mechanism that can link a multitude of data management sources together in order to facilitate accessibility to data—no matter where it resides. These data management sources could be traditional databases, data lakes (IBM 2018), or data warehouses (IBM 2021). Therefore, the tactical data fabric could be a viable solution to facilitate data access across warfighter functions and mission command systems (Patel et al. 2021).

The insight from this research was overlaid with existing concepts such as the data life cycle, and the DOD's common decision-making framework: the observe-orient-decide-act (OODA) loop. There are four general phases to the data life cycle: data creation (or generation), data reading (or consumption), data updating (or modification), and data deletion (or archiving). These phases apply to nearly every type of data in nearly any type of system. It is important to understand how interactions with the data at each of these phases of the life cycle affect the data's inherent reliability. Tracking the movement of data through this data life cycle provides data provenance, which enables a potential data consumer to determine the data's reliability and validity. As decision makers use data (and downstream analysis of that data, say with the assistance of AI) in their implementation of the OODA loop framework, the criticality of data provenance becomes clear. The use of blockchain can provide built-in assurance of data reliability, which in turn decreases OODA loop timing and improves decision-making.

Next, the team developed some generic systems engineering architectures to illustrate how blockchain can address data provenance and ensure trust in those data. This process identified a variety of actors from various users (e.g., such as data owners and consumers) to software systems that would be required, as well as the data fabric, and the Hyperledger Fabric (HLF) network (i.e., the blockchain component). In addition, several application programming interfaces (APIs) would be likely needed: an access API, a data provenance API, and an enterprise API. The overall focus of utilizing blockchain to provide reliable data provenance is to provide a new method where operators can track devices and editors of data.

This architecture was then extended through the development of three use cases, each with its specific architecture, which further illustrates how the implementation of blockchain could work and assesses its utility and limitations. These use cases allowed the team to explore blockchain's potential to verify users, validate sensor data fed into AI models, limit access to data, and provide an audit trail across the data life cycle.

In the first use case, we explored how blockchain can facilitate secure and trustworthy data transfer at the tactical edge to utilize long-range fires. The second use case provided an example in more of an operational context, where blockchain provides an audit trail to enable a robust electronic health record (EHR) that is accessible at any point in the continuum of healthcare delivery. Last, the team's third use case looked at managing the flow of data coming off sensors in the field and into AI models to support specific types of intelligence (e.g., measurement and signature intelligence (MASINT) for chemical defense efforts). This use case has both operational as well as strategic contexts and demonstrates how blockchain ensures that data fed into AI models is valid and reliable.

While these use cases utilized a simplified architecture to facilitate notional applications of blockchain, it nevertheless demonstrated the real potential of this technology to solve or at least mitigate current and future challenges of managing and protecting vast amounts of data. The team was able to explore the options of storing data both on and off the blockchain. These options demonstrate how blockchain technology can be tailored to specific circumstances—not just across strategic, operational, and tactical contexts, but also across the Services to meet their unique mission needs. The Joint Force of the future will need to be savvy in its generation and consumption of data—data that will be imperative to securing an advantage on the battlefield, but is also critical during peaceful, but competitive, periods between armed conflict.

References

Kott, Alexander, Ananthram Swami, and Bruce J. West. 2017. "The Internet of Battle Things." Computer 49 (12) (December): 70–75. https://doi.org/10.1109/MC.2016.355.

International Business Machines (IBM). 2018. Governed Data Lake for Business Insights: Explore the Key Building Blocks to Effectively Deliver Trusted Data. https://www.ibm.com/downloads/cas/RMAMZNRY.

IBM. 2021. *How to Choose the Right Data Warehouse for AI.* https://ibm.com/downloads/cas/QK7MQ7YY.

———. 2022. “What is a Data Lake?” Accessed July 17, 2022. https://www.ibm.com/topics/data-lake.

Patel, Nihar, Upesh Patel, Evert R. Hawk II and Krupal Kapadia. 2021. “Stitching the Army’s Data Fabric.” *Army ALT Magazine* (Fall 2021): 14–19. https://asc.army.mil/web/news-stitching-the-armys-data-fabric/.

Tosh, Deepak K, Sachin Shetty, Peter Foytik, Laurent Njilla, and Charles A Kamhoua. 2018. “Blockchain-Empowered Secure Internet -of- Battlefield Things (IoBT) Architecture.” In *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 593–98. IEEE. https://doi.org/10.1109/MILCOM.2018.8599758.

U.S. Army Combined Army Center. 2022. *Combined Arms Doctrine Newsletter & Doctrine Developer’s Guidance*. Fort Leavenworth, KS: U.S. Army Combined Arms Center.

ACKNOWLEDGMENTS

Team “Off the Chain” has much to be grateful for both in the completion of this capstone project as well as in the completion of the Master’s in Systems Engineering Management curriculum. First, we’d like to thank our advisors, Dr. Bonnie Johnson, Mr. Tony Kendall, and Mr. Mike Green, for providing relentless encouragement but also for the needed structure as we waded into the murky waters of completing a thesis project. Their guidance and support enabled us to get our legs under us so that we could run with our ideas and develop them into something we could write about.

We would also like to thank all the professors that we have had over the past two years. It’s in retrospect that we can see how their teaching, their assignments, and their feedback set us up to be successful in this culminating project.

Last, as adult learners (and distance learners) who are also navigating full-time jobs, careers, and families, the support of both our “work families” and our actual families helped us get through times when deadlines were tight and the workload was high. They gave us slack when we needed it, encouraged us when we felt discouraged, and believed in us even when we had doubts. As we stand on the shoulders of giants and strain to reach new heights, it’s important to recognize that the other hand is often being held by those who help us keep our balance.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This systems engineering capstone thesis report captures the team's work over the last six months in evaluating blockchain and its potential benefits for the DOD, all while using the systems engineering process. However, it is helpful to provide additional context for the strategic, operational, and tactical paradigm the DOD finds itself in as it prepares for the conflicts of the future.

A. BACKGROUND

Future large-scale combat operations against a peer or near-peer adversary will involve a cyberspace domain in addition to the more traditional physical domains of air, land, sea, and space. The U.S. Army's approach to this updated landscape is termed "Multi-Domain Operations." It outlines a continuum of operations from a peaceful competition phase to full-on armed conflict with an adversary (U.S. Army Training and Doctrine Command 2018). The role that data and information play at every point in this continuum cannot be understated. Moreover, the ability to effectively communicate and coordinate across multiple domains simultaneously—to have the necessary command and control—is dependent upon accessible and reliable information.

The importance of information in the future war will be further highlighted in the updated version of FM 3-0 "Operations" (due for publication in summer 2022) that "established multi-domain operations as the Army's operational concept" (U.S. Army Combined Arms Center 2022). This updated field manual adds information as a third dimension to the operational environment; and information is now included in the new combat power model. The (familiar) mission variables of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (abbreviated as METT-TC) have now had information integrated into them and the abbreviation has been updated to METT-TC(I). Last, the Army is also drafting a new Army Doctrine Publication 3-13, titled "Information." This new doctrine "links the military applications of information to all warfighting functions, branches, and forms of warfare" (U.S. Army Combined Arms Center 2022). These shifts and evolutions in how the Army will maintain an advantage on the battlefield underscores the critical role that data and information play as a tool of war.

Engineered, complex adaptive systems-of-systems are now commonplace across the Department of Defense to support Joint and Coalition engagements. Data to support these engagements is sourced from an increasingly diverse collection of sources including ground, air, and sea sensors. Artificial intelligence (AI) models have evolved to ingest data from these disparate sources and make it usable for decision-making. The DOD's common decision-making framework is the observe-orient-decide-act (OODA) loop. The use of AI to support this framework can decrease OODA loop timing. Unfortunately, these AI models are vulnerable to several factors that impact the consistency, timeliness, accuracy, and availability of information. Some factors include the quality of the original data as well as any humans-in-the-loop that interact with these models and influence the analysis or other outside threats that may disrupt the information collected, measured, and processed.

These varied and disparate sensors are analogous to the "Internet of Things" (IoT), the myriad of internet-connected devices that exist in civilian (but also military) settings. In both instances, there is a strong need to ensure the data is secure and reliable, so that the outputs of AI models leveraging data from the IoT can be trusted and used to improve decision-making. While much has been written on the IoT, there is an emerging concept of the "Internet of Battlefield Things" (IoBT). Tosh et al. (2018) write about how the IoBT could fulfill a "strong need of decentralized framework…to serve the purpose of the battlefield environment" (2). This same work also discusses how blockchain technology could be used for a variety of purposes to benefit the IoBT architecture. Of relevance to this capstone project are "transparent and assured data provenance" and "verifiability and audit" of the data being passed (Tosh et al. 2018, 2). Moreover, the decentralization that blockchain can enable further strengthens its use to secure the IoBT.

Firican (2017) also hints at the characteristics and properties of big data—first there were 3 V's, which have since expanded into up to 10 V's of data: volume, velocity, variety, variability, veracity, validity, vulnerability, volatility, visualization, and value (headings of article paragraphs). Of particular focus in this capstone was the veracity of big data. Blockchain delivers a verifiable way to build confidence in AI models at the tactical level for decision makers to feel confident in their operational decisions by providing security, scalability and dynamic class structure opportunities allowing the use of multiple roles by individuals.

Another complementary technology to the IoBT and blockchain is the use of a data fabric. Data fabric is an emerging concept that enables efficient data sharing between systems in tactical and operational environments. The goal is to provide pertinent data at the proper moment using common interfaces to ease the complications of data sharing across unique systems to aid in decision-making. Data fabric also supports and enables decentralization of data and processing. A data fabric is a mechanism that can link a multitude of data management sources together in order to facilitate accessibility to data—no matter where it resides. These data management sources could be traditional databases, data lakes (IBM 2018), or data warehouses (IBM 2021). Data fabrics are proposed to provide full data governance and lineage from data ingest to application usage. It should be noted that data fabrics (as defined by industry) are not meant to replace these data management sources. Instead, data fabrics link them together as each data management solution offers benefits depending on the complexity of data stored and availability of data required.

This shift to more decentralized architectures could help overcome some of the limitations of the current, more centralized infrastructures, and facilitate improved performance and value of the network overall. This shift may already be happening. The DOD is moving from a network-centric model to data-centric model, as expressed in the "Creating Data Advantage" memo signed by the Deputy Secretary of Defense, the Honorable Kathleen Hicks. The memo outlines the goal of "improving performance and creating decision advantage at all echelons from the battlespace to the board room" (Hicks 2021, 1). In a data-centric environment, information is stored in shared locations providing various users access to the same data set. These locations can be architected in centralized or distributed schemes and reside on tactical servers or in the cloud. Data provenance, however, can become challenged when tracing the source of information and the history of changes to that information when data is accessible to multiple users. This becomes further challenged due to the varying clearance levels of users and classification of data which limit who can access what information.

To optimize the processing of data at the tactical edge, AI-enabled computing can be used to validate data before its placement on the data fabric. AI models rely on data to learn behaviors through pattern recognition and/or correlation analysis. Large amounts of data are necessary to increase confidence levels in the accuracy of model output. This data collection, however, can be challenged when sensors are placed within contested regions at the tactical edge. In these regions, AI data validation models are susceptible to various physical and cyber threats including poisoning and impersonation that can cause models to deviate from their intended operation. Poisoning is the purposeful tampering of data that is used to train AI algorithms—a tactic that is nearly untraceable (Culpan 2022). This can cause the AI to behave in unintended ways and prevent it from recognizing patterns or making the desired correlations (Kuzlu 2021). Furthermore, disrupted, disconnected, intermittent and low-bandwidth (DDIL) environments limit how much data can be sent to computing platforms to support multiparty learning of the AI models themselves. To address these challenges, the implementation of a data fabric supported by blockchain may be a means to facilitate the achievement of this DOD goal.

B. PROBLEM STATEMENT

The Armed Services and the DOD, writ large, have openly communicated their strategies to prepare for the future fight—one against a savvy, well-resourced peer or near-peer adversary (e.g., China and Russia). A large impetus of this strategic direction is a huge modernization push to not only keep pace with adversaries but also to forge the leading edge of technology to gain an advantage on the battlefield. This has caused a greater emphasis on tools like digital engineering, artificial intelligence (AI), machine learning (ML), and the use of a distributed ledger to trace the life cycle of data. The DOD's current use of consolidated data centers (data silos) and big data analytics is limited by its own architectural framework(s) and is currently undergoing modernization towards concepts such as data fabrics.

Cloud computing is also limited because it quickly exhausts the available bandwidth at locations with inferior infrastructure and becomes impractical. There are security implications of cloud computing that pose another challenge to its use—one that needs to be mitigated before broader adoption is possible. Vulnerabilities in current AI/ML data influence a program's ability to make expected decisions due to corruption of the imported data. Mobile computing centers are continually put at risk in the field as they are commonly located near enemy sensors, putting them at risk of falling under hostile control. Commercial-based cloud computing environments are also limited by their rigid class structure. Tactical environments often require the use of more fluid roles where the same individual can take on multiple roles (producer, processor, and consumer) at any given time.

Blockchain is an emerging area of technology that could improve the use of big data AI models that process diverse data from disparate sources, ensuring the veracity of the data and subsequent outputs. However, several challenges must be overcome to implement blockchain, including (edge) device access to the blockchain, data processing through the blockchain, and user/device access to this data and subsequent results.

With the exponential growth of IoT devices and now IoBT sensors increasing data velocity and volume, it makes it difficult to manage this big data while assuring its quality to prevent bad data from getting ingested. This could have bad consequences on the battlefield. To keep pace with near-peer threats, data obtained from sensors is used to feed AI model data sets. However, these data sets are vulnerable to physical and cyber threats which need to be addressed to build confidence and trust in AI model performance.

The DOD lacks a modern approach to data curation and provenance, including identity, credential, and access management (ICAM) of users and devices to achieve a truly data-centric architecture in a DDIL environment. Leveraging disparate sources of data from low-cost attributable sensors has further challenged the incorporation of zero-trust principles.

C. CAPSTONE OBJECTIVES

The primary objective of this capstone project was to explore the use of blockchain architecture in a variety of contexts that are relevant to the DOD. These use cases cover the potential to verify users, validate sensor data fed into AI models, limit access to data, and provide an audit trail across the data life cycle.

Supporting objectives include:

- Develop a conceptual design for implementing blockchain for DOD tactical data and AI/ML applications.
- Identify and understand challenges and limitations (including network limitations) involved in implementing blockchain for the DOD's tactical domain.
- Describe the benefits of blockchain for these various applications.
- Evaluate this project's findings to propose future research into a wider set of blockchain applications.

The project team explored the use of a blockchain approach in multiple use cases. One use case demonstrated the use of blockchain at the tactical edge in a "data light" information environment. Another use case explored the use of blockchain in securing medical information in the electronic health record (EHR), a very "data heavy" example that aggregated data from an individually worn sensor all the way back to CONUS hospitals, and even Veterans' Administration-delivered care. Third, the last use case explored securing data from multiple sensors collecting data for chemical weapons defense to support measurement and signature intelligence (MASINT) analysis using AI/ML.

The team used these examples to address the following project questions:

1. Can blockchain enable data traceability to/from a specific sensor asset and user over the entire data life cycle?
2. Can data passed to AI-models and/or digital twins be prioritized to mitigate latency challenges?

3. How can blockchain smart contracts be used to manage data ingest and how can it facilitate tailoring access to accommodate updates to policy/ authorities and address objectives with the DOD's AI Policy memorandum?

D. TEAM ORGANIZATION

Table 1 provides an overview of each team member's responsibilities. However, all team members' participation in each area was integral to the success of this capstone project.

Table 1. Team Member Roles and Responsibilities

Team Member	Roles	Responsibilities
Dr. Bonnie Johnson **Mr. John Green** **Mr. Tony Kendall**	Capstone Advisors	Provide guidance and support to capstone team Coordinate with ONR Blockchain and HLF subject matter expert
Ms. Maria G. Medeiros	Funding Sponsor	Provide funding through the ONR Neptune program, Office of Naval Research, Code 333
Mr. Bruce Nagy	Topic Sponsor	Provide sponsor feedback on project objectives and results
Mr. Jonathan Novoa	Team Lead	Lead team meetings and organize execution of project deliverables Provide updates to capstone advisors and stakeholders
Mr. Greg Dogum	Deputy Team Lead	Provide guidance at team meetings and organize execution of project deliverables Provide updates to capstone advisors and stakeholders
Mr. Rene Villarreal	Lead Engineer	Direct architecture development for use cases Conduct functional analysis to translate requirements into a verified model Use case development
Ms. Kristin Jones Maia	Lead Editor	Quality control and configuration management Report and documentation editing Use case development
Ms. Michele Meszaros	Lead Analyst	Oversee collection and analytics requirements Direct research of historical project related data Use case development

Team "Off the Chain" was composed of five NPS students as shown in Table 1. The team interacted with two capstone advisors: Bonnie Johnson and John "Mike" Green from the Naval Postgraduate School with support from Tony Kendall; and the project sponsors: Bruce Nagy from Naval Air Warfare Command Weapons Division (NAWC/WD) and Maria Medeiros the financial sponsor (ONR Neptune program, Office of Naval Research, Code 333). The capstone advisors provided guidance and support to this capstone team. The team structure included a Team Lead and Deputy Team Lead, followed by provided support.

