American Journal of Computer Science and Technology
2023; 6(4): 126-147
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20230604.12
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Blockchain at the Tactical Edge: Enabling an Internet of Battlefield Things

Bonnie Johnson[1, *], Anthony Kendall[2], John Green[1], Bruce Nagy[3], Gregory Dogum[1], Kristin Jones Maia[1], Michele Meszaros[1], Jonathan Novoa[1], Rene Villarreal[1]

[1]Systems Engineering Department, Naval Postgraduate School, Monterey, USA

[2]Information Sciences Department, Naval Postgraduate School, Monterey, USA

[3]Naval Air Warfare Center, Weapons Division, Ridgecrest, USA

Email address:

bwjohnson@nps.edu (Bonnie Johnson)

[*]Corresponding author

To cite this article:

Bonnie Johnson, Anthony Kendall, John Green, Bruce Nagy, Gregory Dogum et al. (2023). Blockchain at the Tactical Edge: Enabling an Internet of Battlefield Things. *American Journal of Computer Science and Technology*, *6*(4), 126-147.
https://doi.org/10.11648/j.ajcst.20230604.12

Received: August 12, 2023; **Accepted**: September 6, 2023; **Published**: November 24, 2023

Abstract: 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 enable an internet of battlefield things—is dependent upon accessible and reliable information. This paper presents the results of a study that evaluated the use of blockchain technology to address 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 at the tactical edge to support an internet of battlefield thing approach by verifying users, validating sensor data fed into artificial intelligence models, limiting access to data, and providing 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 the findings to propose future research into a wide set of tactical blockchain applications. The team studied three use cases: (1) blockchain at the tactical edge in a "data light" information environment for long range fires, (2) blockchain to secure tactical medical information in electronic health record, and (3) blockchain for collecting multiple types of tactical sensor data for chemical weapons defense to support measurement and signature intelligence analysis using artificial intelligence and machine learning.

Keywords: Blockchain, Internet of Battlefield Things, Hyperledger, Data Fabric, Long Range Fires, Electronic Health Record, Chemical Weapons

1. Introduction

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 [1]. 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 U. S. Army has updated their field manuals to include information as a third dimension to the operational environment; and information is now included in the Army's combat power model [2]. 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). The Army is also drafting a new doctrine publication (3-13), titled "Information" that "links the military applications of information to all warfighting functions, branches, and forms of warfare" [2]. These shifts and evolutions 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.

Engineered, complex adaptive systems-of-systems [3] are now commonplace across the U. S. Department of Defense (DoD) 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 [4]. 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, human operator interactions with these models and influence the analysis, and outside threats that may disrupt the information collected, measured, and processed.

DoD's use of varied and disparate sensors is analogous to the "Internet of Things" (IoT), the myriad of internet-connected devices that exist in civilian (but also military) settings [5]. In both instances, there is a strong need to ensure that 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 called the "Internet of Battlefield Things" (IoBT) [6]. The IoBT could fulfill a "strong need [for a] decentralized framework…to serve the purpose of the battlefield environment" [6]. Also discussed is how blockchain technology could be used for a variety of purposes to benefit the IoBT architecture—to provide data in a secure and trusted manner. Moreover, the decentralization of a future battlefield blockchain could strengthens its ability to secure the IoBT and provide resiliency if some parts of the IoBT are denied or destroyed in combat.

Some military missions may be strengthened by the analysis of big data—very large sets of data and information. Big data was initially characterized by 3 V's, which have expanded into ten V's of data: volume, velocity, variety, variability, veracity, validity, vulnerability, volatility, visualization, and value [7]. A particular focus for military applications is 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 [8]. 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 to facilitate accessibility to data—no matter where it resides. These data management sources could be traditional databases, data lakes [9], or data warehouses [10]. 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 the availability of data required.

This shift to more decentralized architectures could help overcome some of the limitations of the current, more centralized tactical 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 a data-centric model to create a "data advantage" by "improving performance and creating decision advantage at all echelons from the battlespace to the board room" [11]. 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 [12]. This can cause the AI to behave in unintended ways and prevent it from recognizing patterns or making the desired correlations [13]. 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.

This paper is organized into six sections: (1) an introduction,

(2) a section on emerging information concepts and technologies in the context of future warfare, (3) an overview of blockchain technologies, (4) the results of the team's system analysis, (5) a discussion of the team's three use cases, and (6) a conclusion that summarizes the analysis and identifies future work.

2. Emerging Information Concepts and Technologies in the Context of Future Warfare

Through this blockchain research, the team learned that a large undercurrent in computers and networks 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.

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 [14]. Not only does this increased activity generate a tremendous amount of data [14] but can also lead to significant generation of "execution traces"—data that is generated by a system about its performance [15]. In addition, the increased number of "smart" and/ or internet-connected devices pushes this expansion further. Moreover, the rollout of next-gen networks such as 5G further supports a diverse "ecosystem…of interconnected devices and services" [16]. 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.

2.1. 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. The IoT is described 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 [17]. On a pseudo microcosmic level, multi-agent systems (MAS) are like the IoT in that they integrate a diverse range of devices (or "agents") but are intentionally constructed, whereas the IoT emerges organically (unintentionally). MAS still have a degree of being distributed and may include a collection of software agents, robots, sensors, and autonomous agents working together to support processes or perform collection functions [18]. 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 purposes. For example, there is the Industrial Internet of Things (IIoT), sometimes described in connection with the term Industry 4.0. IIoT are described as "making use of intelligent, interconnected cyber-physical systems to automate all phases of industrial operations" [19]. 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, such as issues with data sharing and data privacy; the need to find secure ways to store and handle the data generated by the IIoT as well as the raw data; and the need to find efficient ways to query the vast amounts of generated data [20].

Just as there is an IIoT, the research revealed the military's IoBT as an important concept for orchestrating military operations on an information-dense battlefield. The IoBT is described as the collection of "combat equipment, warfighters, and vehicles that can sense and disseminate information from the battlefield" [6]. The IoBT has also been described as a distributed, interconnected network of devices that execute a myriad of automated tasks to support sensing and coordinated defensive/ offensive actions [21]. 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 [21]. Additionally, "great innovations in robotics, artificial intelligence, nanotechnology and unmanned systems" have been described as great drivers of change in how wars are fought [22]. These emerging technologies on the battlefield will contribute to a heterogeneous IoBT network that supports the U. S.'s ability to fight and win wars.

2.2. Big Data

Another related concept revealed in the research that bears discussion is big data. Big data is defined as "data sets that are large or complex in which traditional data processing applications are inadequate" [23]. 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. AI and machine learning (ML) 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 are identified with the IoT [20], also accompany big data: managing the structure, storage, transfer, sharing, analysis, and visualization—all while ensuring security and privacy protections [23].

2.3. 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: human trust in the IoT. 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. Trust becomes a central factor when considering 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 [24]. Because the data is generated in a distributed and autonomous way, it can make the IoT vulnerable to tampering [23]. When the IoT is providing insight into critical systems like smart cities and smart transportation, this tampering can have significant consequences [23]. The concept of trust also goes beyond trusting the data and extends to the parties that are interacting as well.

2.4. Artificial Intelligence and Machine Learning

Advancing alongside, but also in support of, these various IoTs and big data have been increasingly sophisticated AI and ML tools and systems. The DoD has created the Joint Artificial Intelligence Center (JAIC) as an organization to oversee and provide guidance for AI and ML development in the military. JAIC guidance covers the spectrum of AI technology and differentiates it from ML systems, noting that AI technology has been around for decades and can include mature technology like autopilot on aircraft or missile guidance [25]. The distinguishing difference is that, generally, humans program the AI whereas ML allows machines to learn from data. AI technology is programmed using "if, then" statements; ML systems can program themselves using human-generated algorithms and training data sets.

AI and ML systems require large amounts of secure, valid data that accurately represents the real-world. Data is used for training and developing AI and ML systems. Once algorithms are developed, they operate based on a continued steady stream of data. AI and ML systems can be considered inherently and intimately connected with data. Thus, their development and use require secure and trusted data—making them a good candidate for blockchain applications.

AI and ML systems are "vulnerable to a new type of cybersecurity attack called 'artificial intelligence attacks'" which are profoundly different than more traditional cyber-attacks [26]. 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. The ability to leverage physical objects in an AI attack is one example of why these attacks are so different. An example is the use 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 [26].

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.

3. Overview of Blockchain

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.

Blockchain is a distributed, immutable ledger that records transactions in blocks, and tracks assets stemming from those transactions [27]. 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.

The section provides overviews of smart contracts and data or hyperledger fabric. It discusses some applications and benefits of using blockchain—including security, data value, edge computing, and big data.

