Military Intelligence Applications for Blockchain Technology

Ashley S. M. McAbee
Naval Postgraduate School
Monterey, CA, USA
asmcabee1@nps.edu

Murali Tummala
Naval Postgraduate School
Monterey, CA, USA
mtummala @nps.edu

John C. McEachen
Naval Postgraduate School
Monterey, CA, USA
mceachen@nps.edu

Abstract

In this paper, the authors review documented problems in military intelligence that appear well suited for improvement via blockchain technology. We review guidance from the literature related to determining blockchain technology applicability and propose a decision aid tailored to military intelligence perspectives. We also propose applying batch queueing theory to enable initial feasibility studies and present analysis toward the first known case study of military intelligence incorporation of blockchain technology, a project reviewing blockchain applicability to an intelligence database that stores geographic locations of units of interest.

1. Introduction

As blockchain technology's influence expands beyond the bounds of the cryptocurrency sector initially proposed by Nakamoto [1] in the Bitcoin white paper, various potential use cases for the military seem apparent. For example, work is well underway to see how it might help in additive manufacturing [2]. Another clear candidate is the military intelligence system, which comprises a wide range of networked processes, many of which stand to benefit from the immutable, decentralized ledger at blockchain technology's core. Replace *ledger* with *log*, the more common synonymous term from military vernacular, and the candidate systems nominate themselves.

Underscored by the often-discussed hype surrounding blockchain, we have reached the juncture warranting an in-depth research effort to characterize best-use cases and implementation practices for military intelligence, similar to the perspective for business leaders recently offered by the World Economic Forum (WEF) [3]. This paper will take preliminary steps toward military intelligence adoption of blockchain technology-based solutions by laying the groundwork for such research. Our technique is two pronged, focusing both on analysis of standing military intelligence problems and analysis of blockchain technology strengths to identify areas that seem well aligned. We also frame the path to adoption by proposing an approach to initial analysis of blockchain technology's applicability and potential performance before significant investment.

The paper is organized into four sections as follows: Section 2 provides brief background discussions of both military intelligence and blockchain technology. In Section 3, we review documented hurdles within the military intelligence enterprise that appear to be good candidates for blockchain technology-assisted improvement. Section 4 reviews the guidance toward applicability and feasibility determinations for potential use cases, presenting a draft decision-aid from a military intelligence perspective and proposing techniques to enable abstraction of the blockchain-based process for initial feasibility analysis. In Section 5, we describe an initial case study that should prove beneficial not only immediately to the particular case, but also to a generalized understanding of the path toward wider adoption.

2. Background

As characterized by the joint doctrine of the United States [4], the joint intelligence process "includes the organizations, capabilities, and processes involved in the collection, processing, exploitation, analysis, and dissemination of information or finished intelligence." Doctrine defines the principles of sound joint intelligence with vocabulary that appears to belay a natural pairing with blockchain technology including *networked*, *decentralized*, *shared*, *distributed*, *protected*, and *secure*. The following subsections provide broad background descriptions of military intelligence and blockchain technology to aid in forecasting the relationships between the two fields.

2.1 Military intelligence

At its core, military intelligence is similar to many business processes in that it is about collecting,

URI: https://hdl.handle.net/10125/60038
ISBN: 978-0-9981331-2-6

analyzing, and disseminating information to enable timely decision-making. Figure 1, adapted from Joint Publication 2-0, which sets the overarching doctrine for U.S. military intelligence, depicts a core tenant of intelligence tradecraft. All of the qualities of the operational environment must be winnowed down into the intelligence that truly matters for decision making on a timeline that facilitates action. To do so, the collection, processing and exploitation, and analysis and production processes must be efficient and effective at carrying only the relevant facts through to the next phase of intelligence production.