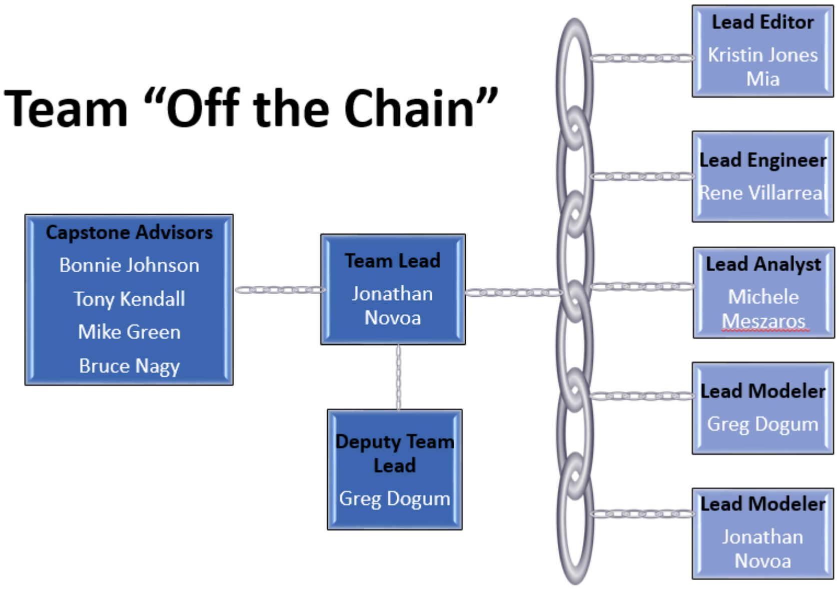
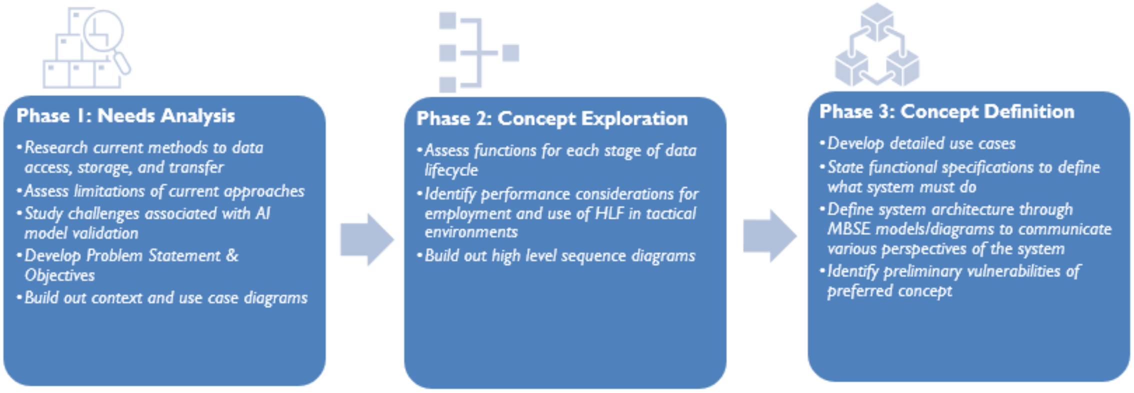


Figure 1. Team Organization

E. PROJECT APPROACH

The team conducted a systems analysis, supported by model-based systems engineering (MBSE), to define, develop, design, and model how blockchain can be used to ensure data veracity from disparate sensors (e.g., IoBT) and sources to support data integrity and security and for use by AI/ML models. A team developed a conceptual architecture that could allow decentralized, but widely accessible access to trusted data to support decision-making. The project approach was based on three phases as referenced in the Project Approach graphic in Figure 2.



Phase 1: Needs Analysis

- *Research current methods to data access, storage, and transfer*
- *Assess limitations of current approaches*
- *Study challenges associated with AI model validation*
- *Develop Problem Statement & Objectives*
- *Build out context and use case diagrams*

Phase 2: Concept Exploration

- *Assess functions for each stage of data lifecycle*
- *Identify performance considerations for employment and use of HLF in tactical environments*
- *Build out high level sequence diagrams*

Phase 3: Concept Definition

- *Develop detailed use cases*
- *State functional specifications to define what system must do*
- *Define system architecture through MBSE models/diagrams to communicate various perspectives of the system*
- *Identify preliminary vulnerabilities of preferred concept*

Figure 2. Project Approach Phases

During phase 1, the team conducted a literature review to provide a foundation of knowledge about blockchain and its applications. The team studied the capabilities and limitations of current approaches and applications of blockchain. The team identified and verified tactical stakeholder needs to align project objectives to overall intended outcomes and research goals. The team developed a problem statement, project objectives, and a project approach to study the application of blockchain. The team identified three potential use case applications to support the project's study of the potential challenges and risks of implementing and integrating the emerging blockchain technology into the DOD.

During phase 2, the team studied the use of blockchain in the tactical domain through concept exploration and system analysis. The team conducted a functional analysis of a generic blockchain system. The team developed MBSE artifacts to capture the blockchain data life cycle, data provenance, functional sequence diagrams, and conceptual architectures.

During phase 3, the team used three scenarios to explore and define the concept of applying blockchain to DOD-specific use cases. We defined system architectures through MBSE models and diagrams for each of the three scenarios. The team evaluated the use of blockchain by identifying and comparing the benefits and challenges in the use cases.

F. CAPSTONE REPORT OVERVIEW

This capstone report covers the team's approach to understanding how the DOD could use blockchain to achieve its strategic, operational, and even tactical objectives in an information-intense competition and conflict landscape. The context for this, the driving forces in this space, and the team's approach to this project were covered in Chapter I. Chapter II covers the research the team conducted to execute the project. This research spanned a variety of sources across a spectrum of topics related to blockchain applications in the DOD. Chapter III covers the team's overarching approach to this problem space and the universal framework that we utilized to develop and evaluate three separate use cases. Chapter IV details those three use cases: long-range fires, medical data and the EHR, and using MASINT to interpret sensor data for chemical defense. These use cases are structured similarly to enable a comparison across the different applications. Chapter V summarizes our conclusions from this project and identifies areas for future research.

II. LITERATURE REVIEW

Team “Off the Chain” performed a literature review to learn about blockchain technology, its potential application to military use cases, existing architectures for blockchain applications, and the possible utility of HLF to our proposed use cases. This review covered peer-reviewed journal articles, conference proceedings, books, DOD publications, and DOD and industry websites. In addition to the topics above, the research also covered the use of blockchain to facilitate and improve the use of artificial intelligence and machine learning. The information gathered from these various sources provided insight into how the DOD could further explore the use of blockchain to achieve strategic, operational, and even tactical mission accomplishment.

Through this blockchain research, the team also learned more about the larger undercurrent that is shifting information systems towards increased decentralization. In many ways, the emergence of blockchain is enabling this transition in ways that may not be possible without it. However, this evolvement does not come without its inherent challenges. Problems around data sharing, security, integrity, and privacy as well as storage and analysis are common themes that arose in the literature when the IoT and decentralized networks were discussed. Most of these sources saw blockchain as a potential solution to some or all of these problems.

A. DECENTRALIZED SYSTEMS AND THE INTERNET OF THINGS

The team’s research revealed the degree to which systems are moving more and more towards decentralization. Driving this trend has been the exponential growth in mobile devices and the services provided on those mobile platforms (Li 2021). Not only does this increased activity generate a tremendous amount of data (Li 2021) but can also lead to significant generation of “execution traces”—data that is generated by a system about its performance (Binlashram 2020). In addition, the increased number of “smart” and/or internet-connected devices pushes this expansion further. Moreover, the roll out of next-gen networks such as 5G further supports a diverse “ecosystem…of interconnected devices and services” (Benzaid 2021, 1). These trends make the shift to decentralization seem nearly inevitable, as a network on this scale would make having a central, organizing authority prohibitive—if not impossible.

1. The Internet of Things

The broadening of devices that connect to the internet (as described above) has led to the term "Internet of Things" (or IoT) and is inherently decentralized, distributed, and global. Clark (2016) describes the IoT as an interconnected network of devices capable of exchanging information on what they are sensing *in* the environment, and information *about* the environment, with external parties. On a pseudo microcosmic level, multi-agent systems (MAS) are similar to the IoT in that they integrate a diverse range of devices (or "agents"), but are intentionally constructed. They still have a degree of being distributed and may include a collection of software agents, robots, sensors, and autonomous agents working together to support business processes (Kapitonov 2017). Despite these differences, both the IoT and a MAS generate a large amount of data that needs to be protected, secured, transmitted, and utilized.

The prevalence of the IoT has allowed certain sectors to leverage its benefits in ways that are specific to their purpose. For example, there is the Industrial Internet of Things (IIoT), sometimes described in connection with the term Industry 4.0. In the preface to the book *AI-Enabled Threat Detection and Security*, the editors described this application of IoT and Industry 4.0 as "making use of intelligent, interconnected cyber-physical systems to automate all phases of industrial operations" (Karimipour and Derakhshan 2021, v). This shift towards a myriad of connected devices that generate large volumes of data, which are then used to make decisions (e.g., automate some processes) is reflective of the potential benefits that the IoT can bring to bear. However, this architecture does come with challenges. Chen et al. (2022) discuss data sharing and data privacy challenges, in addition to secure ways to store the data generated by the IIoT. They also explore storage handling of raw data and efficient ways to query the vast amounts of generated data (Chen et al. 2022).

Just as there is an Industrial Internet of Things, the research revealed that the military also has a niche IoT. The term Internet of Battlefield Things (IoBT) emerged in the literature as an important concept for orchestrating military operations on an information-dense battlefield. Tosh et al. (2018) describe the IoBT as the collection of "combat equipment, warfighters, and vehicles that can sense and disseminate information from the battlefield" (1). Kott, Swami, and West (2016) provide a similar description, where the IoBT is a distributed, interconnected network of devices that execute a myriad of automated tasks to support sensing and coordinated defensive/offensive actions. Much like the IoT and the IIoT, the heterogeneity of this larger IoBT network "in terms of network standards, platforms, (and) connectivity" introduces similar challenges to the IIoT (1, "and" added). Additionally, Crăişor-Constantin Ionită (2020) lists "great innovations in robotics, artificial intelligence, nanotechnology and unmanned systems" as drivers of change in how wars are fought (25). While he does not specifically call these out as part of the IoBT, they certainly are a part of that heterogeneous IoBT network that supports the U.S.'s ability to fight and win wars.

2. Big Data

Another related concept revealed in the research that bears discussion is big data. Kumar et al. (2020) define big data as "data sets that are large or complex in which traditional data processing applications are inadequate" (115). They go on to add that big data also includes not just the creation and analysis of data, but the actions of storing it, searching it, transferring it, and even visualizing it. The IoT is easily capable of generating this big data as it becomes more pervasive and expansive. Artificial intelligence and machine learning (discussed more in a later section) also support the generation of big data as well as subsequent analysis and visualization. The challenges that big data create are part and parcel of the challenges with the IoT. The same challenges that Chen et al. (2022) identify with the IoT, Kumar et al. (2020) also point out with big data: managing the structure, storage, transfer, sharing, analysis, and visualization—all while ensuring security and privacy protections.

3. Trust

In addition to an expanding, diverse network of decentralized devices generating large amounts of data, the issue of how best to share that data and with whom raises another challenge of this paradigm. The literature review revealed considerations around trust and its impact on managing and securing the IoT, the handling of big data, etc. In centrally controlled networks, the owners of the network can vet users and put protections in place to reduce the risk of intrusion or data theft. But this is not possible in decentralized networks with no central authority. Reyna et al. (2018) discuss trust in the integrity of data, and the value in ensuring that shared data (by financial institutions, government agencies, etc.) has not been tampered with or manipulated. Because the data is generated in a distributed and autonomous way, it can make the IoT vulnerable to tampering (Kumar and Sharma 2021). When the IoT is providing insight into critical systems like smart cities and smart transportation, this tampering can have significant consequences (Kumar and Sharma 2021). The concept of trust also goes beyond trusting the data and extends to the parties that are interacting as well.

4. Artificial Intelligence and Machine Learning

Advancing alongside, but also in support of, these various IoTs and big data have been increasingly sophisticated artificial intelligence (AI) and machine learning (ML) tools. Gregory C. Allen (2020), in his role as the Chief of Strategy and Communications at the Joint Artificial Intelligence Center (JAIC) published *Understanding AI Technology*, which covers the spectrum of AI technology and differentiates it from ML systems. Allen's Executive Summary notes that AI technology has been around for decades and can include mature technology like autopilot on aircraft or missile guidance. Modern advancements in AI have led to machine learning (ML), which is a subset of AI. The distinguishing difference is that, generally, humans program the AI whereas ML "allows machines to learn from data" (Allen 2020, 3). AI technology is programmed using "if, then" statements; ML systems can program themselves by using a (human-generated) algorithm and a training data set, that then results in an AI model (Allen 2020). The JAIC document goes on to categorize ML systems into "supervised learning," "unsupervised learning," "semi-supervised learning," and "reinforcement learning" (Allen 2020, 4). Reinforcement learning is perhaps most on the leading edge, where "AI agents gather their own data and improve based on trial and error. As exciting as the development and evolution of AI/ML systems are, these systems are not immune from manipulation and attack" (Allen 2020, 4).

Marcus Comiter (2019) discusses how AI systems are "vulnerable to a new type of cybersecurity attack called an 'artificial intelligence attacks'" and how these types of attacks are profoundly different than more traditional cyber-attacks (1). In these AI attacks, perpetrators would feed data into the system to change the behavior or outputs of that technology to achieve their malevolent objectives (Comiter 2019). The ability to leverage physical objects in an AI attack is one example of why these attacks are so different. Comiter (2019) uses the example of AI in a self-driving car. If an AI attack could "trick" the car into "seeing" stop signs as green stop lights, it could cause significant physical damage and human harm (Comiter 2019, 1).

The concepts and themes introduced above: the IoT, big data, AI/ML, and the challenges of trust, scalability, and data integrity could be addressed with blockchain technology. In fact, that majority of the team's research discussed these themes in the context of how blockchain can make them better—more reliable, more secure, and more scalable.

B. BLOCKCHAIN APPLICATIONS

While its original use was cryptocurrency, blockchain technology has vastly broader applications. It is uniquely poised to expedite the transition to decentralized, data-centric systems. This section covers the team's research on blockchain technology and its applications, both within and outside of a military context. Chapter III will cover a more in-depth discussion of the specific application of blockchain technology to the military, such as the IoBT.

1. What Is Blockchain

Blockchain is a distributed, immutable ledger that records transactions in blocks and tracks assets stemming from those transactions (International Business Machines (IBM) 2022). When a transaction is initiated using blockchain technology, it creates a block for that event (i.e., a record is created in the ledger). This block contains data related to the transaction as well as the asset being exchanged (e.g., as with cryptocurrency). As additional transactions (i.e., events) occur, the blockchain software "strings" these transaction "blocks" together both linearly and chronologically. Put another way, blockchain participants can add records (blocks) to the ledger, but not edit or remove earlier records (blocks). Because the ledger is distributed, it means all participants have the ledger. It is immutable because manipulating or tampering with any of the records on every participant's ledger would be difficult, if not impossible.

2. Smart Contracts

Blockchain can become even more powerful when combined with smart contracts. Smart contracts allow transactions to occur automatically so long as a set of given conditions are met. They are "written rules stored in the blockchain" (Saberi et al. 2018, 2120) that ensure specific conditions are met. As such, they can be used to automate many processes in each IoT network (Palaiokrassas et al. 2021). Examples include actor certification and approval, and automated updating of ownership records of goods as they are bought, sold, and delivered. Battah et al. (2020) also discuss the use of smart contracts for multi-party authentication to facilitate the appropriate sharing of encrypted data on a public platform.

3. Applications and Benefits of Blockchain

Supply chain management is an area that is well suited to early adoption of blockchain technology. Saberi et al. (2018) examined the use of blockchain technology and smart contracts in supply chain management. They looked specifically at how these tools could ensure that supply chains meet certain sustainability metrics, by tracking conditions that could pose environmental, health, and safety concerns. This could include full transparency of a product's origin (Saberi et al. 2018). Malik et al. (2019) propose a consortium blockchain in their paper to track transactions and interactions among supply chain participants. Their model incorporates trust and reputation scores based on the transactions to address the challenges of trust in highly decentralized networks.

This utility also extends to military supply chains. In a March 2020 report, the Value Technology Foundation dedicated an entire chapter to blockchain's potential to improve the efficiency of defense logistics and supply chain operations (Adams et al. 2020). Rahayu et al. (2019) also wrote of blockchain applications within military supply chains. They highlight the issue of counterfeit parts contaminating military supply chains and discuss how blockchain could help prevent this (Rahayu et al. 2019). While Rahayu et al. provide a perspective from the Malaysian military; the Canadian military has also explored this same application of blockchain. Willink (2018) from Defence Research and Development Canada raises a similar concern about counterfeit parts in *On blockchain technology and its potential application in tactical networks*. Kendall et al. (2021) explored applying blockchain to the Navy's logistics through the examples of transaction audit trails (both from a financial and inventory perspective), serial number tracking, and maintenance log integrity.