3.1. 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" [28] that ensure specific conditions are met. As such, they can be used to automate many processes in each IoT network [29]. Examples include actor certification and approval, and the automated updating of ownership records of goods as they are bought, sold, and delivered. Smart contracts are also used for multi-party authentication to facilitate the appropriate sharing of encrypted data on a public platform [30].

3.2. Data and Hyperledger Fabric

Hyperledger fabric (HLF) is an approach intended to overcome limitations of public blockchains. Public blockchains are permissionless—allowing anyone to participate without a specific identity. These types of blockchains suffer from many limitations including that consensus is hard-coded within the platform, the trust model is determined by the hard-coding and is not adaptable, smart contracts are fixed and domain-specific, sequential execution limits performance, transactions are deterministic, and every smart contract runs on all peers [31].

The concept of managing data as a fabric is a shift away from traditional static data storage and databases. A data

fabric approach moves beyond treating data as "mere binary blobs" and constantly "losing and rewriting our digital history" [32]. Data fabric views data as mutable and changing and aims to support decentralized management and collaboration. Trust in the data is achieved through reproducibility, verifiability, and provenance. An HLF approach is intended to bypass data throughput bottlenecks in traditional data management architectures to increase data transactions at scale. HLF incorporates "architectural changes that reduce computation and input/output overhead during transaction ordering and validation" [33].

HLFs are based on an architecture that separates metadata from data, aggressively parallelizes and caches transaction data, exploits the memory hierarchy to provide fast data access, and separates resources into committer and endorser roles [33]. HLF is designed to be "highly modular and extensible, delivering confidentiality, privacy, and scalability to enterprise blockchains" [34].

3.3. Applications and Benefits of Blockchain

Supply chain management is an area that is well suited to early adoption of blockchain technology. Blockchain technology and smart contracts can ensure that supply chains meet certain sustainability metrics, by tracking conditions that could pose environmental, health, and safety concerns and providing full transparency of a product's origin [28]. A consortium blockchain can track transactions and interactions among supply chain participants [35]. This 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 [36]. A Malaysian study on the use of blockchains for military supply chains highlights the issue of counterfeit parts contaminating military supply chains and discusses how blockchain could help prevent this [37]. A Canadian study raises a similar concern about counterfeit parts in tactical networks and proposes a blockchain solution [38]. A U. S. Navy study explores the application of blockchain to naval logistics through examples of transaction audit trails (both from a financial and inventory perspective), serial number tracking, and maintenance log integrity [39].

The following subsections describe four blockchain applications: security, data value, edge computing, and big data.

3.3.1. Security

Blockchain offers a secure means of data exchange for IoT. The integration of blockchain and the IoT offers increased trust because information shared is reliable and traceable which supports increased decentralization and greater autonomy and services [23, 24]. Some of the inherent challenges with IoT, namely security and privacy issues stem from a centralized framework [40]. The application of blockchain can enable the IoT to become decentralized, self-regulated, and more trustable. Blockchain can also address the scalability, security, privacy, trust, and interoperability that exists in the IoT [41].

Blockchain can address security challenges with the IoT with its "immutability, transparency, auditability, data encryption and operational resilience" [42]. IoT devices need to be able to mutually authenticate each other and blockchain offers the capability to support this (with assistance from AI), despite high levels of heterogeneity [43].

3.3.2. Data Value

Blockchain offers a solution for managing IoT-generated data and addressing existing inadequacies of cloud storage [44]. A blockchain approach can help ensure the IoT data is protected and accessible. Blockchain can secure the data generated by the IoT, and when combined with smart contracts, can facilitate and automate data storage, privacy, and sharing [29]. One vision has been proposed for a "Blockchain Marketplace" for the exchange of IoT data to support virtual currencies or other assets [29]. This concept rests on the recent acknowledgement of the importance of data ("data is the new oil"), and that a marketplace is evolving for IoT sensor data [45]. Another study presented a blockchain-based IoT concept with the goal of preventing data loss [46].

3.3.3. Edge Computing

Another application for blockchain is its proposed use to improve the computer performance of the actual devices in the IoT [47]. This concept is based on an architecture for "distributed secure edge computing" where blockchain ensures data integrity in this environment [47]. This application could support edge computing architecture in harsh environments, and the ability of a consortium blockchain to facilitate information security, traceability, and sharing of data [48]. This is particularly relevant to possible applications of blockchain in the IoBT. One study examines blockchain's benefits and use in a way that does not compromise computer performance [49]. This study used HLF in a model to facilitate local authorization of IoT devices and traceability of the data generated. Yet another study proposes the use of HLF to model a proposed blockchain-IoT architecture to preserve privacy for edge devices [50].

3.3.4. Big Data

Blockchain has many applications for the use of big data [51]. A blockchain architecture can be used to share big data securely, ensure trust (in the data), prevent malicious attacks, facilitate and real-time data analysis [52]. One study cites the challenges to making the most of big data and how the assistance of technologies like blockchain can improve big data services [53].

4. Blockchain Systems Analysis for Defense 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. The research team conducted a systems analysis of the use of blockchain for DoD applications. This analysis included a needs analysis (4.1), a study of systems engineering processes (4.2) a study of the IoBT and how it poses a challenge for future DoD data management (4.3), and an evaluation of a HLF approach as a solution to handle the IoBT data challenges (4.4).

4.1. Needs Analysis: DoD Data Lifecycle and Provenance

For most military operations there are three general tiers of decision-making: strategic, operational, and tactical. 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. Table 1 lists some applications and benefits of using blockchain to support DoD data sharing, management, and strategies.

Table 1. *DoD Needs.*

DoD Stakeholder Needs for Blockchain	
Support use of big data for development	Improved intelligence data collection
Support AI development	Enabling adaptive systems
Trusted data	Data Accessibility
Improved decision speed	Mitigation of cyber vulnerabilities
Data integrity	Secure data exchange
Improved wargames	Improved logistics planning

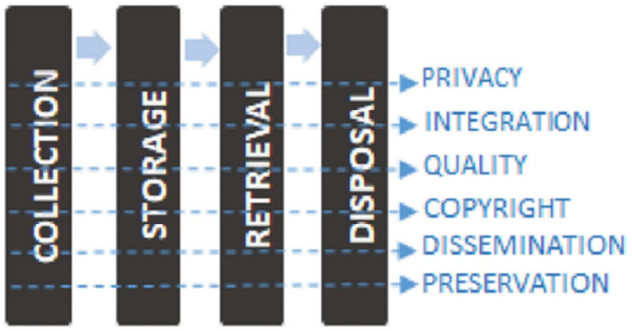

Figure 1. *The Data Life Cycle. Source [54].*

There are four general phases to the data lifecycle: 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 1, 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.

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.

4.2. 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 2 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 chain code, 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.

In this asset diagram (Figure 2), 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 chain code 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.

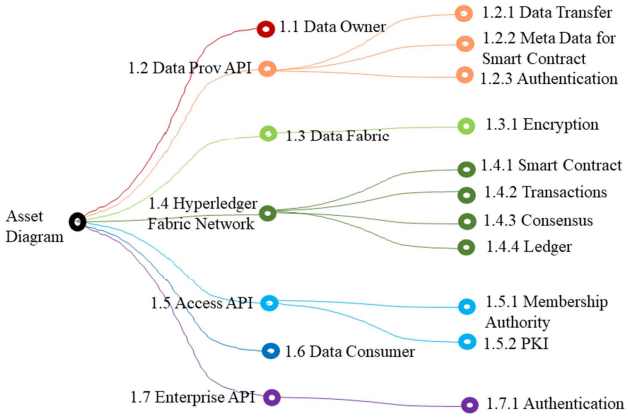

Figure 2. *Example Asset Diagram.*

In the tree diagram in Figure 3, the assets from Figure 2 are decomposed to show a mixture of both components and actions within this notional system.

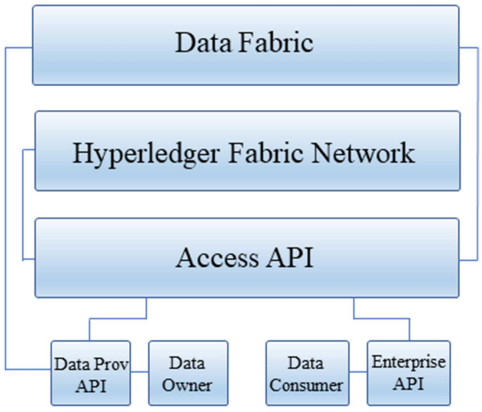

Figure 3. *Tree Diagram of Provenance Assets.*

To illustrate the sequence of actions, Figure 4 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 4 is intended to demonstrate the end-to-end process from data owner (producer) to data consumer.

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.