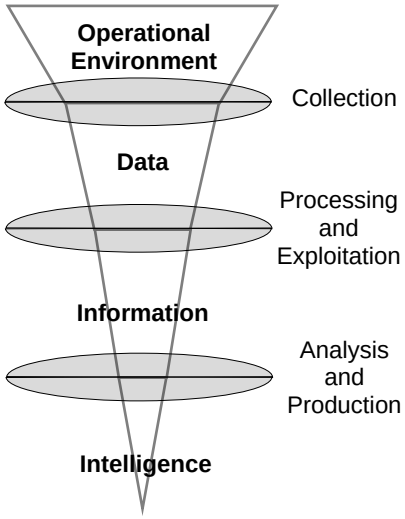

Figure 1. Relationship between data, information, and intelligence; adapted from [4]

As technology has progressed, the variety of resources that contribute to the intelligence process has grown without bound. Data sources run the gambit from manned and unmanned space, airborne, ground, maritime, and cyberspace platforms with any variety of sensors in play, creating a volume of data described as overwhelming [5]. Once collected, the data processing is growing increasingly sophisticated, with headline efforts like Project Maven working to integrate artificial intelligence and machine learning at a rapid pace [5]. Finally, delivery to the strategic, operational, and tactical decision makers requires robust and globally accessible communications infrastructure.

These lofty requirements coupled with similar requirements across the realms of the Department of Defense are the energy behind the Defense Innovation Initiative and the third offset strategy outlined by Deputy Secretary of Defense Work in 2016, which entails a comprehensive effort to advance U.S. military capability by leveraging new technology [6]. The headlines on the effort have underscored artificial intelligence and man-machine learning, but blockchain technology should be right there in the research mix, with dedicated efforts working to distinguish hyperbole from opportunity.

2.2 Blockchain technology

Blockchain technology, the framework behind the cryptocurrency boom, offers a mechanism for securely storing and adding to a body of collective knowledge in a distributed manner. Although there are variations, most blockchain implementations operate as follows, summarized and adapted from references [1], [7], [8], and [9]: Time-stamped and chronologically ordered transactions are grouped into units called blocks. The first entry in the next block in the chain will be its predecessor's cryptographic hash value, thus linking the series of blocks into a chain. That cascading cryptography prevents any single block in the chain from being altered without simultaneous updates to all subsequent blocks.

Additionally, many users store the chain in a decentralized manner so that any changes would also have to occur simultaneously at each of those locations. If differing copies of a chain begin to circulate in the network, the discrepancy is usually solved based on one of three consensus schemes: proof-of-work (POW), proof-of-stake (POS), or round robin.

In POW, each block also includes an additional value called the *nonce*, which is selected to ensure that the complete block, when hashed, will produce a value with a particular pattern, often some set number of leading zero bits. Nodes hunting for these desirable nonce values are called *miners.* When a miner uncovers a new nonce value and completes a block, the miner broadcasts that block out to all other miners who append the chain and begin work on the next block. Because the nonce discovery is computationally expensive, any discrepancies in copies of the chain, i.e., *forks* in the chain, resolve by using the longest available copy of the chain, as it represents the preponderance of available computational power and thus the consensus of the network. In a currency setting, miners are rewarded with coins upon their blocks' acceptance to incentivize participation.

In POS, the network users who hold the most stake in the network hold the power to determine consensus. In cryptocurrency applications, this stake equates to how many coins the user already holds, thus placing the most trust in those who stand to lose the most if the cryptocurrency is untrustworthy. Each user wishing to add a block to the chain is racing to find a nonce value that produces a hash within a range of values proportional to how much stake they have in the network. The more stake, the easier it becomes to find a nonce value, and the more likely it becomes that

particular user's block is the one added to the chain. If the blockchain forks, the longest chain will represent the opinion of the greatest stakeholders, thus fit the consensus definition of the POS network.

Both schemes grew in cryptocurrency based public blockchain models, so monetary incentive made sense in the absence of trust. For applications where some level of trust does exist, round robin consensus models are also in use, where nodes simply take turns adding the next block to the chain.

Blockchain categorization includes permissionless and permissioned models. Most of the discussion thus far has broadly described the original, permissionless model proposed by Nakamoto [1] in which any user can read and write to the chain. The hallmark of the model is the complete lack of required trust or central authority, with even the software of the chain itself abiding by public consensus. Permissioned or privatized blockchains maintain the shared distributed ledger but control who can read and write to the ledger in accordance with centrally applied policy. Easier mining processes usually mark permissioned blockchains because the miners are from a trusted subset of users, which may add vulnerability to the system, for example, if any of the trusted subset choose to act maliciously.

3. Potential application areas

As with any new technology, but particularly one that has achieved these significant levels of hype, there is significant likelihood for mis- and over-application in the eager, early days, as recent publications have warned [10]. To prevent such error, it is important to ensure that we pull test cases from a list of relevant problems that need solved, rather than from processes that work fine, but appear blockchain-ready. Though there are certainly other documented issues, three themes that consistently appear in recent military intelligence official statements and trade publications relate to modernizing the intelligence system in response to overwhelming volumes of incoming data [5], supporting distributed and decentralized capability [11], and ethical accountability requirements [12].