Beyond the direct application of blockchain technology to specific sectors or disciplines, a large portion of the team's research discussed the application of blockchain more generally in the context of the IoT, big data, and AI/ML.

a. Security

Reyna et al. (2018), mentioned previously, explored the integration of blockchain and the IoT. They highlight benefits such as increased trust because the information is reliable and traceable, supporting increased decentralization, and greater autonomy and services among other benefits (179). Makhdoom et al. (2018) also studied blockchain's utility for the IoT. They highlight some inherent challenges with the IoT, namely security and privacy issues that can get neglected in a centralized framework. The application of blockchain can enable the IoT to become more decentralized, self-regulated, and ensure trust. While they highlight other work on blockchain and IoT going back to 2016, their paper also focuses on some of the challenges and impediments they identified with implementing this (Makhdoom et al. 2018). Abdelmaboud et al. (2022) also discuss blockchain's ability to address the scalability, security, privacy, trust, and even interoperability challenges that exist in the IoT. They also propose a blockchain taxonomy and evaluate various blockchain platforms (Abdelmaboud et al. 2022).

Panarello et al. (2018) also look at how blockchain can address security challenges with the IoT with its "immutability, transparency, auditability, data encryption and operational resilience" (1). Kumar and Sharma (2021) also discuss blockchain's ability to assure trust in an IoT environment. Applying this concept further, Attkan and Ranga (2022) discuss the need for IoT devices to be able to mutually authenticate each other and blockchain’s ability to support this (with assistance from AI), despite high levels of heterogeneity.

b. Data Value

Jeong (2021) explored the application of blockchain to IoT-generated data and existing inadequacies of cloud storage. Blockchain could help ensure the data is protected and accessible. Palaiokrassas et al. (2021) also write of blockchain’s ability to secure the data generated by the IoT, and when combined with smart contracts can facilitate and automate data storage, privacy, and sharing. They write that doing so could enable a “Blockchain Marketplace” for the IoT data to be exchanged for virtual currencies or other assets (2). In a similar vein, Draskovic and Saleh (2017) recognized the value inherent in the data itself, claiming “(d)ata is the new oil” and propose a marketplace for IoT sensor data based on blockchain. Moke, Low, and Kahn (2021) also present a blockchain-based IoT model in their paper with the goal of preventing data loss.

c. Edge Computing

Xu et al. (2021) propose using blockchain to improve the computer performance of the actual devices in the IoT. They present an architecture for “distributed secure edge computing” where blockchain ensures data integrity in this environment (1). Of note, this paper uses HLF, a blockchain platform of interest to the DOD, to build out and test their architecture. We will discuss HLF in more detail in Chapter III. Gan et al. (2021) also examine edge computing architecture in harsh environments, and the ability of a consortium blockchain to facilitate information security, traceability, and sharing of data. This is particularly relevant to possible applications of blockchain in the IoBT. Regarding computing or system performance, Pajooh et al. (2021) examine blockchain’s benefits, but in a way that would not compromise performance. These authors also used HLF in their model to facilitate local authorization of IoT devices and traceability of the data they generate. Another paper uses HLF to model a proposed blockchain-IoT architecture to preserve privacy for edge devices (Zhang, Lu, Cheng, Guo, Kang, Zhang, Yuan, and Yan 2021).

d. Big Data

The book *Blockchain, Big Data and Machine Learning* has multiple chapters that delve into the potential of applying blockchain to big data. While chapter 1 (Rahim et al. 2020) introduces both concepts together, chapter 5 outlines use case examples of applying blockchain to big data (Kumar et al. 2020). Kumar et al. (2020) highlight similar benefits as other sources: ensuring trust (in the data), preventing malicious attacks, facilitating real-time data analysis, and data sharing (116–118). N et al. (2021) cite the challenges to making the most of big data and how the assistance of technologies like blockchain can improve big data services.

Altogether, the team's research revealed the degree to which technical experts, industry leaders, academics, and government agencies are exploring blockchain and its benefits. This provided a solid foundation upon which the team could develop their military-specific use cases for blockchain by using a systems engineering approach.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SYSTEMS ENGINEERING APPROACH TO BLOCKCHAIN FOR DOD APPLICATIONS

The DOD recognizes the importance of decision-making in a fast-paced, highly dynamic battle landscape. Leaders will have to navigate the large volume and variety of data that will be coming from the IoBT. While the layering of information onto the more traditional domains of battle is a newer approach to planning, it does not replace the decision-making frameworks that the military has used to date.

The team used systems engineering principles and practices in our evaluation of blockchain applications in the DOD to support decision-making at the strategic, operational, and tactical levels.

A. METHODOLOGY

The team researched the various applications of blockchain, including existing uses within the DOD as well as areas that were ripe for blockchain to solve key problems. The team also performed a stakeholder analysis based on input from the project sponsor, experience from our careers, our organizations' missions, and our research. This stakeholder analysis helped the team to carve out the specific needs for blockchain that this project could address. After the research and the stakeholder analysis, the team explored a variety of potential use cases but settled on three unique use cases that are not only relevant to the DOD but also have Joint applicability.

The team used a systems engineering approach to build out a system architecture that leverages blockchain to solve key problems within each use case. A variety of diagrams illustrate how blockchain would be used. Each use case highlights (and leverages) different strengths of the application of blockchain and reveals potential weaknesses.

1. Stakeholders

Team "Off the Chain" conducted a stakeholder analysis focused on projected interests and beneficiaries of a HLF integration project. The goal of this exercise was to describe not only the primary beneficiaries, but also the second- and third-order stakeholders of the proposed transition across the space. The team assigned roles to each stakeholder ranging from the project's primary sponsor, the Office of Naval Research (ONR), to the software supplier, IBM/Linux foundation, and the various potential users such as data scientists and engineers. The broad application of blockchain and tactical data fabric also required consideration of regulatory influence by the JAIC and Cyber Command. They could likely impact the efforts and progress of all related projects. Table 2 contains the results of the team's stakeholder analysis.

Table 2. Project Stakeholders

Stakeholder	Role	Interest	Benefit to Stakeholder	Impacts to Project
ONR	sponsor	results of academic research	results applicable to mission space	guidance and direction
NPS	academic oversight	supporting students' learning	quality products by students demonstrate relevancy and rigor in their program	
IBM/Linux Foundation	supplier	broader application of their open source platform	improved usage through additional user feedback	support or code improvements
Department of Army/ Navy	executive	needs "smarter adaptive systems which will require data it can trust", protecting national interests, interoperability	improved decision speed	modernization of legacy systems
JAIC	regulator	possible adoption of blockchain	improvement of AI with the integration of blockchain	regulatory actions impeding the adoption of blockchain
Data scientist Data analyst Data engineer	user	develop machine learning models for complex systems and decision-makers	data integrity improved trust	adoption and culture
Operations Research	user	improved war gaming logistics planning	data integrity improved trust	adoption and culture
Intel Community	user	improved collection	data integrity improved trust	adoption and culture

Stakeholder	Role	Interest	Benefit to Stakeholder	Impacts to Project
Defense Industrial Base	user	future collaboration opportunities	data accessibility	adoption and culture
Cyber Command	regulator	may desire another layer of information protection	improved decision speed mitigation of cyber vulnerabilities	
Congress/Politicians		protecting constituents allocating federal funding	way to meet strategic objectives	
Allied Partners		interoperability keeping pace with near peers;	data accessibility	

2. Limitations to This Study

This study was limited by time constraints that made it difficult to implement some of the architectures that we developed. For example, the team wanted to develop a model of the use cases presented in Chapter IV to conduct simulations of these systems' performance with the addition of blockchain. Additionally, the team also wanted to develop some of the chain code for one or more of these use cases in HLF. Unfortunately, time did not allow for either of these activities. However, extending the work that has started with this thesis is a potential area for further research.

B. THE DATA LIFE CYCLE AND DATA PROVENANCE

For the military, strategic, operational, and tactical decisions are three general tiers of the decision-making chain. The typical decision-making process is framed through what is known as the OODA loop; focused on observing, orienting, deciding, and acting. However, as the number of sensors the military relies on to make decisions increases, known as the IoBT or the Internet of Military Things (IoMT), the provenance of information becomes an increasingly difficult task to automate. This could have important implications on the OODA loop if data considered during the observing and orienting steps is unreliable.

1. The Data Life Cycle

There are four general phases to the data life cycle: data creation (or generation), data reading (or consumption), data updating (or modification), and data deletion (or archiving). These four basic operations on data come from a computer programming background and perspective. From Figure 3, one can draw parallels to the data life cycle process from collection (creation), reading and updating (retrieval) and the end of the data usefulness cycle during disposal (deletion or archiving). These phases or operations on data apply to every type of military system. Systems are becoming increasingly data dependent and understanding the provenance across the life cycle of data will assist in providing reference material in areas such as explainable AI. It is important to understand how actors interact with the data at each of these phases of the life cycle, and the implications of those interactions on the data's inherent reliability.

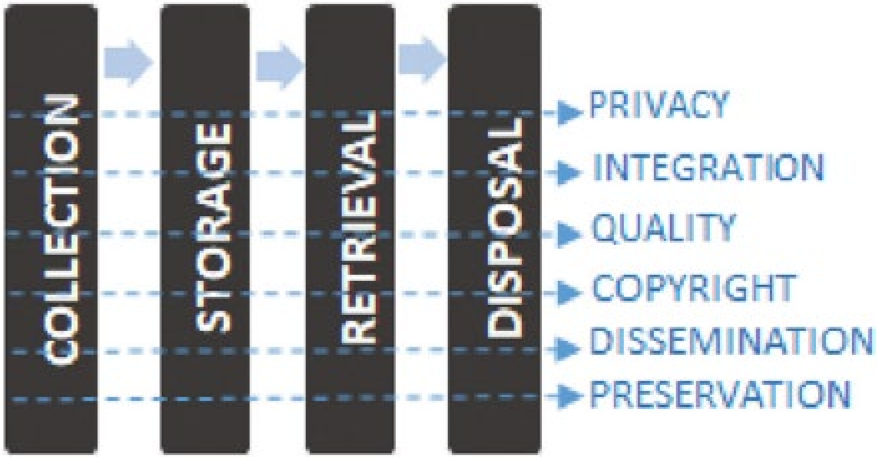


Figure 3. The Data Life Cycle. Source: Fruend, Fagundes, and Macedo (2020).

2. Data Provenance

Fundamentally, the concept of data provenance (or data lineage) should address several questions to ensure trust. This could even be done through an automated verification process. Regardless, data provenance addresses some basic questions that any analyst, soldier, or computer system would need to know to trust data through a verification-first process. The objective of tactical data provenance is to trace the who, what, when, where, why, and how of the data. That is, who produced the data? This can help trace the organization that collects, deploys, or owns the data, as well as create a historical log of who has accessed the data. What data was produced? This can help describe the data with meta descriptions, which can further be used in future query functions to identify if certain kinds of information are available on a network. When was the data produced? This provides a timestamp for when the data was collected or generated, which is an important piece of information to future users regarding the relevancy of data or freshness. Where was the data produced? This can help geolocate the source of information, which may be important for logisticians who need to see how supply data is used from one location to another. Why was the data produced? This can explain data intentions, and if the right data is being collected for the right reasons. How was the data produced? This can define the system/sensor/version to trace performance, or if software changes in a system has caused the data to change.

3. Systems Engineering Processes for Blockchain Applications

The team developed some use-agnostic systems engineering diagrams to illustrate how blockchain can address data provenance and ensure trust in those data. Figure 4 is an asset diagram showing various layers of a system. The assets capture a variety of actors from various users to software systems that would be required, such as data owners and consumers, as well as the data fabric, and the HLF network (i.e., the blockchain component). There are several application programming interfaces (APIs) captured in this diagram: an access API, a “data prov” (short for data provenance) API, and an enterprise API. In this case, the “data prov” API is a gateway to simultaneously deliver appropriate metadata to satisfy a chaincode, which all the nodes within the HLF verify. This API also facilitates delivery of the raw data for storage in the data fabric. On the consumption side of data, an enterprise API allows for querying of data across both the data fabric and the blockchain to confirm the authenticity of data, the historical provenance information, and the raw data. Last, the data provenance API’s function is to transfer data to the data fabric, provide metadata to the blockchain, as well as authenticate the user or IoBT device.

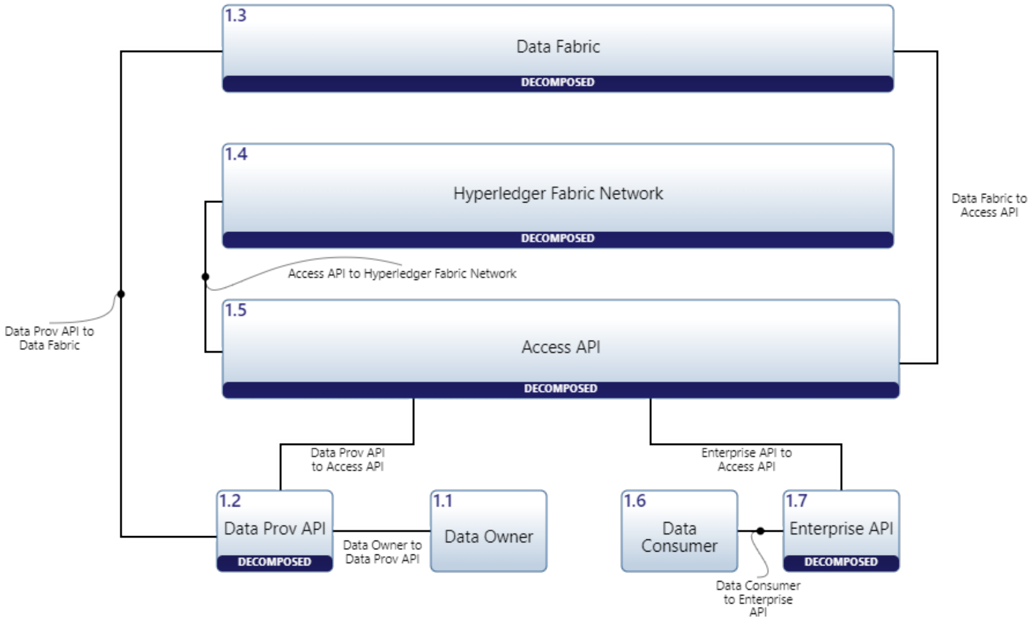

1.3
Data Fabric
DECOMPOSED
1.4
Hyperledger Fabric Network
DECOMPOSED
Data Fabric to Access API
Access API to Hyperledger Fabric Network
Data Prov API to Data Fabric
1.5
Access API
DECOMPOSED
Data Prov API to Access API
Enterprise API to Access API
1.2
Data Prov API
DECOMPOSED
Data Owner to Data Prov API
1.1
Data Owner
1.6
Data Consumer
1.7
Enterprise API
DECOMPOSED
Data Consumer to Enterprise API

Figure 4. Example Asset Diagram

In this asset diagram (Figure 4), while some of the APIs may have similar functions, the way a human or a machine interface with the data fabric or HLF would be slightly different. Humans or machines will generate, measure, or aggregate data. The data fabric serves as storage for data but also provides encryption and is a common point where other organizations can access this information. The details of the data (i.e., metadata, or the answers to each of the provenance questions) are also recorded in the HLF chaincode for each transaction, where it is permanently stored. These transactions can include other time points in the data life cycle beyond the moment of data creation. Additionally, the HLF network collects information that supports the use of smart contracts and conducts consensus. The hashing capability inherent in blockchain also means that a representation of the data can be recorded as a hash, thus enabling a future user to verify that the data is unaltered, increasing data confidence.

In the tree diagram in Figure 5, the assets from Figure 4 are decomposed to show a mixture of both components and actions within this notional system.