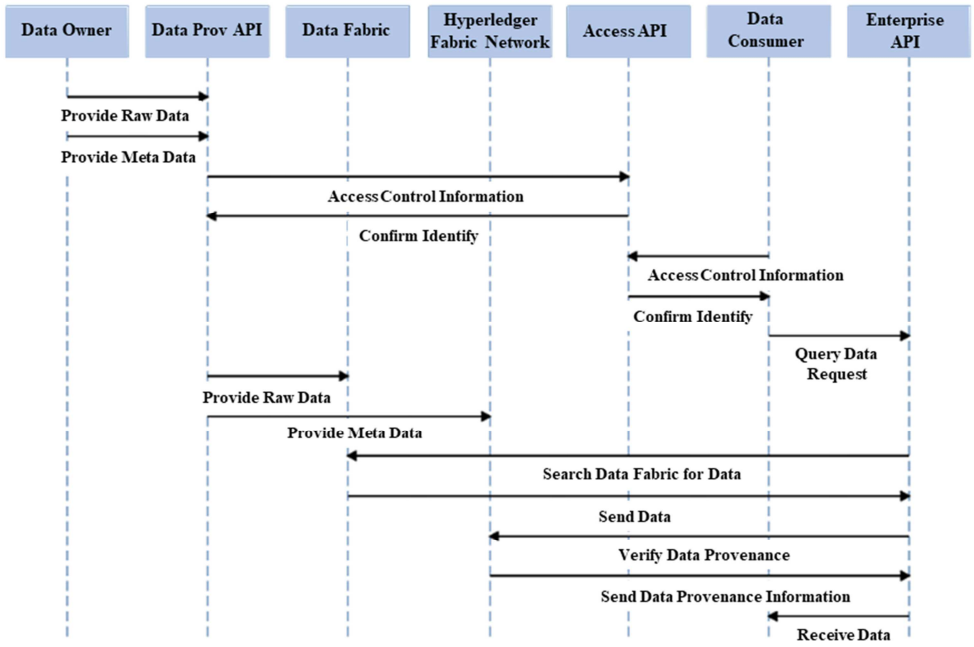

Figure 4. *Sequence Diagram of Provenance-Focused Blockchain Application.*

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.

4.3. The Internet of Battlefield Things

The use of IoBT will impose numerous challenges on already resource-constrained military communications networks, especially when factoring in cybersecurity and bandwidth limitations in DDIL environments [55].

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 because 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.

Several cybersecurity challenges are associated with IoBT: availability, confidentiality, and integrity [55]. 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 5. *Illustration of the Internet of Battlefield Things. Source [55].*

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 [56]. 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.

4.4. 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. 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 [57]. 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 [57]. 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 makes 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 [58]. 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 [58]. 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 [59].

This method forces a tradeoff between speed and scalability. As the network grows, so does 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 6, each with a unique function. Nodes in a blockchain network are virtual, independent entities that collectively work with other nodes to complete transactions [60]. 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 [61]. 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 [61]. 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 [59].

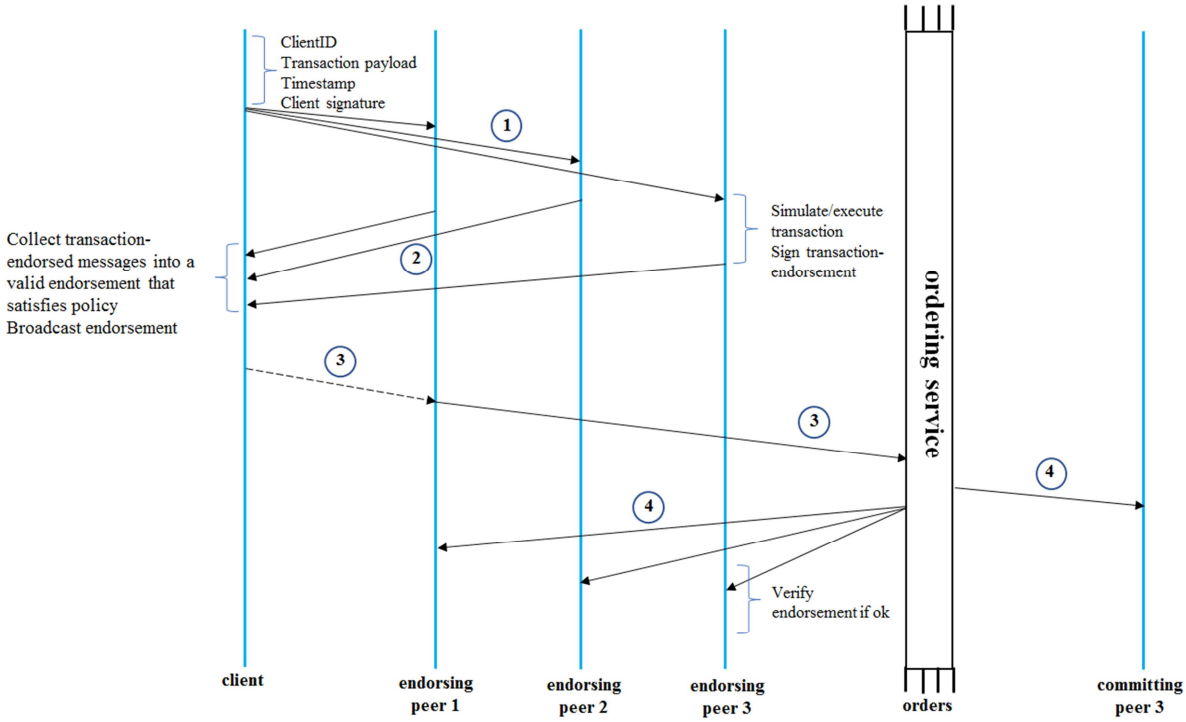

Figure 6. *Transaction Flow in Hyperledger Fabric. Source [58].*

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 [58]. 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 identity, credential, and access management (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 [62].

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.

4.5. Data Storage: On-Chain vs. Off-Chain

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, 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.

For DOD data architectures at the tactical edge, storing data off-chain offers some benefits, but also comes with risks. The use of a data fabric for off-chain data storage will greatly reduce the bandwidth required to share data needed by warfighters and warfare systems at the edge. Studies indicate the potential to facilitate data access across warfighter functions and mission command systems [63]. However, this architecture will not offer the data saving and recoverability of on-chain data storage. Other architectural approaches for data storage include data lakes and data warehouses [27].

5. Blockchain Use Case Analysis

This section discusses future use cases where blockchain could be applied to enhance operations at the tactical edge. Each of the three following subsections presents one of the use cases. The first use case discusses the use of blockchain to share targeting data securely and safely to support long-range fires (LRF) involving distributed sensors and weapon systems working together to precisely identify, track, target, and attack enemy threats. The second use case presents the use of blockchain to share critical medical status and information of warfighters in a secure manner to support battlespace awareness and readiness and to streamline medical and rescue support to wounded warfighters. The third use case proposes the use of blockchain to share measurement and signature intelligence (MASINT) concerning chemical warfare threats to support a secure method for developing and maintaining a chemical threat "picture" of an operational area. Each use case discussion includes an overview of how blockchain can be leveraged, a series of system artifacts that capture proposed system architectures, contextual information, and data sequences and lifecycles, and an assessment of the use of blockchain for the application.

5.1. Use Case 1 – Long-Range Fires

The LRF use case applies the IoBT concept to a scenario in which data from intelligence, surveillance, and reconnaissance (ISR) sensors is provided to weapon systems (or firing units) located in widely distributed places. The sensors provide targeting information to the weapon systems, extending the range of fires to very long distances, thus "long-range fires." This process of providing ISR data at great distances is vulnerable to enemy exploitation as the data can be intercepted, jammed, or spoofed. The solution to ensuring data is safely and securely transmitted in this use case, is to leverage a blockchain architecture.

An example of LRF is the use of Air Force ISR sensors to provide targeting data to Army weapon systems. The USAF is deploying manned and unmanned vehicles that collect ISR data. Both the Army and Air Force are developing tactical data fabric capabilities driven by AI. For the purposes of this study, these capabilities are referred to as "Army AI and "Air Force AI." The intended goal of applying a blockchain approach to these AI systems for LRF is to extend the effective range of the Army's artillery and mission systems through the use of the Air Force long-range targeting sensor data.

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 AI components 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 new vulnerabilities with the AI components. 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. It created a risk in which adversaries could exploit a compromised AI system to fire upon unintended targets.

This project proposes a solution that leverages 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 [63]. This addresses the second

problem and ensures the process cannot be compromised by enemy exploitation.

5.1.1. Blockchain-Supported LRF Conceptual Design

The team developed an activity diagram (Figure 7) that depicts the cycle of data without interruptions or vulnerabilities exploited. In this conceptual diagram, the data exists independently on the Air Force data fabric and also on an 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.