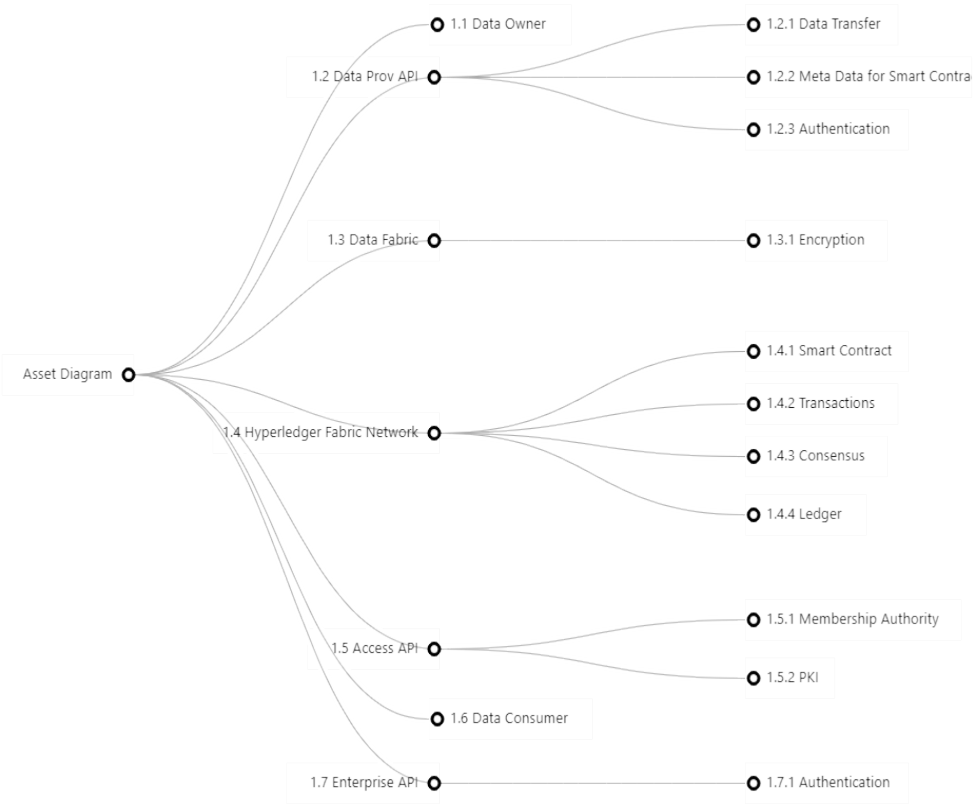


Figure 5. Tree Diagram of Provenance Assets

To illustrate the sequence of actions, Figure 6 steps through the various components and how each would communicate with several aspects of data provenance during the data life cycle of the system. Figure 6 is intended to demonstrate the end-to-end process from data owner (producer) to data consumer.

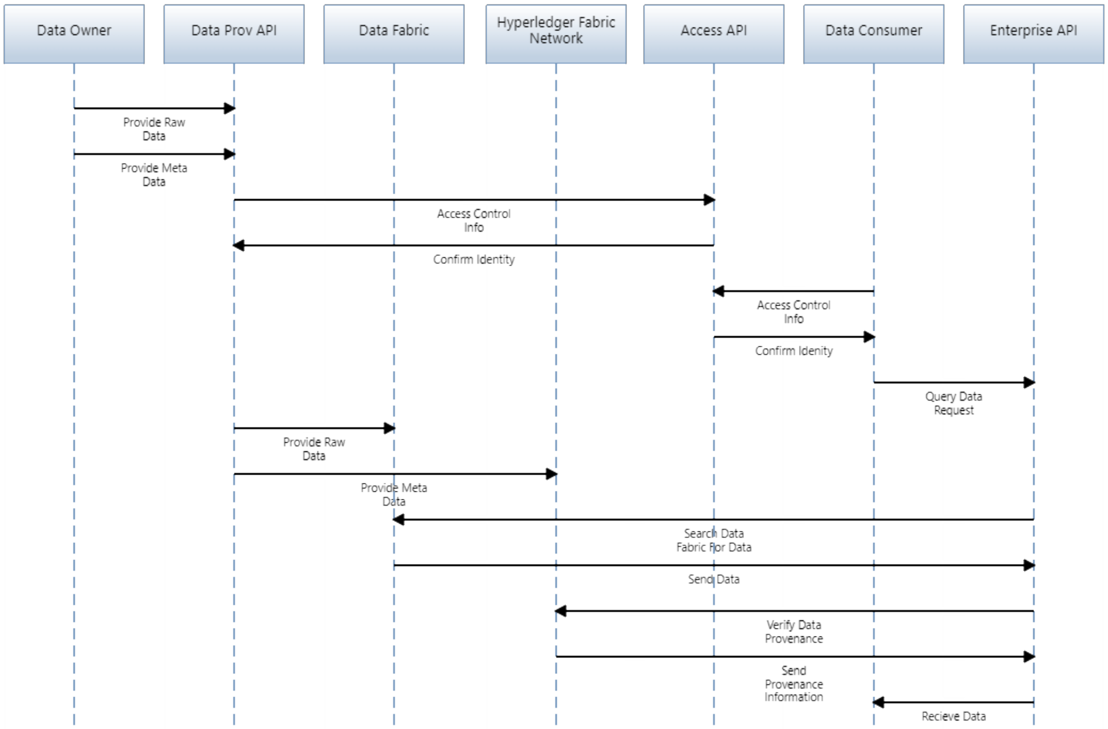


Figure 6. Sequence Diagram of Provenance-Focused Blockchain Application

This process is agnostic of many of these data provenance questions, but can still support the concept of data traceability, data auditability, data verification, or even explainable AI. However, the process would need to be employed at each step of the data life cycle from data generation, data manipulation, data consumption, and data archiving. There are many challenges to achieving these goals. For example, adequate education and understanding involve a cultural shift of the users and training to improve technical skills. There are also challenges with the added computing costs, not to mention challenges with scalability and integration.

The overall focus of utilizing blockchain to provide reliable data provenance is to provide a new method where operators can track devices and editors of data. This allows the inclusion of the timestamp of all operations, the physical location of the data, and a record of every file creation or deletion. Additionally, as the DOD moves towards greater data centricity (as opposed to network centricity), blockchain (and specifically HLF) could facilitate a new, decentralized way to allow analysts to query metadata for sharing and discovery.

C. THE INTERNET OF BATTLEFIELD THINGS

The use of IoBT will impose numerous challenges on an already resource-constrained military communications networks, especially when factoring in cybersecurity and bandwidth limitations in DDIL environments (Kott, Ananthram, and West 2016). According to Kott, Ananthram, and West (2016):

> Communication among things will also be challenged by the IoBT's complexity, dynamics, and scale. Finding, sharing, and managing communication channels among large numbers of competing, heterogeneous, and often unpredictable things will require novel approaches. Highly intelligent automation will be required to continually allocate and reconfigure the communication network's resources. Information-sharing strategies and policies—who talks to whom, when, about what, and for how long—will have to be automatically designed and modified dynamically. Highly scalable architectures and protocols will be necessary, along with rigorous methods to determine and validate their properties. In extreme situations, when the IoBT experiences catastrophic collapse or becomes largely unavailable or untrustworthy as a result of enemy actions, the autonomous management of the IoBT will need to provide a "get me home" capability, which will enable operations to continue, albeit at a limited level of functionality. (72)

Kott, Ananthram, and West (2016) have highlighted several cybersecurity challenges associated with IoBT availability, confidentiality, and integrity. These challenges impede assurance that devices are available as designed, data access is limited to authorized entities, and data remains trustworthy. Blockchain, when combined with the use of a data storage mechanism, is proposed here to aid in the availability, confidentiality, and integrity of IoBT devices and their data.

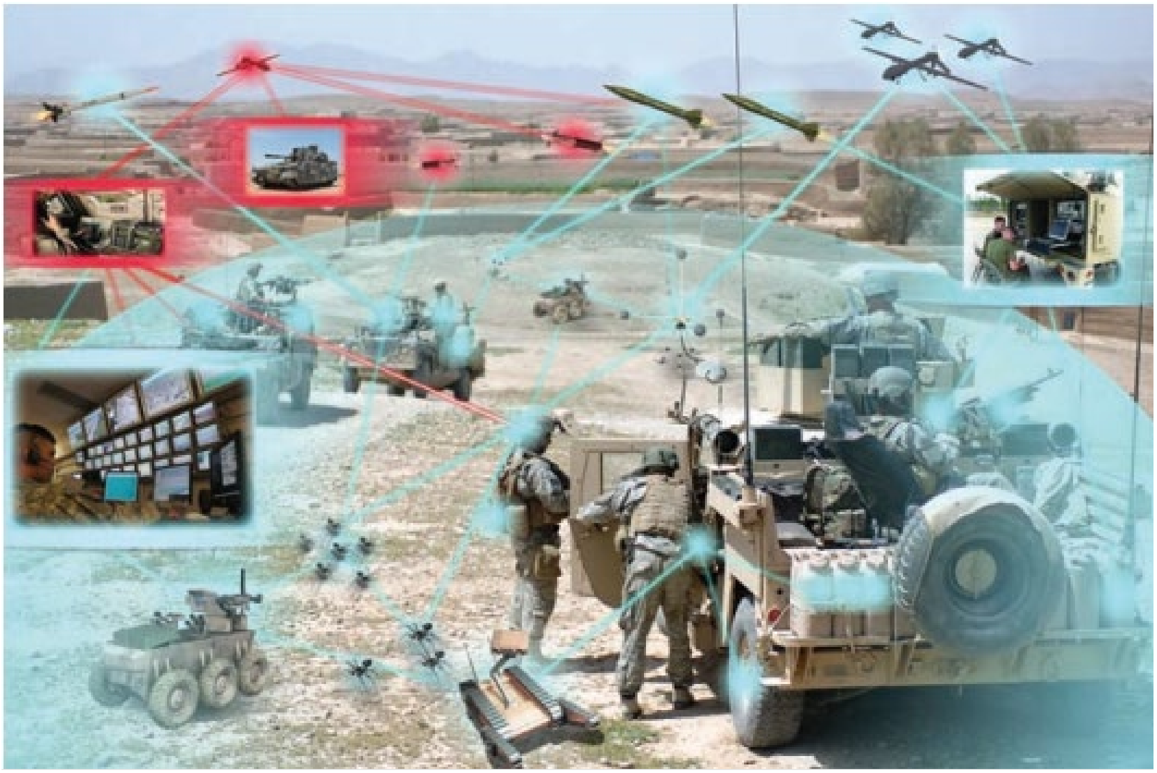


Figure 7. Overview of the Internet of Battlefield Things. Source: Kott, Ananthram, and West (2016), 71.

During the exchange of IoBT device information across the network, blocks created within the blockchain would store metadata associated with the transaction. The underlying blockchain architect can tailor this metadata based on their specific needs (IBM 2022b). However, information related to the condition of the asset providing the data may be a valuable consideration. With respect to IoBT, this condition could be useful when tagging device firmware versions associated with respective data exchange. This could be critical for data validation on items with available (but uninstalled) patches, or for older devices that may no longer be vendor-supported. During the logging of blockchain transactions, information pertaining to the transaction is shared throughout the network. This will validate the creation of the block, as well as the historical information related to that block, before making the record permanent. This historical information is important as we look at data integrity. This validation process is accomplished through various consensus mechanisms, each with unique pros and cons with respect to the speed of transaction validation, the scalability of nodes requiring validation, and how visible these transactions are to users on the network.

D. PERMISSIONED BLOCKCHAINS AND REACHING CONSENSUS WITH HYPERLEDGER FABRIC

The consensus mechanisms available for blockchain are based on the type of blockchain used. For example, there are permissioned or permissionless blockchains. Permissionless blockchains (also referred to as public blockchains) rely on the user's digital resources to support consensus and information exchange with all others on the blockchain network. According to Shetty et al. (2019), these digital resources could be digital money as in the case of proof-of-stake consensus mechanism or computational resources in the case of proof-of-work consensus mechanism. Permissioned blockchains differ in that they are private in nature. An administrator can add or remove participants or this can be done through an external selection process (Shetty et al. 2019). This adds an additional level of security because the participants are pre-selected. Permissioned blockchains can be thought of as centralized in access but decentralized in execution because participant selection is outside the scope of the selected consensus protocol, which make them well-suited to DOD applications. If implemented, use of the DOD's common access cards could determine access into the permissioned blockchain. However, there may be instances in the DOD where certain transactions need to be secured between parties, or more specifically, Service organizations. This is an area where HLF, a specific implementation of a permissioned blockchain, offers benefit. For the purposes of this capstone, HLF was chosen as a candidate platform due to its maturity. IBM is actively developing it and the Linux Foundation is supporting it.

IoBT leverages disparate sensor data to inform a user or system about conditions in a region of interest. As conditions change, the baseline record of data must be updated. However, when using blockchain, consensus is required to make this change. This serves as a "check" on the change to ensure it is valid. Consensus is the process by which new transactions are validated before being added to the ledger (i.e., or creation of a new block) of the blockchain (Hyperledger Architecture Working Group 2017). It is important to be mindful when tailoring a blockchain service—and more specifically, its consensus mechanism, for a resource constrained tactical environment. HLF utilizes permissioned-voting for consensus (Hyperledger Architecture Working Group 2017). Algorithms facilitate this permissioned-voting to reach consensus by requiring nodes to transfer messages to other nodes on the network. Consensus is reached when most of these nodes validate the transaction (IBM 2017).

This method forces a tradeoff between speed and scalability. As the network grows, so do the number of nodes required to reach a majority consensus. Additionally, the increase in nodes also increases network utilization as messages must be shared among greater and greater numbers of nodes. This increased network utilization inherently decreases the speed at which transactions can be completed and reduces network throughput available for other traffic. However, the degree of this impact may vary based on the network links available (wired, satellite, terrestrial) as well as the priority given to a specific device or system on that network.

HLF makes use of different types of nodes, as referenced in Figure 8, each with a unique function. Nodes in a blockchain network are virtual, independent entities that collectively work with other nodes to complete transactions (Hyperledger Performance and Scale Working Group 2018). To further differentiate, peer nodes (also referred to simply as “peers”) are areas in the network architecture where the ledger and smart contracts are hosted (Hyperledger 2022). Peers can be broken down as committing peers, which maintain the ledger and commit transactions; and endorsing peers, which are a specialized type of committing peer that grants or denies endorsement proposals from a transaction (Hyperledger 2022). In addition to peer nodes, ordering nodes execute the ordering service to approve the inclusion of transaction blocks into the ledger through communication with the peer nodes (IBM 2017).

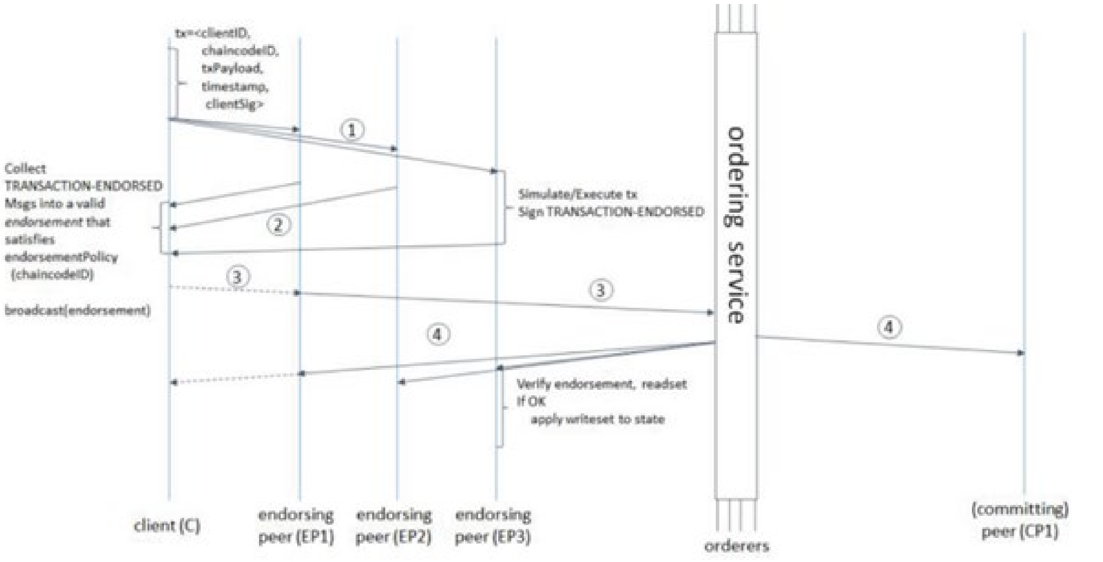


Figure 8. Illustration of One Possible Transaction Flow in Hyperledger Fabric. Source: Hyperledger Architecture Working Group (2017), 8.

The transaction update process begins with a client or application initiating a transaction. This request then goes to the endorsement peer nodes that set the endorsement policy (i.e., who or what must be done to approve the specific transaction). In the DOD, it is possible that this may be done based on data classification type, either by the type of mission the data is supporting (intelligence, fires, etc.), or the parties involved (intra-service, cross-service, partner environment, etc.). Smart contracts manage this endorsement and contain the business logic that defines what makes a transaction valid based on predetermined policies (Hyperledger Architecture Working Group 2017). As a result, policies must be set appropriately to ensure that those users or devices requesting updates are authorized to do so. Within the DOD, this would be where ICAM and zero-trust policies play a large role in the overall network, whether enterprise or tactical. The network must be able to discern a user based on credentials and/or a unique “fingerprint” before it can execute those smart contract policies. It is worth noting that within the U.S. Army there are efforts to bridge the gap between the enterprise and tactical networks that will facilitate this process (U.S. Army 2021).

Once the endorser nodes execute the transaction, they will then confirm what the application intends to write to the blockchain database. The application then pings the ordering nodes that receive transactions from other nodes across the network. This ordering service distributes the next block to all the endorsing and committing peer nodes. These committing peer nodes then validate the transaction against the endorsement policy and, combined with the endorsing nodes, send out a notification to all nodes and the application that the transaction has been added as a block on the blockchain.

E. DATA STORAGE: ON- VS. OFF-CHAIN DATA

Data, whether created manually or automatically via a sensor, can be stored on the blockchain or off the blockchain. Storing information on the blockchain, known as "on-chain data," supports increased security and recoverability of data as the data elements themselves are stored on the immutable and distributed ledger. An example of this is a sensor that collects information over a set period of time, packages that information into a file, and uses the blockchain to store and exchange that file with other parties. This method is limited by file storage sizes and network challenges associated with validating and transferring large files through the blockchain.

By contrast, data can also be stored off the blockchain, commonly referred to as "off-chain data." With this method, files are stored in a separate repository while the metadata associated with these files is stored on the blockchain. Although this limits data recoverability, it reduces the overhead associated with processing data onto the blockchain. Using the example from above, once the sensor packages the information into a file, a record of the transaction is logged onto the blockchain using only the relevant metadata associated with the transaction, but not the data itself. This metadata could include geographic positioning of the sensor, time/date stamp, and security classification. Once the transaction and metadata are logged into the blockchain, the file itself is transferred to the data repository. Additional metadata "stamps" are then logged onto the blockchain as this file is then updated and/or transferred throughout the entire data life cycle.

The team explored the costs and benefits of using on- versus off-chain data storage options in the development of these use cases. This included evaluating the potential use of a tactical data fabric as an "off chain" data storage. There are many architectural approaches like this in this space (including data lakes and data warehouses, among others)

(IBM 2022a). The tactical data fabric was seen as a viable solution due to ongoing research across the DOD to facilitate data access across warfighter functions and mission command systems (Patel et al. 2021). Data fabrics automate the discovery, governance, and consumption of data that enables users to access data when and where they need it, without requiring any knowledge of where the data resides. In recent years, the DOD has explored applying this enterprise capability to the tactical space to improve timely access to data in support of Joint All Domain Command and Control (JADC2). This project explored the potential to improve the performance of tactical data fabrics by overlaying a HLF blockchain to improve the security of data during storage and at point of receipt. Another benefit to this approach is data can be stored by using the HLF exclusively or in conjunction with the tactical data fabric.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. USE CASES FOR DOD BLOCKCHAIN APPLICATIONS

The team used three use cases to explore the potential application of blockchain within the DOD. These use cases provided the foundation upon which a systems engineering approach was applied to understand stakeholder needs, existing systems, system goals, etc. For each use case, the team developed an architecture with corresponding context and sequence diagrams to illustrate how the blockchain application would work in these diverse examples.

A. USE CASE 1: LONG-RANGE FIRES

This first use case applies the IoBT concept to a scenario where separate branches of the military need to securely leverage data from independent systems driven by artificial intelligence. To describe it simply, the U.S. Army has a tactical platform that needs to receive targeting data from a U.S. Air Force intelligence, surveillance, and reconnaissance (ISR) sensor. However, this process is vulnerable to exploitation from the enemy based on the various components required to enable this targeting data transfer. The first component is Long-Range Fires (LRF), the U.S. Army's program to enhance current artillery and missile systems by extending their effective range. There are also the U.S. Air Force ISR sensors, a suite of sensors deployed by manned and unmanned aerial vehicles. The next component is Rainmaker, the U.S. Army's tactical data fabric driven by artificial intelligence and machine learning systems. The last component is the Advanced Battle Management System (ABMS), the U.S. Air Force's tactical data fabric driven by artificial intelligence and machine learning systems.

Two obstacles exist in this scenario. The first obstacle is the inability of the two data fabrics to communicate directly with one another. The second is that the artificial intelligence component(s) is(are) vulnerable to attack. Early attempts to address the direct communication issue required soldiers and airmen to transfer the data manually. In 2019, a Joint exercise conducted by the U.S. Army Rapid Capabilities and Critical Technology Office, the U.S. Air Force Rapid Capabilities Office, and the 101st Airborne Division Artillery successfully used translation software to transfer data from sensor to shooter.

However, solving this first problem led to the identification of vulnerabilities with the artificial intelligence component(s). By removing the human element from a sequence that could result in fatalities, it created an opportunity for exploitation of that process, despite the latest encryption solutions used by the military. The U.S. is committed to the ethical use of artificial intelligence, and this risk put the U.S. in a position where adversaries could exploit a compromised AI system to fire upon unintended targets.

The proposed solution is to leverage a blockchain, specifically the HLF platform, to validate the transactions between the two data fabrics. This not only solves the vulnerability of data transfer but also can be augmented with smart contracts to ensure that the correct, translated data is included in the transaction (Patel et al. 2021). This solves the second problem and ensures the process cannot be compromised by enemy exploitation.

1. Conceptual System Architecture and Design

The activity diagram in Figure 9 depicts the cycle of data without interruptions or vulnerabilities exploited. Data exists independently on a U.S. Air Force data fabric and then on a U.S. Army data fabric. The HLF blockchain component provides the bridge between the two, where each data transfer is a secure transaction that is validated and logged on the blockchain's ledger. This facilitates data transfer without requiring human intervention.

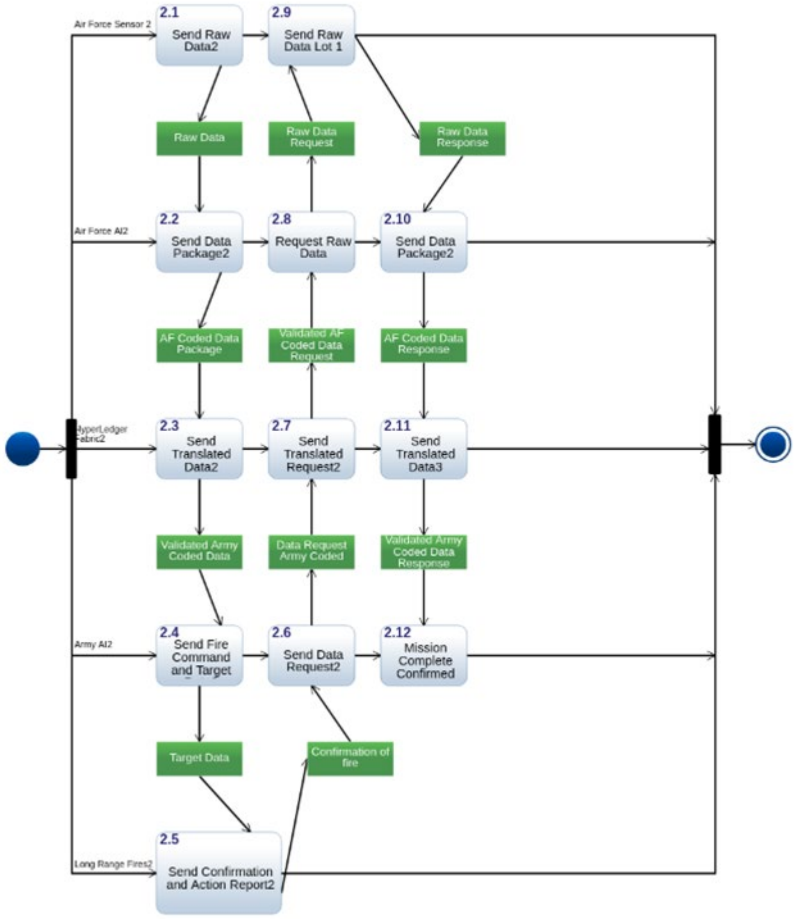


Figure 9. Activity Diagram for Long-Range Fires

2. Context Diagrams and Subsystems

In the context diagram in Figure 10, we show how the HLF blockchain ties two tactical data fabrics together by validating each AI component and allowing the transfer of data. Multiple sensors and LRF components exist on the periphery of the diagram to illustrate how the number of sensors and/or LRF involved in an operation can vary using the same architecture.

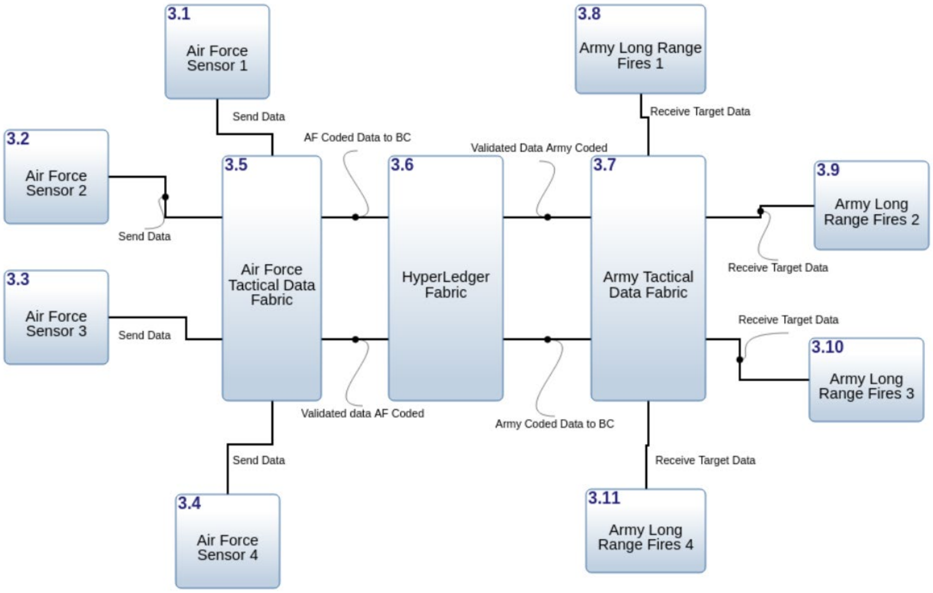


Figure 10. Context Diagram for Long-Range Fires

3. Sequence Diagrams

The sequence diagram shown in Figure 11 lays out this concept from sensor to shooter. The flow of data originates from a sensor (or group of sensors), is packaged by ABMS, and then sent to Rainmaker via the HLF blockchain. Rainmaker is then able to process the data and send out targeting information to LRF. In this sequence, Rainmaker seeks confirmation of a successful strike by sending an updated data request back to ABMS. The flow of sensor data repeats where the collected data is sent from ABMS to Rainmaker via HLF to confirm the successful strike.

Data runs back and forth along this sensor-to-shooter path across two distinct data fabrics driven by AI. The blockchain interface provided by HLF ensures only transactions from validated components are processed and added to the ledger. The AI components are now able to interact securely despite being on two distinct networks and can verify each transaction via the ledger on the blockchain.

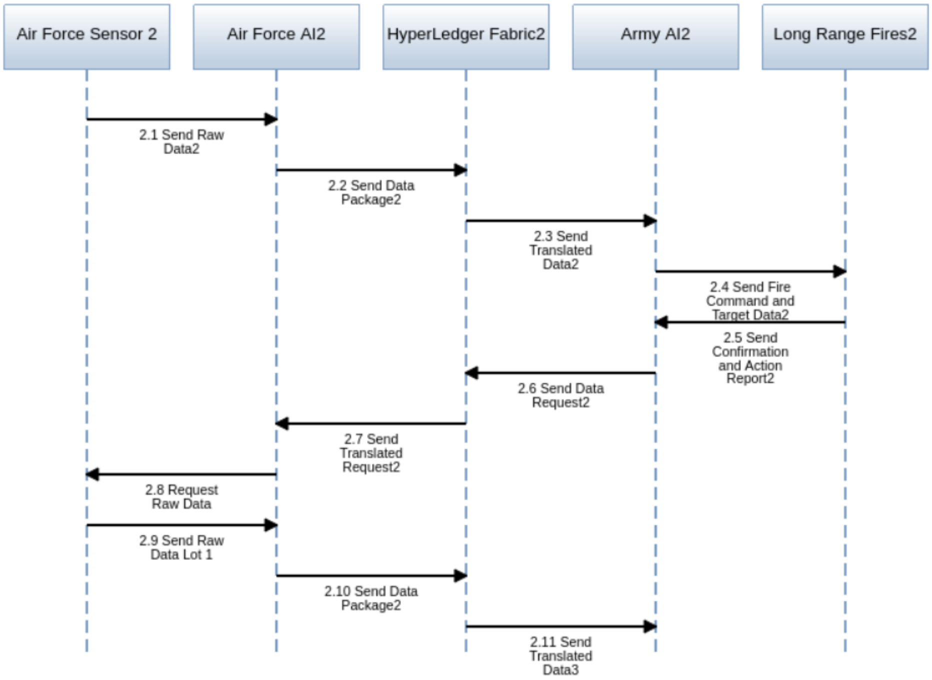


Figure 11. Sequence Diagram for Long-Range Fires

4. The Data Life Cycle for Long-Range Fires

The sequence diagram in Figure 11 also illustrates the four stages of the data life cycle. In the data creation phase, U.S. Air Force ISR sensors generate (or collect) raw data. The frequency of collection and specificity of range may be scheduled or ad hoc to satisfy mission requirements. For the data reading phase, both AI components read the sensor data from within their networks as well as the validated data that comes across the blockchain. The next stage, data updating, occurs within the AI components where data is processed and packaged. For example, the U.S. Air Force AI collects and packages the raw data and converts it to a format that the U.S. Army AI can read. In turn, the U.S. Army AI processes that same data package into targeting information for a LRF strike. The final stage, data deleting/archiving, depends on whether data is written on the blockchain or not. Validated transactions are written to the blockchain ledger where they serve as a record. On the other hand, transactions that fail validation requirements never make it onto the ledger. The originating AI component has the choice of either deleting or archiving the failed data set for further analysis.

5. Architecture Assessment

The architecture proposed above has some strengths and weaknesses. In this architecture, data flow is focused on a sensor-to-shooter path with minimal sensors and shooters displayed. This is because the AI's ability to process data is not in question. We also assumed that one target data package would equate to one transaction on the blockchain to maintain focus on the HLF and not the AI components.

a. Strengths/Weaknesses

One strength of this architecture is that data is contained within two distinct data fabrics, offering redundancy without bogging down transactional bandwidth. The AI-driven data fabrics do all of the analytics and computations while relying on the blockchain to validate user authenticity and data provenance. Considering the prospective size and computing power of the U.S. Army and U.S. Air Force AI components, one could question the scalability of this construct as it is commonly seen as a weakness for blockchain platforms. However, prior testing of HLF v1.4.0 and v1.4.1 displayed capabilities of 13,000 (13K) transactions per second (TPS) as channels were expanded from 1 to 325 being used by up to 128 peers (Ferris 2019) Assumptions can be made as to whether or not 13K TPS will suffice in a full-scale tactical scenario, but in reality, it will be the Services that need to make that determination.

b. Alternate Architectures

The primary focus of the LRF use case was the utilization of HLF to enable secure transactions between two major systems. An alternative approach would be to use HLF to validate every transaction in the sequence. An alternative sequence diagram (Figure 12) illustrates this alternative architecture. A single sensor and LRF component are shown to depict the path of sensor data, but it is important to understand that data from multiple sensors will, often, be compiled and processed to produce a targeting data package.

The primary benefit of this alternative architecture is the creation of a decentralized system securing every transaction between increased numbers of nodes on a blockchain. The increased security directly affects the integrity of all AI components by reducing vulnerability during data transfers. On the other hand, the increase in nodes magnifies the system's vulnerability to certain nefarious acts, such as denial of service attacks, where nodes are overwhelmed with transactions making them inoperable. The full integration of a HLF blockchain across two distinct systems is not without its challenges, but the scalability and use of smart contracts through the chaincode can make it possible.

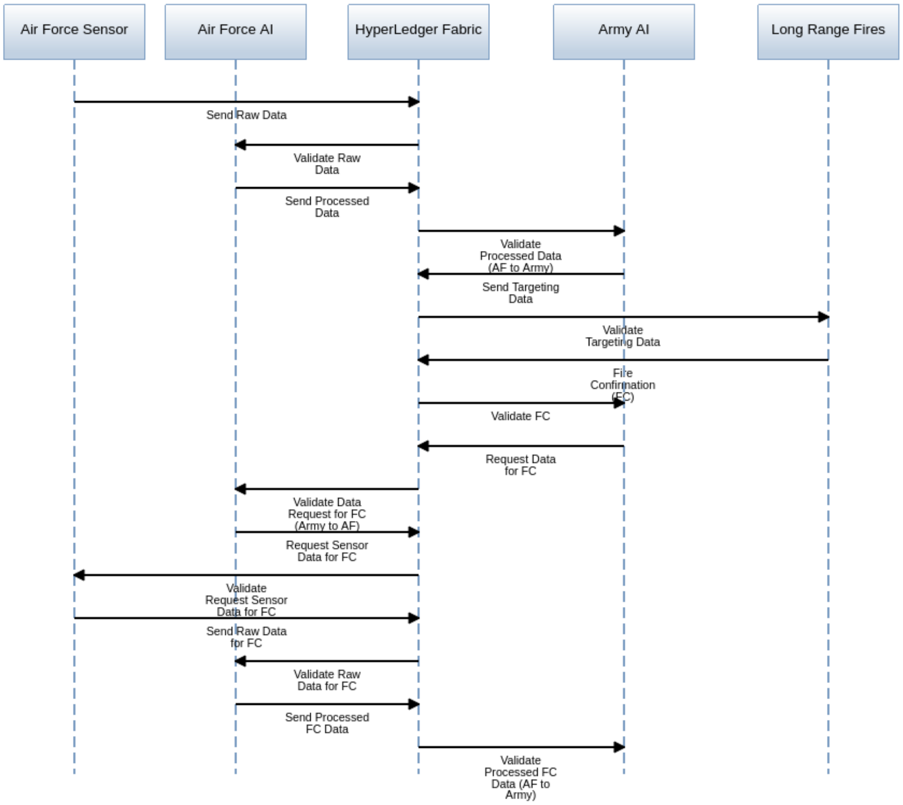


Figure 12. Alternative Sequence Diagram for Long-Range Fires

B. USE CASE 2: MEDICAL DATA AND THE ELECTRONIC HEALTH RECORD

Much like there is an IoBT, there is also an Internet of Medical Things (IoMT). It is, in essence, a subset of the IoT that is focused on healthcare services. Guntur, Gorrepati, and Dirisala (2019) describe it as "physical devices and smart systems (that) are transmitting essential information in real time enabling specialists, healthcare providers and patients to interface in new ways and recognize life-threatening situations" (272).