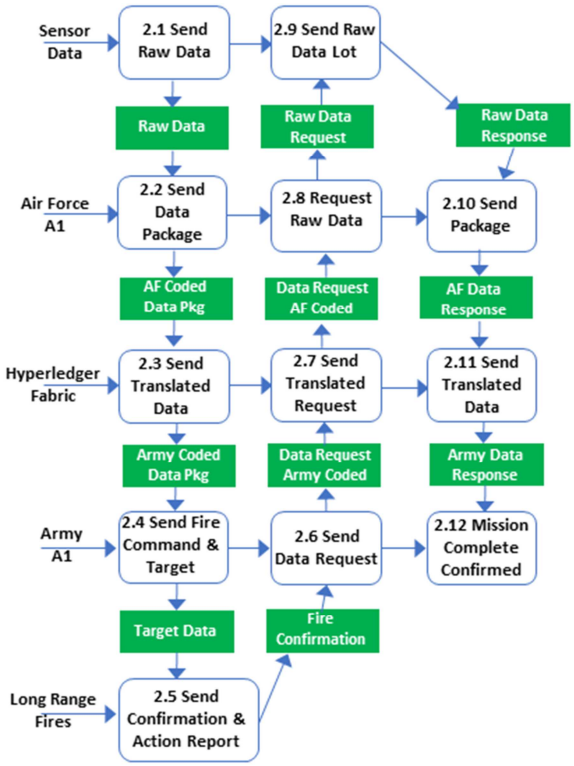

Figure 7. *Activity Diagram for Blockchain-Supported LRF.*

5.1.2. Blockchain-Supported LRF Context and Subsystems

The team developed a context diagram (Figure 8) to show how the HLF blockchain ties the 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.

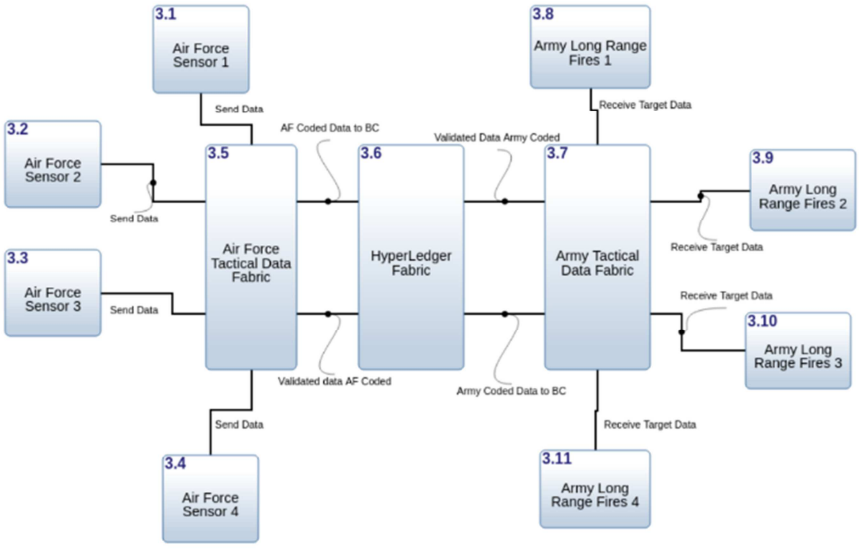

Figure 8. *Context Diagram for Blockchain-Enabled LRF.*

5.1.3. Blockchain-Supported LRF Event Sequence

The team created a sequence diagram (Figure 9) to explore the sequence of events for this concept from sensor to shooter. The flow of data originates from a sensor (or group of sensors), is packaged by the Air Force data fabric (Air Force AI), is then sent to the Army data fabric (Army AI) via the HLF blockchain. The Army data fabric processes the data and then sends targeting information to the LRF unit. In this sequence, the Army AI seeks confirmation of a successful strike by sending an updated data request back to the Air Force AI. The flow of sensor data repeats where the collected data is sent from Air Force AI to Army AI 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.

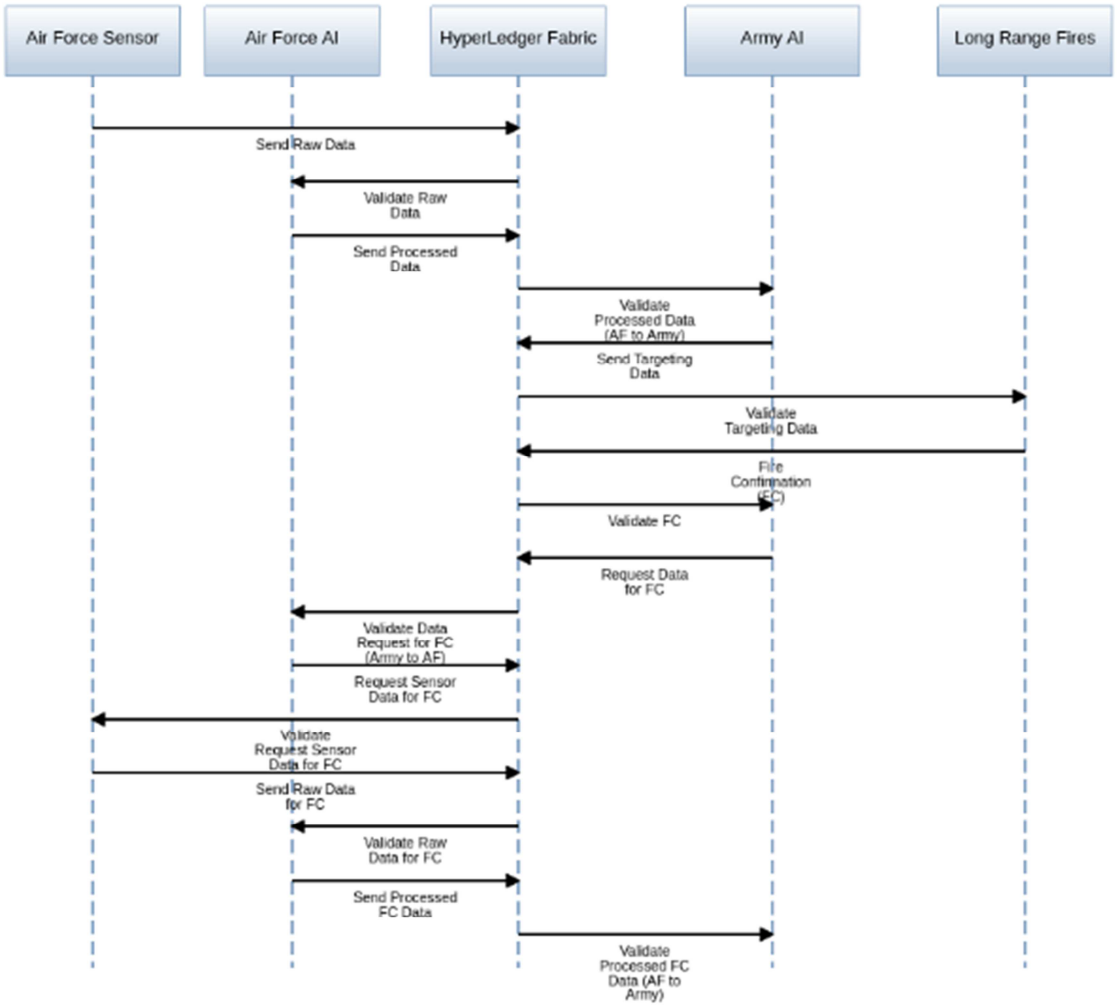

Figure 9. *Sequence Diagram for Blockchain-Enabled LRF.*

5.1.4. The Data Lifecycle for LRF Data

The team studied the lifecycle of data for the blockchain—enabled LRF capability. The team developed an event sequence diagram (Figure 10) that illustrates the four stages of the data life cycle. In the data creation phase, 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 Air Force AI collects and packages the raw data and converts it to a format that the Army AI can read. In turn, the 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.