Virgos et al. (2021) also note that the IoMT establishes a framework to integrate and manage a variety of these medical things. This also leads to significant amounts of data, which can lead to better diagnoses of disease, and even better prediction and prevention. The same way the IoT supports and contributes to big data in a broader sense, the same is true of the IoMT. Elezabeth and Mishra (2019) put it perhaps best, that "(t)this medical big data is stored not simply for the sake of storing, but contains valuable information, which if and when analyzed and methodized properly, can aid in understanding the 'concepts' of illness and health and thus bring about major breakthroughs in the medical field, especially in the areas of disease diagnosis and prevention" (2).

The IoMT and medical big data face the same inherent challenges that the Team's research revealed with the IoT and big data (in general). Security is of paramount concern (Virgos et al. 2021), even more so because of the Health Insurance Portability and Accountability Act (HIPAA) in the United States (Elezabeth and Mishra 2019). In addition, there are the familiar concerns of data storage and transmission, but also issues such as unstructured, and unstandardized data. Blockchain also has the potential to solve—or at least mitigate—some of these challenges in a medical context, just like in a more general context. While there are multiple ways in which blockchain could be applied to the IoMT and medical big data, there is one application of relevance to the DOD—the EHR. Elezabeth and Mishra (2019) describe the importance of the EHR and the vast information it contains such as "clinical history, lab reports and other relevant statistics among others" (11). These patient records (and medical big data, overall) can be stored in highly centralized systems (Elezabeth and Mishra 2019, 16) that are vulnerable to attack or in cloud-based platforms that can (in essence) outsource ownership of those records (Cao et al. 2019). Even in centralized systems, large healthcare networks may still require that distributed medical facilities and medical providers access and append their patients' EHR. To prevent manipulation of these records and ensure data integrity within the EHRs, Cao et al. (2019) propose blockchain as a way to ensure that every time a doctor creates an EHR (this would also apply to every time the EHR is appended), a transaction is logged on the blockchain.

The Military Health System (MHS) has also implemented an EHR system called MHS Genesis (MHS 2022). The system is still being rolled out across the many hospitals and clinics that are a part of the MHS but does not capture patient data from within theater in real (or even near real) time. In separate efforts, the DOD is also investing in sensor technologies that would provide a variety of health insights on service members. These sensors could provide squad or platoon leaders (and even commanders) with data on their troops' stress and fatigue levels during training or other missions. This could help prevent heat casualties, inform appropriate work/rest cycles, and give insight into other human performance factors. These leaders may have access to this aggregated sensor data on a smart device and/or through a command-and-control interface or dashboard.

In addition to this scenario of individual sensor data, there is a desire to improve information sharing within theater during the evacuation process. For example, if a brigade area support company (e.g., a "Charlie Med") or field hospital not only knew how many patients were being evacuated to them but could access information about their injuries and even see their vital signs during the transport—before they arrive—it would enable them to prepare for those patients' arrivals in a way that is not possible now. These advancements will greatly increase/improve the amount of information they have available to them when providing care to patients—both for combat casualties but also in instances of disease and non-battle injuries. In addition, the MHS would likely provide care to service members (and their families) not just during their service, but also after separation or retirement through to the VA system. MHS Genesis supported by blockchain could help provide continuity for their health records throughout that span of care.

Blockchain has the potential to not only improve the security and data integrity of the MHS Genesis EHR as its used in hospitals and clinics across the DOD, but it also has the potential to facilitate the inclusion of EHR data for care provided in a combat theater. In this use case, the team explores how blockchain can provide an audit trail for every time a service member's EHR is touched—both in theater and at non-deployment locations. The terminology of blockchain often uses "transaction" to describe events that are logged in the ledger. In this use case, these events or "transactions" will include any touchpoint with a patient's EHR—whether it is to retrieve (i.e., view), add to, or even edit data in the record.

By doing this, the blockchain creates an immutable record of each event as a block on the chain. In this proposed architecture, the blockchain platform would not be used to store all medical data, but rather the metadata of each of these events. However, to protect against certain types of tampering, these metadata could include medical data such as tests ordered, test results, diagnoses, medications prescribed.

In addition to preventing tampering and unauthorized access to the information internally, and ensuring with HIPAA, it also prevents enemy access. This is of paramount importance when appending data from theater to the EHR. Aggregated information on the numbers of casualties (including the number of fatalities), or even illness or injury patterns, can provide the enemy with insight on whether their offensive tactics are effective and to what degree.

As mentioned earlier in this use case, the IoMT and medical big data enable the use of AI/ML to support greater insight into the injuries and diseases experienced by Service Members, and lead to improved diagnostics and prevention measures. Having the EHRs of the larger military population would support improved research on conditions that may be unique to military service members, as well as identifying new treatments and improved standards of care. By having the EHR supported by a blockchain platform, it ensures data integrity but also can facilitate patient confidentiality for any research and analysis.

1. Conceptual System Architecture and Design

As mentioned above, blockchain is a distributed ledger at its core. In the same way that a product (and its movement through a supply chain) is the primary focus of a blockchain-based supply chain, the patient (and their healthcare) is the primary focus of a blockchain-based EHR. Because of this, the EHR is central to this proposed architecture. Based on the team's research combined with the DOD's interest in HLF as a possible blockchain platform, HLF was also chosen as the likely blockchain platform for the blockchain-based EHR.

The architecture in Figure 13 includes wearables sensors (worn by the patient), smart devices that provide aggregated squad (or other level) information for commanders in the field, as well as the medical providers who are providing treatment and recording their notes in the EHR. The HLF supports the EHR by generating the audit trail of every event on the EHR in real-time. While not specifically called out in this diagram, the architecture could include other devices within the IoMT, including lab results off of internet-connected lab equipment, images off of x-ray or CT scans, pharmacy data (e.g., prescriptions filled), appointment information/history, and so on.

In this architecture, the totality of medical data is not stored on the blockchain. In other words, the blockchain does not become the EHR, but rather supports the EHR. The key purpose and function of the blockchain is to record every time the EHR is "touched" in some way—whether by a person or a device in the IoMT, thus providing an audit trail.

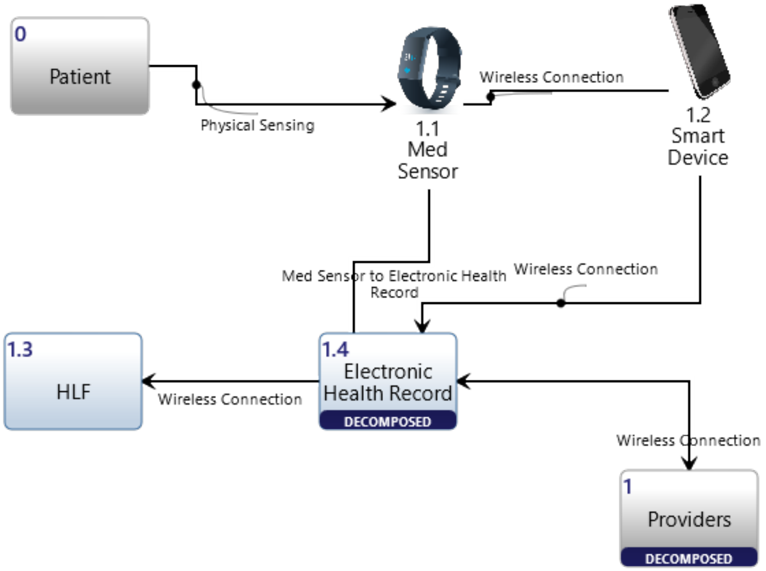


Figure 13. Asset Diagram of Blockchain-Supported EHR System

2. Assets, Actors, and Definitions

In this use case, the team has generalized some terms to distill this use case down to its essential components to facilitate straightforward diagrams. As such, it is worthwhile to provide some definitions to show the breadth and depth of this potential use case.

Because this is a military use case, in this context a *patient* is a service member who receives healthcare services from the MHS. While this use case could also apply to family members who are cared for by the MHS, (without the in-theater portion of the architecture), our discussion will focus on service members. That said, this use case spans the entire timeframe of their military career—from the moment they enter the service through their separation and even transfer to care under the Veterans Administration, as applicable. This includes any/all instances when that service member may have an interaction with the MHS, such as during training events, deployments, routine medical appointments, etc.

Throughout these service members' military careers, medical *providers* will render care to this population of patients. The term providers here can cover everything from medics to nurses, physicians' assistants, nurse practitioners, doctors, surgeons, specialists, etc. These providers will render care throughout the care continuum, from the field all the way to the large hospitals on military installations, and everything in between.

The EHR will also include a wide variety of data. This can include data taken directly off any *medical sensors* or other smart devices that collect continuous data. *Devices*, as identified in Figure 14, can also include other pieces of equipment within a hospital, clinic, or aid station that generates data on a patient, such as lab results, images, or other readings. In addition, appointment histories with provider notes and observations, diagnoses and prognoses, prescriptions, procedures, and family history would all be included within the EHR.

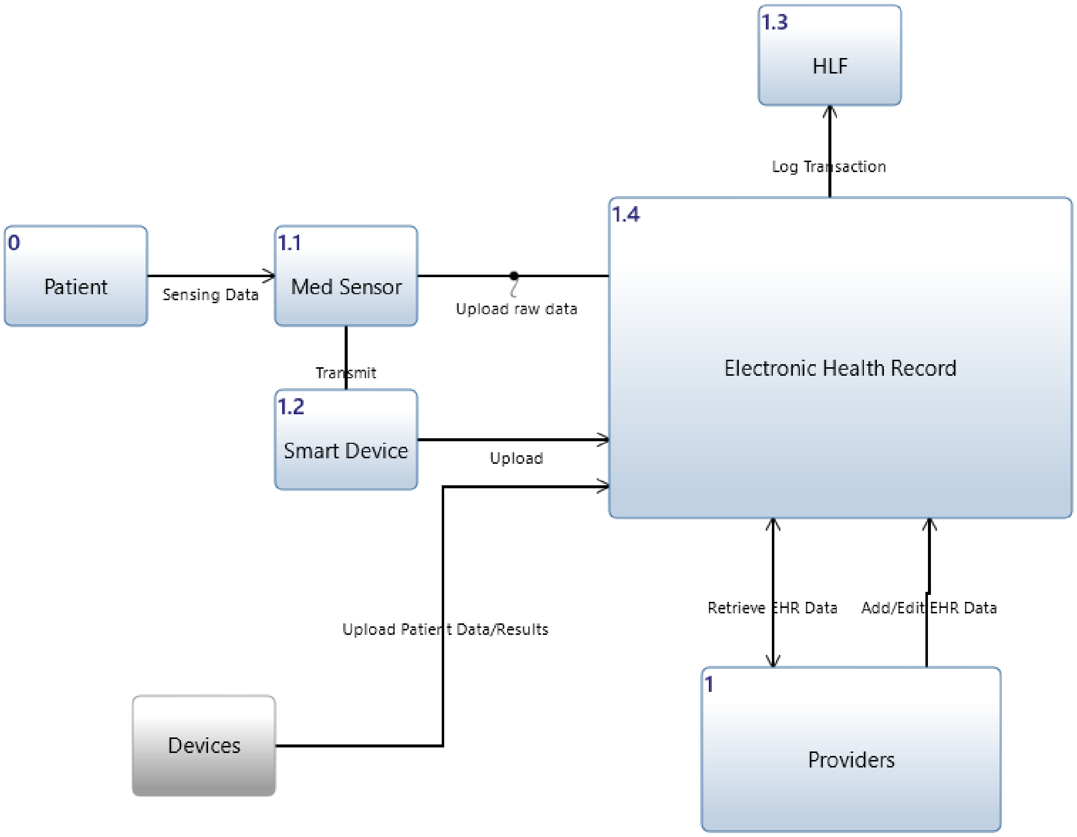


Figure 14. Blockchain-Supported EHR Inputs and Outputs

3. Sequence Diagram

The sequence diagram in Figure 15 shows the data moving from a far-forward environment, from a med sensor to a smart device (perhaps as part of a commander's dashboard), but also directly to the EHR. That touchpoint, or event, is recorded in the blockchain ledger. In addition, anytime a service member is seen by a provider or has some sort of test or scan done, each of these events and the relevant details are appended in the EHR and the event is recorded on the blockchain. Through this sequence, regardless of how or where the event is initiated, the EHR is updated and the blockchain creates the audit trail.

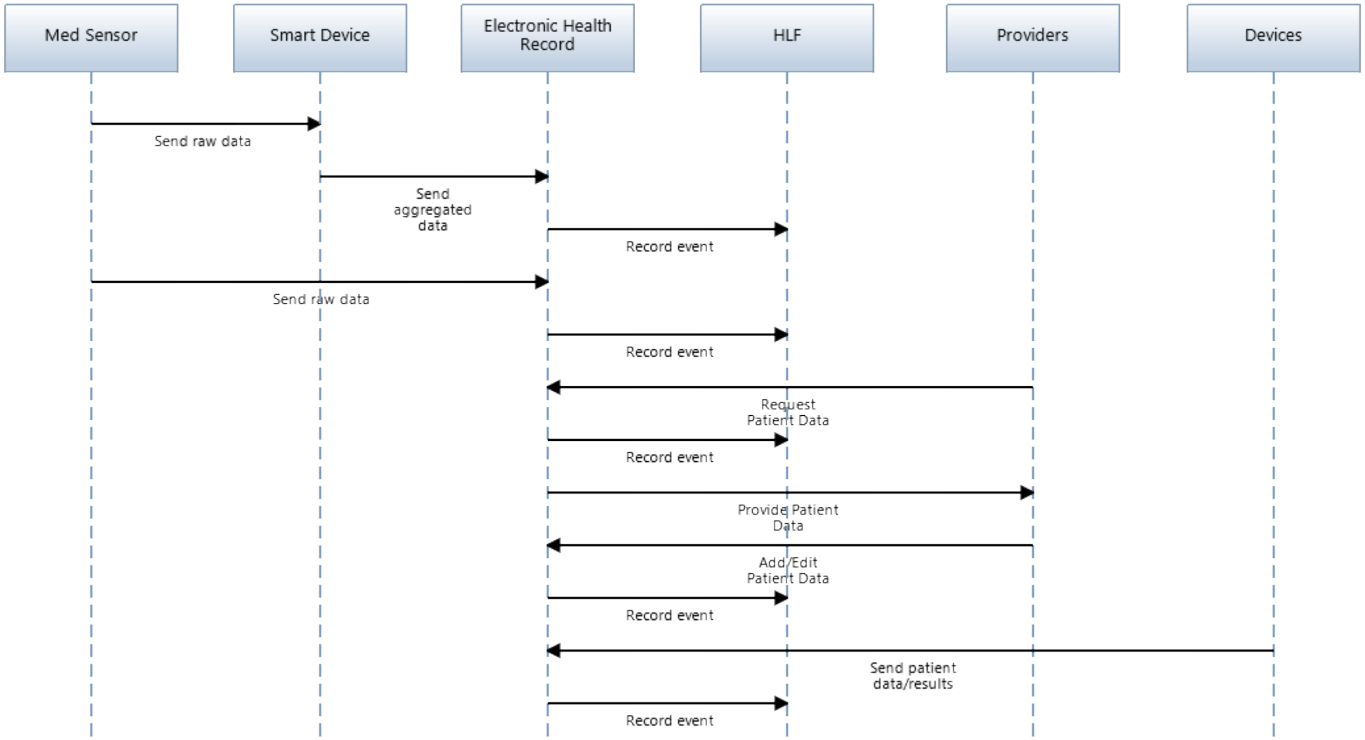


Figure 15. Sequence Diagram for Blockchain-Supported EHR

4. The Data Life Cycle for Medical Data

This use case demonstrates all four stages of the data life cycle. The “creating” of data happens anytime new data that is appended to the EHR. This happens all along the continuum of care, from a wearable sensor to a visit to the clinic, a prescription being filled, or a surgical procedure. The “reading” of data occurs whenever providers (or even the service member themselves) need to access the patient’s EHR record. Providers will do this routinely to review the patient’s medical history when rendering care; patients may do this in the management of their healthcare. The “updating” stage would occur every time a result from a test becomes available, updating the original order of the test with those results. A provider may also need to adjust a treatment protocol, cancel a test order, cancel a prescription, or annotate another similar update. It is also possible that mistakes could be made as providers enter their notes in the EHR, which if caught later, need to be corrected. This would also count as an “updating” phase event. Last, the “deleting” phase would occur as medical records are ultimately archived. The DOD has policies to keep certain types of medical data on record for as much as 90 years, and an appropriate arching strategy may allow that data to be preserved correctly. Additionally, when a service member passes away or leaves the Service (without continued medical benefits), that archiving strategy would help preserve their data while taking it out of the active EHR database. The archiving strategy could also support research goals such as longitudinal, retrospective, and cohort studies. Last, because of the audit trail that the blockchain facilitates, it would provide an easy way to locate those archived records should they need to be retrieved in the future.