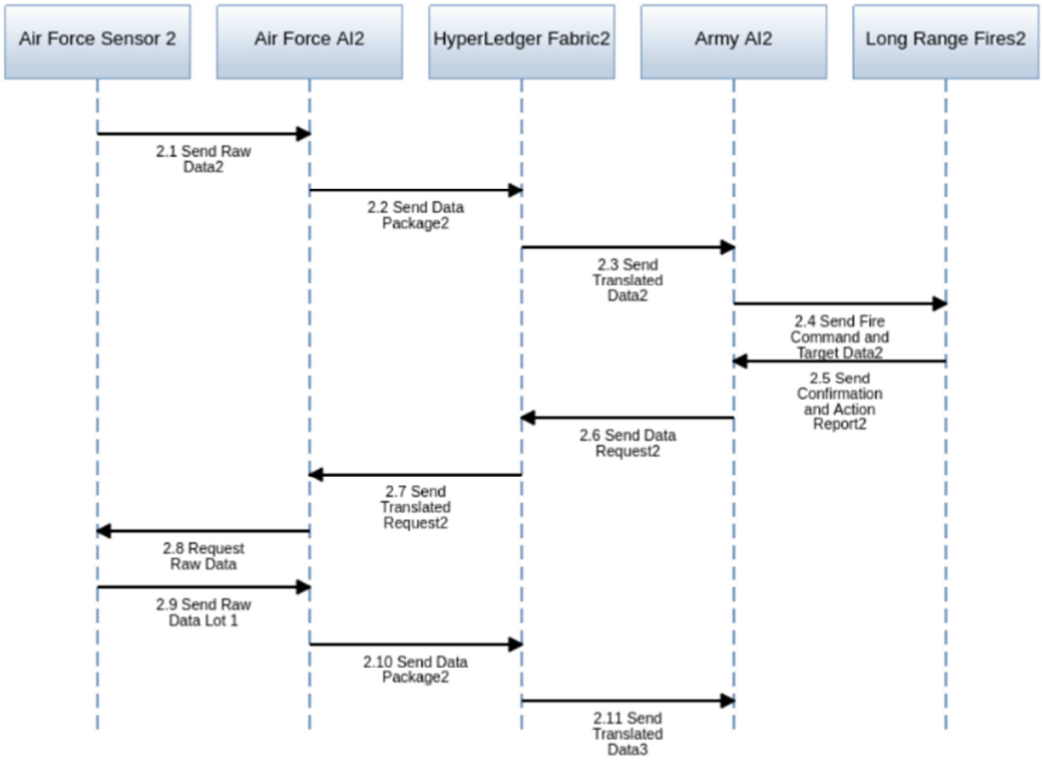

Figure 10. *Data Lifecycle Event Sequence for LRF Blockchain.*

The primary focus of the LRF use case was the utilization of HLF to enable secure transactions between two major systems (illustrated in Figure 9). An alternative approach would be to use HLF to validate every transaction in the sequence (illustrated in Figure 10). Note that a single sensor and LRF component are shown to depict the path of sensor data, but it is likely that data from multiple sensors will be compiled and processed to produce a targeting data package.

5.1.5. Blockchain-Supported LRF Assessment

The use of blockchain for LRF offers some appealing benefits in terms of data security. However, there are some significant implementation challenges that pose drawbacks to this solution strategy.

A primary strength of the blockchain-enabled approach for this LRF use case is that data is contained within two distinct data fabrics, offering redundancy without bogging down transactional bandwidth. The AI-driven data fabrics perform 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 Army and 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 [64]. It can be debated as to whether 13K TPS will suffice in a full-scale tactical scenario. Each Service (Army, Airforce, etc.) will have to make that determination.

Limitations of this team's analysis were the simplifications made in the use case scenario assumptions; namely that it focused on a minimal number of sensors, shooters, and targets and one data flow at a time. In the team's architecture, data flow was focused on a sensor-to-shooter path with minimal sensors and shooters displayed and assumed that the AI would be able to process the data sufficiently. The team 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. In a real-world combat scenario, data flows would be more complex, as would sensor-shooter-target dynamics and timelines.

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.

5.2. Use Case 2 – Medical Data on the Battlefield

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. IoMT has been described 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" [65]. IoMT establishes a framework to integrate and manage a variety of these medical things [66]. This also leads to significant amounts of data, which can lead to better diagnoses of diseases, and even better prediction and prevention [67]. The same way the IoT supports and contributes to big data in a broader sense, the same is true of the IoMT.

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 [66], even more so because of the Health Insurance Portability and Accountability Act (HIPAA) in the United States [67]. 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: electronic health records (EHR). EHR comprises vast amounts of information including "clinical history, lab reports and other relevant statistics among others" [67]. These patient records (and medical big data, overall) can be stored in highly centralized systems [67] that are vulnerable to attack or in cloud-based platforms that can (in essence) outsource ownership of those records [68]. 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, a blockchain approach may 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 [68].

The Military Health System (MHS) has also implemented an EHR system called MHS Genesis [69]. 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 Veteran's Affairs 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 explored how blockchain can provide an audit trail for every time a service member's EHR is updated—both in theater and at non-deployment locations. The terminology of blockchain often uses "transactions" 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, and 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.

The addition of AI/ML to the IoMT can process and analyze the medical big data 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 could 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 additional research and analysis.

5.2.1. Blockchain-Supported EHR Conceptual Design

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 chosen as the likely blockchain platform for the blockchain-based EHR.

The team developed an architecture (shown in Figure 11) that 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 from internet-connected lab equipment, images from 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.

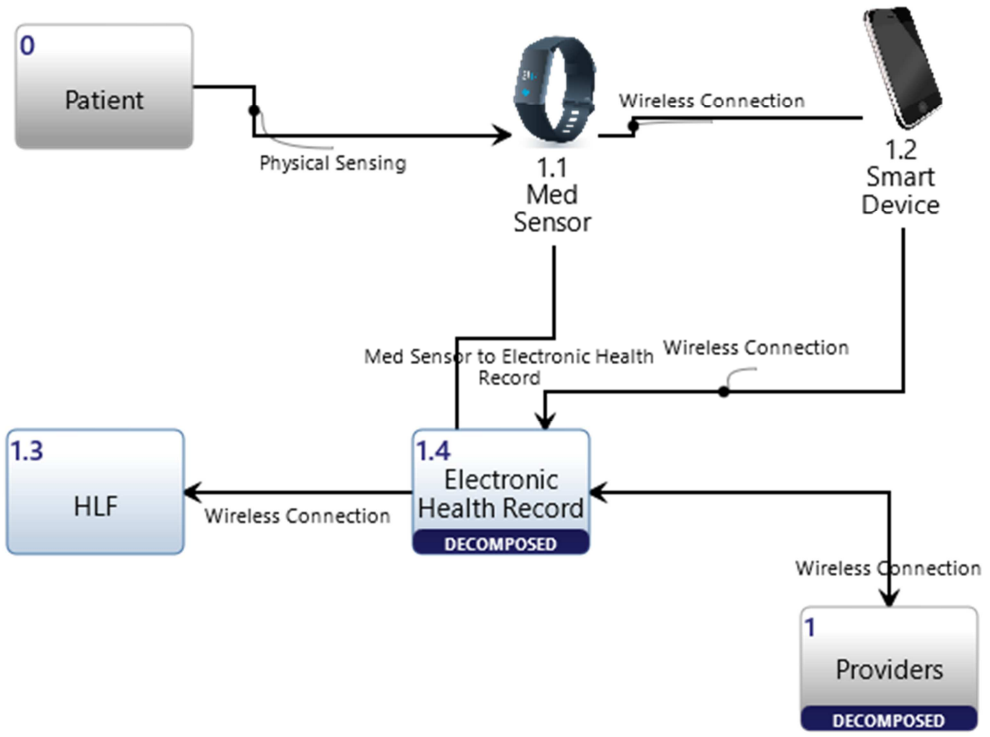

Figure 11. *Blockchain-Supported EHR System Architecture.*

5.2.2. Blockchain-Supported EHR Assets, Actors, and Definitions

In this use case, the team generalized some terms to distill the use case down to its essential components to facilitate straightforward diagrams. As such, this section provides 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), this study focused 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 to the large hospitals at military installations, and everything in between.

The HER 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 12, 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.

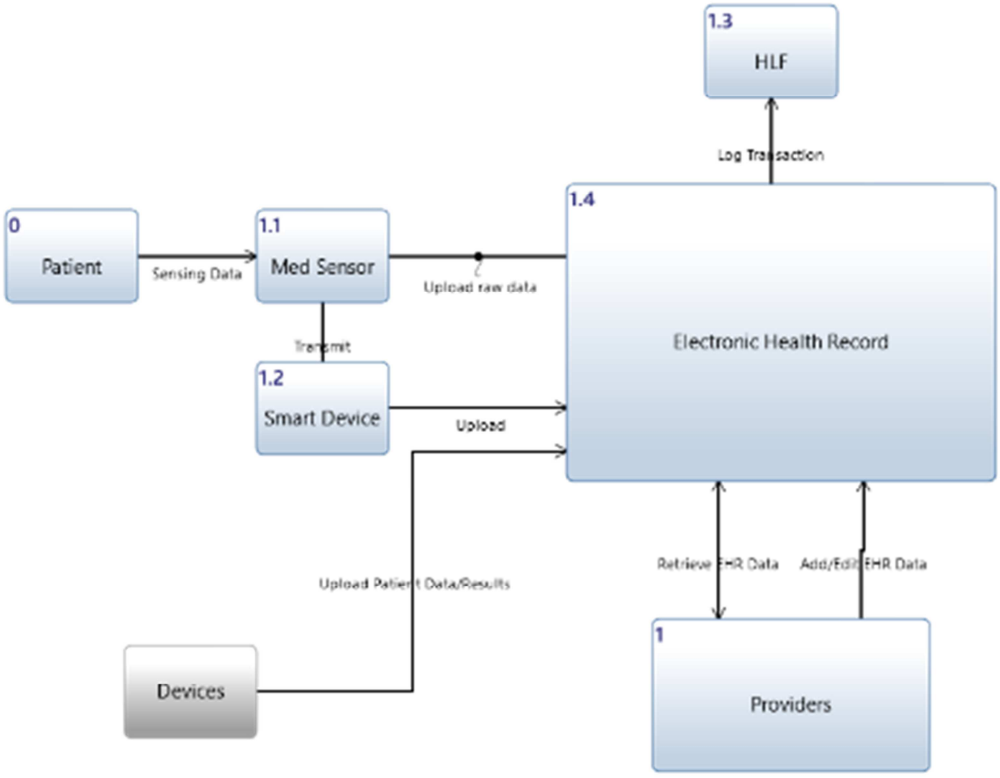

Figure 12. *Blockchain-Supported EHR Inputs and Outputs.*

5.2.3. Blockchain-Supported EHR Event Sequence

The team studied blockchain-supported EHR event sequences and developed a sequence diagram (shown in Figure 13). The diagram 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.

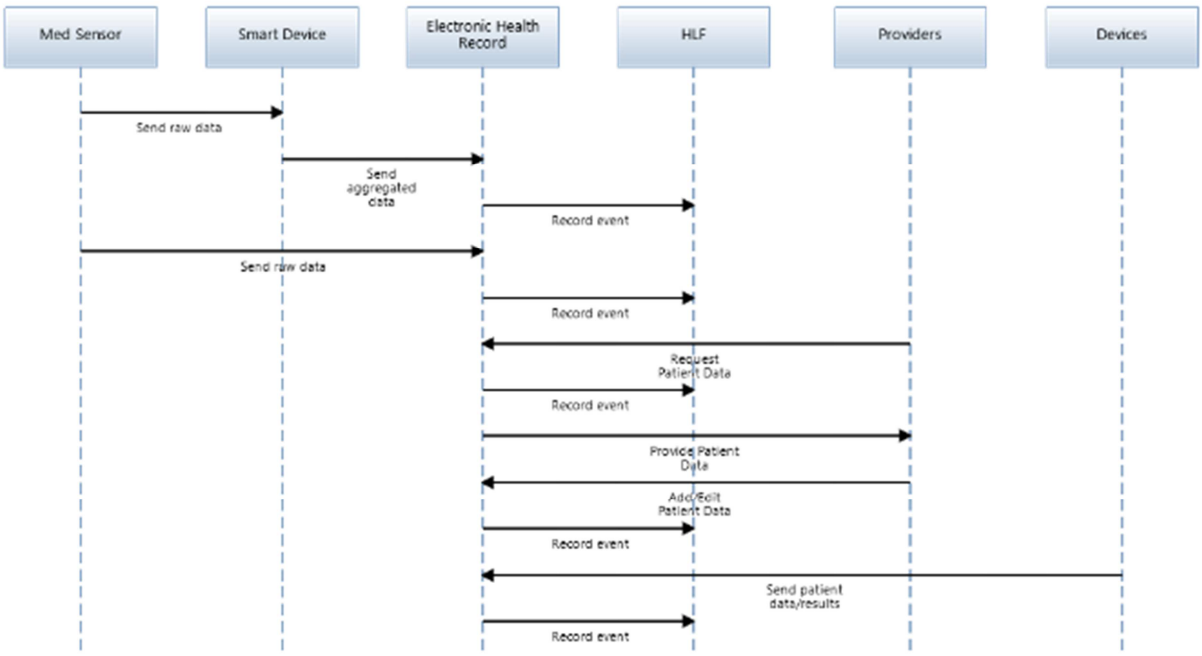

Figure 13. *Sequence Diagram for Blockchain-Supported HER.*

5.2.4. The Data Lifecycle for Medical Data

This use case demonstrates all four stages of the data life cycle. The "creating" of data happens anytime new data 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 military (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. Finally, 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.

5.2.5. Blockchain-Supported EHR Assessment

The blockchain architecture proposed for a military EHR system has some strengths and weaknesses. The team purposefully simplified the concept 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 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.

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 Veteran's Affairs 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 [70]. 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 [70]. 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.

5.3. Use Case 3 – 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 [71]. 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 [72]. Collecting this kind of intelligence is extremely important in detecting, tracking, and identifying chemical targets [71] 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 the vision of how HLF would be used 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 makes a positive detection, it enables the AI to alert a live analyst to an event that requires further investigation. This helps maximize the 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 observe-orient-detect-act (OODA) loop of decision-making in instances where a situation needs to be elevated and/ or acted upon.

5.3.1. Blockchain-Supported Chemical Defense Conceptual 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. Figure 14 illustrates the HLF blockchain architecture for the MASINT chemical defense capability.

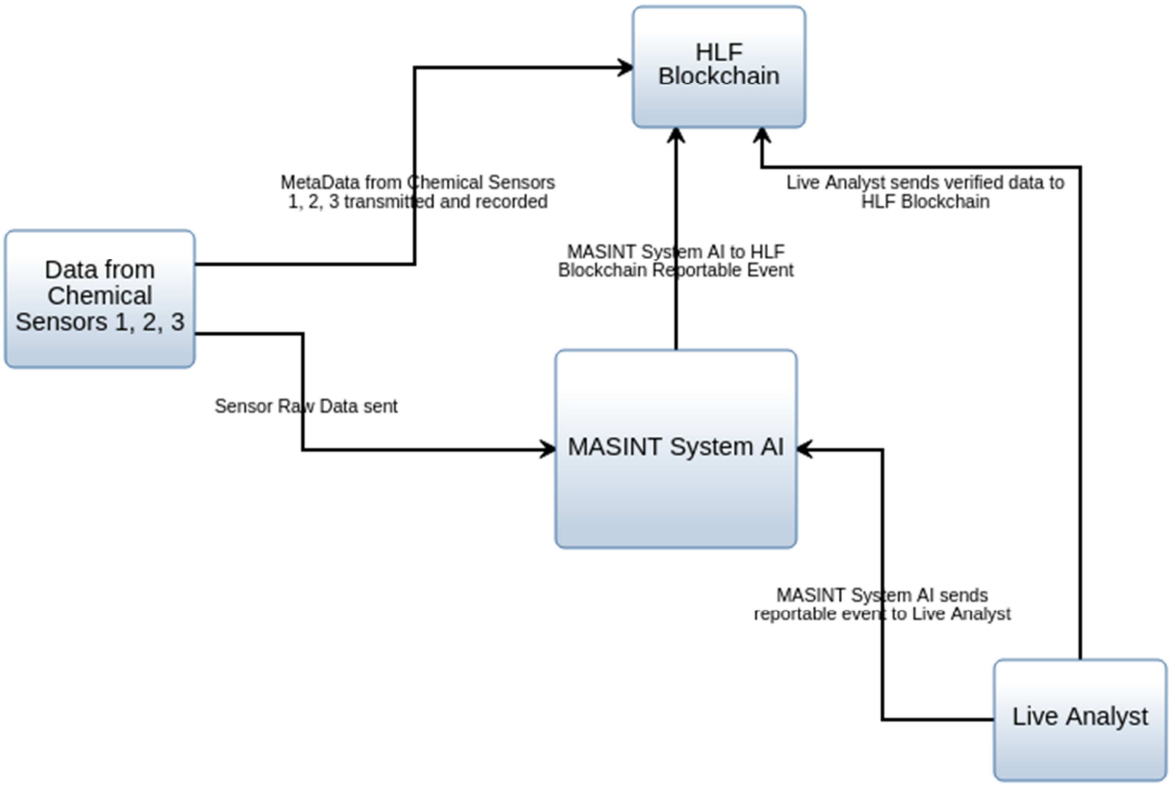

Figure 14. *Conceptual Architecture for a Blockchain-Supported Chemical Defense Capability.*

5.3.2. Blockchain-Supported Chemical Defense Event Sequence

The team studied the sequence of events for the blockchain supported chemical defense capability. Figure 15 captures a simplified series of events for this capability and illustrates how this architecture could support more complex, real-world scenarios. If any of the sensors provides 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. The sequence in Figure 15 shows the data moving from a chemical sensor to the blockchain where the metadata from those sensors' data is 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 while 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.