5. Architecture Assessment

The architecture proposed above has some strengths and weaknesses. It is purposefully simple to facilitate systems engineering diagrams that are universal and not unnecessarily complex. However, medical data is highly heterogeneous and unstructured. The addition of wearable medical sensors also means nearly continuous data generation on a service member. The simplified model might belie the complexity of implementing this use case.

a. Strengths/Weaknesses

One strength of this architecture is that it supports the collection of medical data into the EHR regardless of where the service member is located. This is a limitation of the current system, which the use of blockchain could resolve. It also maximizes the utility of AI/ML tools by providing greater amounts of medical data, with the assurance that it is reliable data based on the blockchain audit trail. The insights derived from the AI/ML analysis can help improve patient care through improved standards of care and patient administration policies. It is also possible that this architecture could help reduce omissions in the patient's EHR data.

However, this architecture assumes a consistent and secure connection to the network that allows the data to be transferred and the blockchain ledger to be appended. It does not address how this would work in situations with compromised or non-existent communications. It may be possible that the blockchain could facilitate transmission of the data over networks that are otherwise unsecure, due to blockchain's hashing function. In addition, the architecture also does not address if sufficient computing power is available at the edge (e.g., at the wearable sensors, or smart device nodes) to enable continuous updates to the blockchain. There could also be additional layers within this architecture that are needed to ensure regulatory compliance for handling patient information and other personally identifiable information.

b. Alternate Architectures

This architecture is merely a starting point for this use case, and other architectures should be considered. This simple architecture could be extended to include the VA and a more diverse base of IoMT, such as patient monitors used at home. A framework for the metadata included on the blockchain could also demonstrate what implementation might look like. Additionally, this architecture utilizes off-chain data storage. An architecture where all the data is stored on the blockchain may provide benefits over the current architecture.

There are even applications for blockchain in a medical context beyond the EHR. These are not either/or choices but could be implemented in concert with one another. For example, blockchain could be used to track the manufacture, distribution and dispensing of pharmaceuticals, as described by Rayan and Tsagkaris (2021). This would prevent counterfeit drugs from entering the system, and help keep patients' EHRs up to date with the medications they are taking over time. There are also applications of blockchain to improve clinical trials, or to support the development of personalized pharmaceuticals based on a patient's genomic information (Rayan and Tsagkaris 2021). These blockchain applications could be used in conjunction with one another to create a broader medical blockchain universe that works together to support many dimensions of healthcare.

C. USE CASE 3: SENSORS AND MASINT TO SUPPORT CHEMICAL DEFENSE ACTIVITIES

Measurement and signature intelligence (MASINT) utilizes information aggregated from different types of sensors and then analyzed to detect signals of interest against a background or baseline. MASINT is essentially a set of specialized sensors that are used to identify certain characteristics of a source, emitter, or sender (Pre-Employment Checks 2019). MASINT-based systems are used in various roles that can range from detection of intruders, strategic missile launch cautionary, nuclear weapons test monitoring and even chemical defense (Pike 2020). Collecting this kind of intelligence is extremely important in detecting, tracking, and identifying chemical targets (Pre-Employment Checks 2019) to determine the location they are coming from, and perhaps more significantly, the direction they are moving towards.

In this use case, the team envisioned how blockchain can support data provenance from sensors used in chemical weapons detection. This simplified model incorporates three chemical sensors collecting the same information from different, but nearby locations, and sends the data they generate to a MASINT AI system. Each time this happens, the metadata for each data push is recorded as a transaction on the blockchain, in addition to the raw data being digested by the AI system. This is similar to how HLF was utilized in the first use case. Because there are no humans-in-the-loop in this part of the process, the team's proposed architecture incorporates the use of a smart contract to pre-process the data, identify when a reportable event may have occurred, and initially flag those data when they are pushed to the MASINT AI system. In this architecture with three sensors, a simple example might be if one of the three sensors records a positive detection. While this could be an instance of a sensor going bad, or an erroneous measurement (i.e., a false positive), it could also be a true positive. By pre-processing instances where one or more sensors has a positive detection, it enables the AI to alert a live analyst to an event that requires further investigation. This helps maximize use of limited human resources, without impeding the AI system's ability to continuously characterize the data it receives. This would also help support the OODA loop of decision-making in instances where a situation needs to be elevated and/or acted upon.

1. Conceptual System Architecture and Design

In this use case, the MASINT AI system is the primary component. It could be considered the "center of the universe" for this system. As the chemical sensors generate data and push that data to the MASINT AI, the blockchain records these events using the metadata from the data pushes. These metadata could include sensor name, geographical location, date/time stamp of the data generation, and any other pertinent information about the sensor. This provides data provenance and supports trust in the data, such that reportable events can be handled appropriately, and time is not wasted to verify the sensor or the data after the event has been flagged.

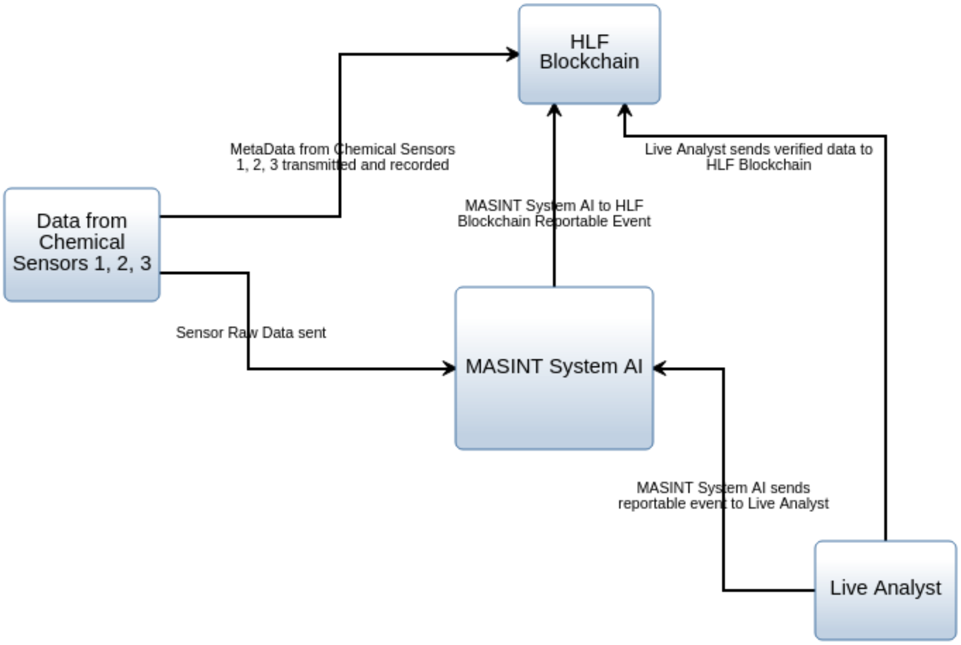

HLF Blockchain
MetaData from Chemical Sensors 1, 2, 3 transmitted and recorded
Live Analyst sends verified data to HLF Blockchain
Data from Chemical Sensors 1, 2, 3
MASINT System AI to HLF Blockchain Reportable Event
Sensor Raw Data sent
MASINT System AI
MASINT System AI sends reportable event to Live Analyst
Live Analyst

Figure 16. MASINT AI and Chemical Sensor Context Diagrams

2. Sequence Diagrams

The sequence diagram in Figure 17 represents the process that this simplified model has used. That said, it illustrates how this architecture could support more complex, real-world scenarios. If any of the sensors provide a positive result, it satisfies the conditions of the smart contract and triggers a reportable event. If all the sensors provide a negative result, then the smart contract is not satisfied, and no action is needed as the technology would recognize no inconsistencies are happening. This sequence shows the data moving from a chemical sensor to the blockchain where the metadata from those sensors' data are recorded. The raw data goes directly to the MASINT AI system to be verified against other sensor data. If the smart contract activates a reportable event, the MASINT AI system records that in the blockchain ledger at the same time that it notifies an analyst of the event. Through this process the blockchain provides an audit trail of how the data is moving through the system.

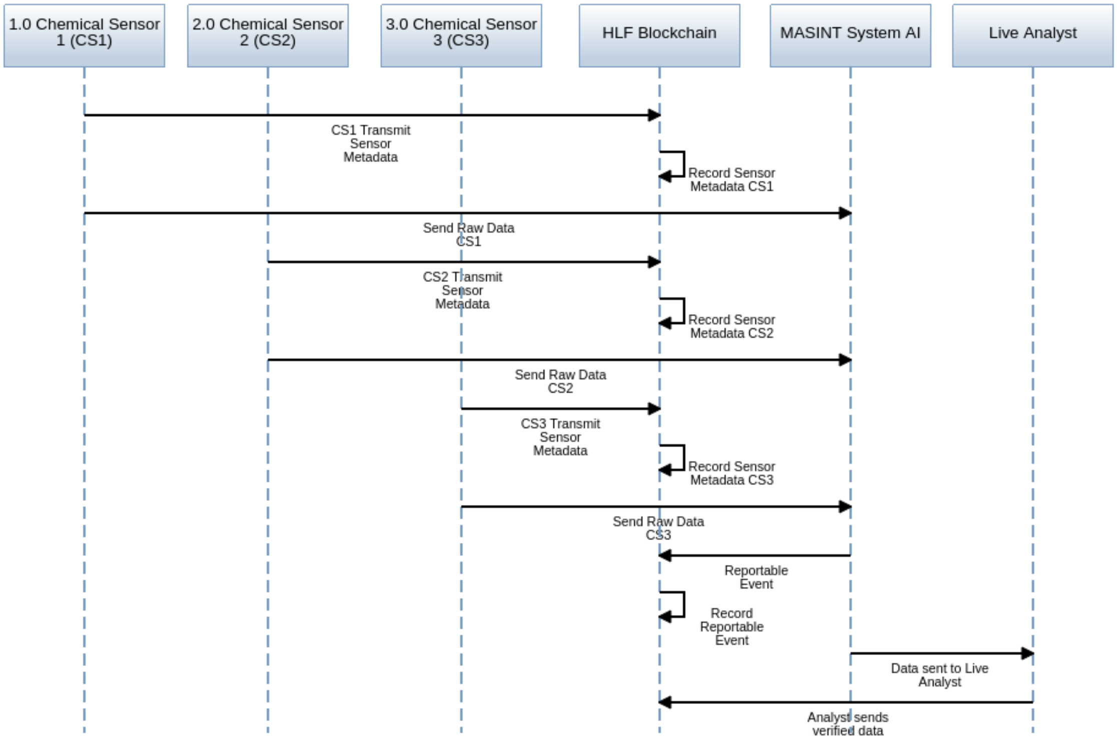

1.0 Chemical Sensor 1 (CS1)
2.0 Chemical Sensor 2 (CS2)
3.0 Chemical Sensor 3 (CS3)
HLF Blockchain
MASINT System AI
Live Analyst
CS1 Transmit Sensor Metadata
Record Sensor Metadata CS1
Send Raw Data CS1
CS2 Transmit Sensor Metadata
Record Sensor Metadata CS2
Send Raw Data CS2
CS3 Transmit Sensor Metadata
Record Sensor Metadata CS3
Send Raw Data CS3
Reportable Event
Record Reportable Event
Data sent to Live Analyst
Analyst sends verified data

Figure 17. Sequence Diagram for MASINT Use Case

3. The Data Life Cycle for Sensor Data in Chemical Defense

This use case also reflects the phases of the data life cycle. Data creation occurs as raw data is generated/collected by the chemical sensors (CS 1, 2, 3). The frequency of collection would be determined by the requirements of the mission. The data reading phase is represented both by the MASINT AI's analysis of the data as well as the analyst's investigation of reportable events. With regards to data updating, this can occur after the live analyst has investigated reportable events, and perhaps tags the positive results as either false or real. For the final phase, data deleting, this can occur as data is archived in a dedicated archival location.

4. Architecture Assessment

The architecture proposed above has some strengths and weaknesses. In this architecture, the data from these sensors are focused on identifying specific parameters set in advance. For example, types of chemical compositions. The application of blockchain technology helps provide data provenance and gives data consumers' confidence in the trustworthiness of the sensor data. This architecture stores the data off the chain.

a. Strengths/Weaknesses

Strengths include a reduction in computing power and space by housing the data in a repository off the chain. The blockchain ensures that the data is reliable and maintained to a certain standard. Data stored off-chain has added security because it is not limited in the same way a typical on-chain transaction might be.

Weaknesses include not having the actual data on the chain for quick access.

b. Alternate Architectures

Data for this use case is stored currently off the chain. An alternate architecture would be to store the data on the chain. However, this could pose issues as far as capacity to store the data and computing power to keep that data stored on the chain.

D. COMPARISON OF USE CASES

The team has presented three distinct, yet similar use cases in that the benefit of integrating HLF into to each system is increased trust and data provenance. In a data centric environment, whether it be for targeting, soldier health or threat detection, trust equates to speed and speed can save lives. The LRF and MASINT cases both rely heavily on AI components for data processing, but the data that is processed must first be from a validated source and then satisfy the requirements of a smart contract to be deemed acceptable. The MHS case, although not as AI dependent, also shows the benefits of trusted data and security regarding soldier health records updated from data provided by sensors and devices. All three use cases involve systems relying on sensors for some or all the data. Side by side comparisons of the conceptual system architectures and sequence diagrams show consistency in data flow with HLF serving as an amendment to the system.

The differences identified in these use cases are mainly based on the type of data being moved. The breadth of applications within these three use cases speaks to the possible benefits of integrating HLF within AI sensor-driven systems. The data within these three examples, although unique in terms of formatting and size, still behave within the norms of the data life cycle. Strengths identified for all three are parallel in that AI/ML utility is maximized and overall system integrity is increased. Conversely, weaknesses identified in this report include questions of scalability and the ability to leverage unsecure networks reliably in hostile zones. Research behind these two topics is ongoing as they are novel issues across the blockchain space.

V. CONCLUSION

The future battlefield will be the most technologically advanced ever seen, with decision makers at all levels grappling with a tremendous amount of data and information. Recent updates to the DOD's strategy documents reflect this future and a desire to be ready to fight and win in that environment. To achieve this, the DOD must explore cutting edge tools to deftly leverage the vast amounts of data being generated for success. Blockchain is one of those new tools that could solve several of the challenges of conventional methods of generating, storing, and transferring data.

In this capstone report, the team captures the background forces and current problems that are driving the need to evaluate blockchain's utility for the DOD. Our report includes a literature review of the body of existing work that helped to inform the capstone project and shape the development of both the generic models as well as specific use cases. An overview of our findings and results, as well as future areas of research are captured in this chapter.

A. SUMMARY OF FINDINGS AND RESULTS

The team evaluated the DOD's potential use of blockchain using a systems-engineering approach. This evaluation was extended through the development of three unique use cases within a military context. In the first use case, we explored how blockchain can facilitate secure and trustworthy data transfer at the tactical edge to utilize long-range fires. The second use case provided an operational example, where blockchain provides an audit trail to enable a robust EHR that is accessible at any point in the continuum of healthcare delivery. Last, the team's third use case looked at managing the flow of data coming off sensors in the field that feed into AI models to support specific types of intelligence (e.g., MASINT for chemical defense efforts). This use case has both operational as well as strategic contexts and demonstrates how blockchain ensures that data fed into AI models is valid and reliable.

While these use cases utilized a simplified architecture to facilitate notional applications of blockchain, it nevertheless demonstrated the real potential of this technology to solve or at least mitigate both current and future challenges of managing and protecting vast amounts of data. The team was also able to explore the options of storing data both on and off the blockchain. The fact that these options exist for implementing blockchain demonstrates the degree to which the technology can be tailored to specific circumstances—not just across strategic, operational, and tactical contexts, but also across the Services to meet their unique mission needs. The Joint Force of the future will need to be savvy in its generation and consumption of data—data that will be imperative to securing an advantage on the battlefield but is also critical during peaceful yet competitive periods between armed conflict.