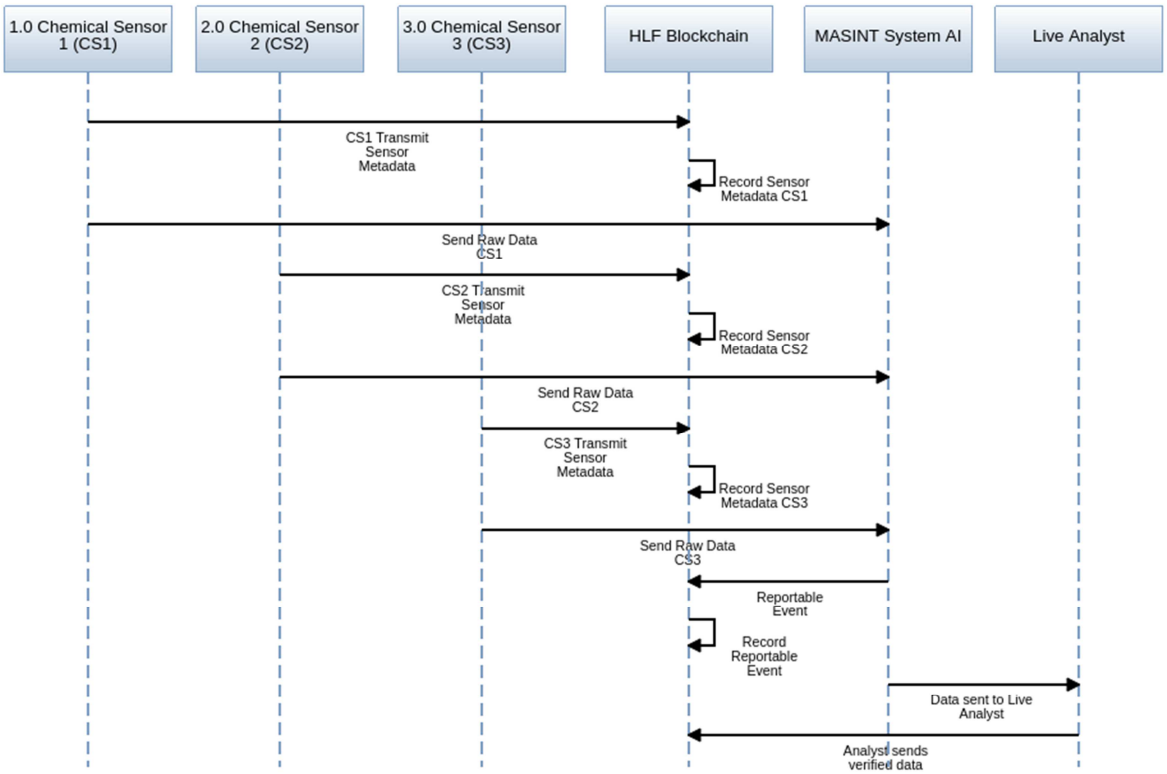

Figure 15. *Sequence Diagram for a Blockchain-Supported Chemical Defense Capability.*

5.3.3. The Data Lifecycle 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.

5.3.4. Blockchain-Supported Chemical Defense Assessment

The team's blockchain-supported 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. 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.

6. Conclusion

Warfare decision-makers at all levels are grappling with tremendous amounts of data and information in battlespace environments. Recent updates to DoD strategy documents reflect the importance of information operations in future warfare and indicate a desire to explore cutting edge capabilities to leverage data for success. Blockchain is one of the new tools that could solve several of the challenges of conventional methods of generating, storing, and transferring data throughout the battlespace environment and at the tactical edge.

This project evaluated the DoD's potential use of blockchain using a systems analysis and conceptualizing blockchain-supported solutions in three use cases at the tactical edge. The first use case explored how blockchain can facilitate secure and trustworthy data transfer to support long-range fires. The second use case studied the use of blockchain to support a robust EHR capability that is accessible at any point in the continuum of healthcare delivery. The third use case conceptualized a blockchain solution for managing MASINT data from multiple sensors to feed into AI models that identify possible chemical weapon threats.

While the team developed simplified design architectures for the three use cases, the designs demonstrated the real potential of this technology to solve or at least mitigate both current and future challenges of managing, protecting, and sharing vast amounts of data at the tactical edge. The team explored options of storing data both on and off the blockchain. The fact that these options exist shows the versatility of

blockchain and how this technology can be tailored to specific circumstances—not just across strategic, operational, and tactical contexts, but also across very different DoD mission areas to meet their unique needs. The Joint Forces of the future will need to be savvy in its generation and consumption of data. And data will be critical to securing the military advantage during crises and also during periods of competition and peacetime.

References

[1] U. S. Army Training Doctrine Command. (2018) "The U. S. Army in multi-domain operations." TRADOC Pam 525-3-1. Newport News, VA.

[2] U. S. Army Combined Army Center. (2022) "Combined arms doctrine newsletter and doctrine developer's guidance." Fort Leavenworth, KS.

[3] B. Johnson. (2019) "A framework for engineered complex adaptive systems of systems," Diss. Monterey, CA, Naval Postgraduate School.

[4] F. P. Osinga. (2007) *Science, Strategy and War: The Strategic Theory of John Boyd*, Routledge.

[5] K. Rose, S. Eldridge, and L. Chapin. (2015) "The internet of things: an overview," *The internet society (ISOC),* 80, pp. 1-50.

[6] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua. (2018) "Blockchain-empowered secure internet-of-battlefield things (IoBT) architecture." In *MILCOM 2018 IEEE Military Communications Conference*, pp. 593-598.

[7] G. Firican. (2017) "The 10 Vs of big data," *Transforming Data with Intelligence*, 8.

[8] S. Miktoniuk and O. N. Yalcin. (2021) "Open data fabric: a decentralized data exchange and transformation protocol with complete reproducibility and provenance." *arXiv preprint*, arXiv.2111.06364.

[9] 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.

[10] IBM. (2021) "How to choose the right data warehouse for AI," https://ibm.com/downloads/cas/QK7MQ7YY.

[11] K. Hicks. (2021) "Creating data advantage," Memorandum, Washington, DC: Department of Defense.

[12] T. Culpan. (2022) "The next cybersecurity crisis: poisoned AI," *Bloomberg*, last modified 14 April 2022.

[13] M. Kuzlu. (2021) "Role of artificial intelligence in the internet of things (IoT) cybersecurity," *Discover Internet of Things.*

[14] X. Li, Z. Wang, V. Leung, H. Ji, Y. Liu, and H. Zhang. (2021) "Blockchain-empowered data-driven networks: a survey and outlook." *ACM Computing Surveys* 53 (3): 1-38. https://doi.org/10/1145/3446373.

[15] A. Binlashram, L. Hsairi, H. Bouricha, and H. A. Ahmadi. (2020) "A new multi-agents system based on blockchain for prediction anomaly from system logs." In *22nd International Conference on Information Integration and Web-based Applications Services*. https://doi.org/10.1145/3428757.3429149.

[16] C. Benzaid, T. Taleb, and M. A. Farooqi. (2021) "Trust in 5G and beyond networks." *IEEE Network* 35 (3) 212-22. https://doi.org/10/1109/MNET.011.2000508.

[17] J. Clark. (2016) "What is the Internet of Things (IoT)?" IBM Business Operations Blog. November 16. https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/.

[18] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. 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.

[19] H. Karimipour and F. Derakhshan. (2021) *AI-Enabled Threat Detection*. Cham: Springer AG.

[20] C. Chen, J. Yang, W. Tsuar, W. Weng, C. Wu, and X. Wei. (2022) "Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in IIOT's application." *Sensors* (Basel, Switzerland) 22 (3) https://doi.org/10.3390/s22031146.

[21] A. Kott, A. Swami, and B. West. (2016) "The Internet of Battle Things." *Computer* 49 (12) December: 70-75. https://doi.org/10.1109/MC.2016.355.

[22] C. C. Ionită. (2020) "The 'Mosaic' warfare: a new American strategy for the future." *Strategic Impact*, 75: 25-42.

[23] R. Kumar and R. Sharma. (2021) "Leveraging blockchain for ensuring trust in IoT: a survey." *Journal of King Saud University*. Computer and Information Sciences. http://doi.org/10.1016/j.jksuci.2021.09.004.

[24] A. Reyna, C. Martin, J. Chen, E. Soler, and M. Diaz. (2018) "On blockchain and its integration with IoT – challenges and opportunities." *Future Generation Computer Systems* 88: 173-190.

[25] G. Allen. (2020) "Understanding AI technology." Department of Defense Joint Artificial Intelligence Center. https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf.

[26] M. Comiter. (2019) "Attacking artificial intelligence: AI's security vulnerability and what policymakers can do about it." Belfer Center Paper, Harvard Kennedy School.

[27] IBM. (2022a). "What is blockchain technology?" https://www.ibm.com/topics/what-is-blockchain.

[28] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. 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.

[29] G. Palaiokrassas, P. Skoufis, O. Voutyras, T. Kawaksaki, M. Gallissot, R. Azzabi, and A. Tsuge. (2021) "Combining blockchains, smart contracts, and complex sensors management platform for hyper-connected smart cities: an IoT data marketplace use case." *Computers* (Basel, Switzerland) 10 (10): 133-. https://doi.org/10.3390/computers 10100133.

[30] A. Battah, M. Madine, H. Alzaabi, I. Yaqoob, K. Salah, and R. 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.

[31] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. DeCaro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. Cocco, and J. Yellick. (2018) Hyperledger fabric: a distributed operating system for permissioned blockchain." In EuroSys '18: Thirteenth EuroSys Conference 2018, April 23-26, 2018, Porto, Portugal. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3190508.3190538.

[32] S. Mikhtoniuk and O. Yalcin. (2021) "Open data fabric: a decentralized data exchange and transformation protocol with complete reproducibility and provenance." arXiv: 2111.06364v1 [cs. DB] 11Nov2021.

[33] C. Gorenflo, S. Lee, L. Golab, and S. Keshav. (2019) "Fastfabric: scaling Hyperledger fabric to 20,000 transactions per second." arXiv: 1901.00910v2 [cs. DC] 4Mar2019.

[34] A. Baliga, N. Solanki. S. Verekar, A. Pednekar, P. Kamat, and S. Chatterjee. (2018) "Performance characterization of Hyperledger fabric." IEEE. Crypto Valley Conference on Blockchain Technology. DOI 10.1109/CVCBT.2018.00013.

[35] S. Malik, V. Dedeoglu, S. Kanhere, and R. Jurdak. (2019) "TustChain: trust management in blockchain and IoT supported supply chains." In *2019 IEEE International Conference on Blockchain*, 184-93.

[36] V. Adams, M. Alonso, W. Henry, D. Hyland-Wood, W. Jansen, V. Kodumudi, and A. Nannra. (2020) "Potential uses of blockchain by the Department of Defense." Washington, DC: Value Technology Foundation.

[37] S. B. Rahayu, N Jusoh. (2019) "Military blockchain for supply chain management." *Journal of Education and Social Sciences* 13 (1): 9-14.

[38] T. J. Willink. (2018) "On blockchain technology and its potential application in tactical networks." *Defense Research and Development,* Ottawa, Canada.

[39] A. Kendall, A. Das, B Nagy, B. Johnson, and A. Ghosh. (2022) "Increasing confidence and data availability from IoT and other sources supporting artificial intelligence and analytical tools using hyperledger fabric blockchain." Naval Postgraduate School White Paper, 2022.

[40] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni. (2019) "Blockchain's adoption in IoT: challenges, and a way forward." *Journal of Network and Computer Applications* 125: 251-279.

[41] A. Abdelmaboud, A. Ahmed, M. Abaker, T. Eisa, H. Albasheer, S. Ghorashi, and F. Karim. (2022) "Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges, and future research directions." *Electronics* (Basel, Switzerland) 11 (4): 630-. https://doi.org/10.3390/electronics11040630.

[42] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito. (2018) "Blockchain and IoT integration: a systematic survey." *Sensors* (Basel, Switzerland) 18 (8): 2575.

[43] A. Attkan and V. Ranga. (2022) "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security." *Complex and Intelligent Systems*. https://doi.org/10.1007/s40747-022-00667-z.

[44] Y. Jeong. 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.

[45] D. Draskovic and G. Saleh. (2017) "Datapace: decentralized data marketplace based on blockchain." White Paper, Datapace, http://datapace.io/.

[46] K. Moke, T. Low, and D. Khan. (2021) "IoT blockchain data veracity with data loss tolerance." *Applied Sciences* 11 (21): 9978. https://doi.org/10.3390/app11219978.b

[47] R. Xu, L. Hang, W. Jin, and D. 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.

[48] B. Gan, Q. Wu, X. Li, and Y. 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.

[49] H. Paiooh, M. Rashid. F. Alam, and S. Demidenko. (2021) "Hyperledger fabric blockchain for securing the edge internet of things." *Sensors* (Basel, Switzerland) 21 (2): 359. https://doi.org/10.3390/s21020359.

[50] J. Zhang, C. Lu, G. Cheng, T. Guo, J. Kang, X. Zhang, X. Yuan, and X. Yan. (2021) "A blockchain-based trusted edge platform in edge computing environment." *Sensors* (Basel, Switzerland) 21 (6): 2126. https://doi.org/10.3390/s21062126.

[51] R. Rahim, R. Patan, R. Manikandan, and S. Kumar. (2020) "Introduction to Blockchain and Big Data." In *Blockchain, Big Data, and Machine Learning: Trends and Applications*, edited by N. Kuman, N. Gayathri, M. A. Rahman, and B. Balamurugan. 1-23. Boca Raton: CRC Press. https://doi.org/10.1201/9780429352546.

[52] H. Kumar, M. Manu, R. Indrakumari, and B. Blamurugan. (2020) "Blockchain use cases in big data." In *Blockchain, Big Data, and Machine Learning: Trends and Applications*. Edited by N. Kuman, N. Gayathri, M. A. Rhaman, and B. Balamurugan. 111-139. Boca Raton: CRC Press. https://doi.org/10.1201/978042935246.

[53] N. Deepa, Q. Pham, D. Nguyen, S. Bhattacharya, B. Prabadevi, T. Gadekallu, P. Maddikunta, F. Fang, and P. Pathirana. (2021) "A survey on blockchain for big data: approaches, opportunities, and future directions." *arXiv.org*.

[54] G. Fareund, P. Fagundes, and D. Jeronimo de Macedo. (2020) "An Analysis of Blockchain and GDPR Under the Data Lifecycle Perspective." Mobile Networks and Applications 26 (1): 266-76. https://doi.org/10/1007/s11036-020-01646-9.

[55] A. Kott, A. Swami, and B. West. (2017) "The Internet of Battle Things." Computer 49 (12) (December): 70-75. https://doi.org/10.1109/MC.2016.355.

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

[57] S. Shetty, C. Kamhoua, and L. Njilla. (2019) "Blockchain for Distributed Systems Security." 1st edition. Newark: Wiley. https://doi.org/10.1002/9781119519621.

[58] 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.

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

[60] Hyperledger Performance and Scale Working Group (2018) Hyperledger Blockchain Performance Metrics. *https://www.hyperledger.org/learn/publications/blockchain-performance-metrics*

[61] Hyperledger (2022) "Peers." https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peer.html.

[62] U. S. Army (2021) "The Army Unified Network Plan." Arlington, VA: Office of the Undersecretary of the U. S. Army.

[63] N. Patel, U. Patel, E. Hawk II, and K. Kapadia. (2021) "Stitching the Army's Data Fabric." *Army ALT Magazine* (Fall 2021): 14-19.

[64] C. Ferris. (2019) "Does Hyperledger Fabric Perform at Scale?" IBM Supply Chain and Blockchain Blog (blog).

[65] S. Guntur, R. Gorrepati, and V. Dirisala. (2019) "Robotics in Healthcare: An Internet of Medical Robotic Things (IoMRT) Perspective." In *Machine Learning in Bio-Signal Analysis and Diagnostic Imaging* (pp. 293-318). Academic Press.

[66] L. Virgos, M. Vidales, F. Hernandez, and J. Granados. (2021) Internet of Medical Things: Current and Future Trends." *Internet of Medical Things*, 19-36.

[67] L. Elezabeth and V. 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.

[68] S. Cao, G. Zhang, P. Liu, X. Zhang and F. 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.

[69] Military Health System and Defense Health Agency. (2022) "MHS Genesis: The Electronic Health Record." Heatlth.mil, health.mil/Military-Health-Topics/Technology/MHS-Genesis.

[70] R. Rayan, C. Tsagkaris, and R. Iryna. (2021) "The Internet of Things for Healthcare: Applications, Selected Cases, and Challenges." *IoT in Healthcare and Ambient Assisted Living*, 1-15.

[71] Pre-Employment Checks. (2019) "Understanding MASINT and Its Practical Uses." Pre-Employment Checks. Last modified July18, 2019. https://www.Pre-employment-checks.com/en/understanding-masint-and-its-practical-uses/.

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