B. FUTURE AREAS OF RESEARCH

There are many obstacles and challenges to implementing blockchain technology within the DOD. From a management perspective, adequate training and education on the benefits that blockchain networks and decentralized distributed ledger technology can bring to current and future systems will be important. From a technical standpoint, the DOD community would benefit from rigorous modeling and simulation to understand the computing requirements, scalability, safety, and vulnerabilities from a cyber-perspective. As military systems become increasingly digital, the adoption of a blockchain network will organically bring these complex systems together across the Services, units, soldiers, and civilians.

Beyond modeling and simulation, future work that performs comparisons and virtual demonstrations of an HLF network or other blockchain platforms is needed to test and verify if/how the network can effectively provide the functions and behaviors we describe. This future research would help address questions regarding the degree of scalability that is possible with blockchain technology in DOD contexts. The communication and information hurdles that DDIL environments present cannot be overlooked, and the ability to recover data uplinks to the blockchain if that link is broken also needs to be examined and understood. As with most new technology, significant experimentation that balances the changing needs of stakeholders and DOD requirements to modernize is still required.

LIST OF REFERENCES

Abdelmaboud, Abdelzahir, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Abaker, Taiseer Abdalla Elfadil Eisa, Hashim Albasheer, Sara Abdelwahab Ghorashi, and Faten Khalid Karim. 2022. "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions." *Electronics (Basel)* 11 (4): 630–. https://doi.org/10.3390/electronics11040630.

Adams, Victoria, Mike Alonso, Wendy Henry, David Hyland-Wood, Walter "Chip" Jansen, Venkat Kodumudi, Anoop Nannra et al. (2020). *Potential Uses of Blockchain by the U.S. Department of Defense.* Washington, DC: Value Technology Foundation.

Allen, Greg. (2020). *Understanding AI Technology*. https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf.

Attkan, Ankit, and Virender Ranga. 2022. "Cyber-Physical Security for IoT Networks: a Comprehensive Review on Traditional, Blockchain and Artificial Intelligence Based Key-Security." *Complex & Intelligent Systems*. https://doi.org/10.1007/s40747-022-00667-z.

Battah, Ammar Ayman, Mohammad Moussa Madine, Hamad Alzaabi, Ibrar Yaqoob, Khaled Salah, and Raja Jayaraman. 2020. "Blockchain-Based Multi-Party Authorization for Accessing IPFS Encrypted Data." IEEE Access 8: 196813–25. https://doi.org/10.1109/ACCESS.2020.3034260.

Ben Dhaou, Imed, Mousameh Ebrahimi, Meriam Ben Ammar, Ghada Bouattour, and Olfa Kanoun. 2021. "Edge Devices for Internet of Medical Things: Technologies, Techniques, and Implementation." *Electronics (Basel)* 10 (17): 2104–. https://doi.org/10.3390/electronics10172104.

Benzaid, Chafika, Tarik Taleb, and Muhammad Zubair Farooqi. 2021. "Trust in 5G and Beyond Networks." *IEEE Network* 35 (3): 212–22. https://doi.org/10.1109/MNET.011.2000508.

Binlashram, Arwa, Lobna Hsairi, Hajer Bouricha, and Haneen AL Ahmadi. 2020. "A New Multi-Agents System based on Blockchain for Prediction Anomaly from System Logs." In *The 22nd International Conference on Information Integration and Web-based Applications Services*. https://doi.org/10.1145/3428757.3429149.

Cao, Sheng, Gexiang Zhang, Pengfei Liu, Xiasong Zhang and Ferrante Neri. 2019. "Cloud-Assisted Secure eHealth Systems for Tamper-Proofing EHR via Blockchain." *Information Sciences* 485: 427–440. https://doi.org/10.1016/j.ins.2019.02.038.

Chen, Chin-Ling, Jiaxin Yang, Woei-Jiunn Tsaur, Wei Weng, Chih-Ming Wu, and Xiaojun Wei. 2022. “Enterprise Data Sharing with Privacy-Preserved Based on Hyperledger Fabric Blockchain in IIOT’s Application.” *Sensors* (Basel, Switzerland) 22 (3): 1146–. https://doi.org/10.3390/s22031146.

Clark, Jen. 2016. “What is the Internet of Things (IoT)?” *IBM Business Operations Blog* (blog), November 16, 2016. https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/.

Comiter, Marcus. 2019. Attacking Artificial Intelligence: AI’s Security Vulnerability and What Policymakers Can Do About It. Belfer Center Paper, Harvard Kennedy School.

Culpan, Tim. 2022. “The Next Cybersecurity Crisis: Poisoned AI.” Bloomberg. Last modified April 24, 2022. https://www.bloomberg.com/opinion/articles/2022-04-24/ai-poisoning-is-the-next-big-risk-in-cybersecurity

Deepa, Natarajan, Quoc-Viet Pham, Dinh C Nguyen, Sweta Bhattacharya, B Prabadevi, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, Fang Fang, and Pubudu N Pathirana. 2020. “A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions.”

Defense Health Agency. 2022. “Electronic Health Record: MHS Gensis.” Defense Health Agency. Accessed July 24, 2022. https://www.health.mil/Military-Health-Topics/MHS-Transformation/MHS-GENESIS.

Draskovic, Drasko and George Saleh. 2017. “Datapace: Decentralized Data Marketplace based on Blockchain.” White paper, Datapace, https://datapace.io/.

Elezabeth, Laura and Ved P. Mishra. “Big Data Mining Methods in Medical Applications.” In *Medical Big Data and Internet of Medical Things: Advances, Challenges and Applications*, edited by Aboul Ella Hassanien, Nilanjan Dey and Surekha Borra, 1—23. Milton: CRC Press. https://doi.org/10.1201/9781351030380.

Ferris, Christopher. 2019. “Does Hyperledger Fabric Perform at Scale?” *IBM Supply Chain and Blockchain Blog* (blog), April 2, 2019. https://www.ibm.com/blogs/blockchain/2019/04/does-hyperledger-fabric-perform-at-scale/

Firican, George. 2017. “The 10 vs. of Big Data.” Transforming Data With Intelligence (TDWI). February 8, 2017. https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx?m=1.

Freund, Gislaine Parra, Priscila Basto Fagundes, and Douglas Dyllon Jeronimo de Macedo. 2020. “An Analysis of Blockchain and GDPR Under the Data Life cycle Perspective.” *Mobile Networks and Applications* 26 (1): 266–76. https://doi.org/10.1007/s11036-020-01646-9.

Gan, Bo, Qiwu Wu, Xiang Li, and Yang Zhou. 2021. "Harsh Communication Environment Oriented Consortium Blockchain Construction on Edge for Internet of Things." *Journal of Physics*. Conference Series 1972 (1): 12001–. https://doi.org/10.1088/1742-6596/1972/1/012001.

Hicks, Kathleen. 2021. "Creating Data Advantage." Memorandum. Washington, DC: Department of Defense.

Hyperledger. 2022. "Peers." https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peers.html.

The Hyperledger Architecture Working Group. 2017. *Hyperledger Architecture, Volume 1: Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus*. https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf.

The Hyperledger Performance and Scale Working Group. 2018. *Hyperledger Blockchain Performance Metrics*. https://www.hyperledger.org/learn/publications/blockchain-performance-metrics

Indumathi, J, Achyut Shankar, Muhammad Rukunuddin Ghalib, J Gitanjali, Qiaozhi Hua, Zheng Wen, and Xin Qi. 2020. "Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6 HCS)." *IEEE Access* 8: 216856–72. https://doi.org/10.1109/ACCESS.2020.3040240.

International Business Machines (IBM). 2017. "How Nodes Reach a Consensus on a Blockchain." YouTube video, September 20, 2017. https://www.youtube.com/watch?v=DqtzxJP6Y9k.

IBM. 2018. Governed Data Lake for Business Insights: Explore the Key Building Blocks to Effectively Deliver Trusted Data. https://www.ibm.com/downloads/cas/RMAMZNRY.

———. 2021. *How to Choose the Right Data Warehouse for AI.* https://ibm.com/downloads/cas/QK7MQ7YY.

———. 2022a. "What is a Data Lake?" IBM. Accessed July 17, 2022. https://www.ibm.com/topics/data-lake.

———. 2022b. "What is Blockchain Technology?" IBM. Accessed June 12, 2022. https://www.ibm.com/topics/what-is-blockchain.

Ioniţă, Crăisor-Constantin. 2020. "The 'Mosaic' Warfare: A New American Strategy for the Future." *Strategic Impact*, no. 75: 25–42.

Jeong, Yoon-Su. 2021. “Blockchain Processing Technique Based on Multiple Hash Chains for Minimizing Integrity Errors of IoT Data in Cloud Environments.” *Sensors* (Basel, Switzerland) 21 (14): 4679–4694. https://doi.org/10.3390/s21144679.

Kapitonov, Aleksandr, Sergey Lonshakov, Aleksandr Krupenkin, and Ivan Berman. 2017. “Blockchain-Based Protocol of Autonomous Business Activity for Multi-Agent Systems Consisting of UAVs.” In *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, 84–89. IEEE. https://doi.org/10.1109/RED-UAS.2017.8101648.

Karmipour, Hadis and Farnaz Derakhshan. 2021. “Preface.” In *AI-Enabled Threat Detection*, edited by Hadis Karimipour and Farnaz Derakhshan, v—vi. Cham: Springer AG.

Kendall, Anthony, Arijit Das, Bruce Nagy, Bonnie Johnson, and Avantika Ghosh. (n.d.) “Increasing Confidence and Data Availability from IoT and Other Soures Supporting Artificial Intelligence (AI) and Analytical Tools Using Hyperledger Fabric Blockchain.” Naval Postgraduate School.

Kott, Alexander, Ananthram Swami, and Bruce J. West. 2017. “The Internet of Battle Things.” *Computer* 49 (12) (December): 70–75. https://doi.org/10.1109/MC.2016.355.

Kumar, Harsh, Manu, M.R., Indrakumari, R., and Blamurugan, B. 2020. “Chapter 5 Blockchain Use Cases in Big Data” In *Blockchain, Big Data and Machine Learning: Trends and Applications*, edited by Neeraj Kumar, N. Gayathri, Md. Arafatur Rahman, and B. Balamurugan. 111—139. Boca Raton: CRC Press. https://doi.org/10.1201/9780429352546.

Kumar, Rajesh, and Rewa Sharma. 2021. “Leveraging Blockchain for Ensuring Trust in IoT: A Survey.” *Journal of King Saud University*. Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2021.09.004.

Kuzlu, Murat, Corinne Fair and Ozgur Guler. 2021. “Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity.” *Discover Internet of Things* 1 (1). https://doi.org/10.1007/s43926-020-00001-4

Li, Xi, Zehua Wang, Victor C. M. Leung, Hong Ji, Yiming Liu, and Heli Zhang. 2021. “Blockchain-Empowered Data-Driven Networks: A Survey and Outlook.” *ACM Computing Surveys* 54 (3): 1–38. https://doi.org/10.1145/3446373.

Makhdoom, Imran, Mehran Abolhasan, Haider Abbas, and Wei Ni. 2019. “Blockchain’s Adoption in IoT: The Challenges, and a Way Forward.” *Journal of Network and Computer Applications* 125: 251—279.

Malik, Sidra, Volkan Dedeoglu, Salil S Kanhere, and Raja Jurdak. 2019. "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains." In *2019 IEEE International Conference on Blockchain (Blockchain)*, 184–93. IEEE. https://doi.org/10.1109/Blockchain.2019.00032.

Moke, Kwai Cheong, Tan Jung Low, and Dodo Khan. 2021. "IoT Blockchain Data Veracity with Data Loss Tolerance." *Applied Sciences* 11 (21): 9978–. https://doi.org/10.3390/app11219978.

N, Deepa, Quoc-Viet Pham, Dinh C. Nguyen, Sweta Bhattacharya, B. Prabadevi, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, Fang Fang, and Pubudu N. Pathirana. 2021. *A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions*. arXiv.org

Pajooh, Houshyar Honar, Mohammed Rashid, Fakhrul Alam, and Serge Demidenko. 2021. "Hyperledger Fabric Blockchain for Securing the Edge Internet of Things." *Sensors* 21 (2): 359. https://doi.org/10.3390/s21020359.

Palaiokrassas, Georgios, Petros Skoufis, Orfefs Voutyras, Takafumi Kawasaki, Mathieu Gallissot, Radhouene Azzabi, Akira Tsuge et al. 2021. "Combining Blockchains, Smart Contracts, and Complex Sensors Management Platform for Hyper-Connected SmartCities: An IoT Data Marketplace Use Case." *Computers (Basel)* 10 (10): 133–. https://doi.org/10.3390/computers10100133.

Panarello, Alfonso, Nachiket Tapas, Giovanni Merlino, Francesco Longo, and Antonio Puliafito. 2018. "Blockchain and IoT Integration: A Systematic Survey." *Sensors (Basel, Switzerland)* 18 (8): 2575–. https://doi.org/10.3390/s18082575.

Patel, Nihar, Upesh Patel, Evert R. Hawk II and Krupal Kapadia. 2021. "Stitching the Army's Data Fabric." *Army ALT Magazine* (Fall 2021): 14–19. https://asc.army.mil/web/news-stitching-the-armys-data-fabric/.

Pike, John. 2020. "Measurement and Signature Intelligence (MASINT)." FAS Intelligence Resource Program. Last modified May 8 2020. https://irp.fas.org/program/masint.htm

Pre Employment Checks. 2019. "Understanding MASINT and Its Practical Uses." Pre Employment Checks. Last modified July 18, 2019. https://www.pre-employment-checks.com/en/understanding-masint-and-its-practical-uses/.

Rahayu, Syarifa Bahiyah, Norizam Jusoh RMN, Nur Diyana Kamarudin, and Afiqah Mohammad Azahari. 2019. "Military Blockchain for Supply Chain Management." *Journal of Education and Social Sciences* 13 (1) (June): 9—14.

Rahim, Robbi, Rizwan Patan, R. Manikandan, and S. Rakesh Kumar. 2020. “Chapter 1 Introduction to Blockchain and Big Data.” In *Blockchain, Big Data and Machine Learning: Trends and Applications*, edited by Neeraj Kumar, N. Gayathri, Md. Arafatur Rahman, and B. Balamurugan. 1—23. Boca Raton: CRC Press. https://doi.org/10.1201/9780429352546.

Reyna, Ana, Cristian Martin, Jaime Chen, Enrique Soler, and Manuel Diaz. 2018. “On Blockchain and its Integration with IoT. Challenges and Opportunities.” *Future Generation Computer Systems* 88: 173–190.

Saberi, Sara, Mahtab Kouhizadeh, Joseph Sarkis, and Lejia Shen. 2019. “Blockchain Technology and Its Relationships to Sustainable Supply Chain Management.” *International Journal of Production Research* 57 (7): 2117–35. https://doi.org/10.1080/00207543.2018.1533261.

Shetty, Sachin, Charles A Kamhoua, and Laurent L Njilla. 2019. *Blockchain for Distributed Systems Security*. 1st ed. Newark: Wiley. https://doi.org/10.1002/9781119519621.

Solanki, Vijender Kumar, Cecilia E. GarciÌ□a Cena, and Manuel Cardona. 2021. *Internet of Medical Things : Paradigm of Wearable Devices.* Edited by Vijender Kumar Solanki, Cecilia E. GarciÌ□a Cena, and Manuel Cardona. Boca Raton, Florida : CRC Press.

Tosh, Deepak K, Sachin Shetty, Peter Foytik, Laurent Njilla, and Charles A Kamhoua. 2018. “Blockchain-Empowered Secure Internet -of- Battlefield Things (IoBT) Architecture.” In *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 593–98. IEEE. https://doi.org/10.1109/MILCOM.2018.8599758.

U.S. Army. 2021. *The Army Unified Network Plan*. Arlington, VA: Office of the Under Secretary of the United States Army.

U.S. Army Combined Army Center. 2022. *Combined Arms Doctrine Newsletter & Doctrine Developer’s Guidance*. Fort Leavenworth, KS: U.S. Army Combined Arms Center.

U.S. Army Training and Doctrine Command. 2018. *The U.S. Army in Multi-Domain Operations 2028*. TRADOC Pam 525–3-1. Newport News, VA: U.S. Army Training and Doctrine Command.

Willink, T.J. 2018. *On Blockchain Technology and It Potential Application in Tactical Networks*. Ottawa, Canada: Defence Research and Development Canada.

Xu, Rongxu, Lei Hang, Wenquan Jin, and Dohyeun Kim. 2021. “Distributed Secure Edge Computing Architecture Based on Blockchain for Real-Time Data Integrity in IoT Environments.” *Actuators* 10 (8): 197–. https://doi.org/10.3390/act10080197.

Zhang, Jinnan, Changqi Lu, Gang Cheng, Teng Guo, Jian Kang, Xia Zhang, Xueguang Yuan, and Xin Yan. 2021. “A Blockchain-Based Trusted Edge Platform in Edge Computing Environment.” *Sensors* (Basel, Switzerland) 21 (6): 2126–. https://doi.org/10.3390/s21062126.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California