3.1 Big data

As data sources diversify, questions of the validity and accuracy of incoming data arise. Carefully implemented, blockchain technology might enable us to weed out data from mis-calibrated sensors or even deceptive adversary activity. As an initial validation is offered by Raab, et.al., [13] via a mechanism that uses blockchain technology to overcome global positioning system (GPS) spoofing. Their patent application points to a variety of other uses in areas with similar reliance on semi-public data. For maritime domain awareness applications, the Automated Information System (AIS) seems an obvious place to start.

More data, even if all validated, does not directly lead to better intelligence, though. As we automate the initial processing, presentation, analysis, and archiving of information using the sophisticated techniques adopted under Project Maven and similar efforts, our human power is free to focus on actually *understanding* information and transitioning it to meaningful intelligence [5]. Yet there remains a significant impediment to the adoption of automated learning into the intelligence process: the black-box nature of algorithm-based processes makes it difficult for some commanders to trust intelligence based on the results. Here again, blockchain technology offers potential solutions.

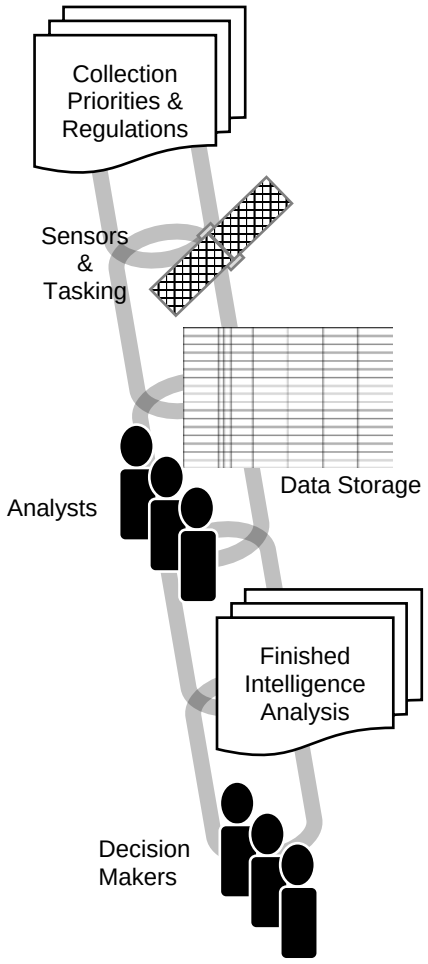

Figure 2. A blockchain technology use case for preserving the providence of tasking-to-decision processes

First, it may offer a new mechanism to trace assessments back to data, preserving a dissectible path. From the realm of academia, Extance describes how the science community is eagerly looking to this technology to "enhance reproducibility and the peer review process by creating incorruptible data trails" in scientific research [14]. In a related use case, blockchain based solutions are being incorporated into various supply chains in hopes of adding accountability and transparency to historically cloudy products such as diamonds [15].

For intelligence, the providence of both information and assessment could be preserved for the decision maker at the far end. Blockchain technology implemented to preserve data/assessment connections also significantly enhances our ability to corral assessments later found to be incorrect, preventing a false assessment from one watch floor from continuing to replicate through the products of others. The preliminary entities involved in such a system are presented in Figure 2.

Similar to the black box navigation recorders in ships and aircraft, the system would create an audit trail of the intelligence support to a given military decision by linking the initial legal and justified collection priorities to the sensor tasking, raw data collection, automated or human-powered analysis, and finished products that were presented before a decision was made. Well integrated, the system should be persistent and nearly transparent so that the records exist before we know the magnitude of the decision, as this is an environment where seemingly inconsequential decisions can have life or death consequences.

Such a system might also help us develop better ties between analysts at disparate organizations who could benefit from one another's work. The same blockchain technology will allow us to follow a single analyst's workflow in a new, more detailed way, termed "cyber profiling" by Ford, et. al., in a recent patent filing [16]. We can cross-pollinate based on patterns of intelligence analysis beyond the traditional lines of regional expertise by discerning multiple other traits from the immutable record of the analysis process.

Also picking away at the black box of algorithm-based processes, the innovative concept of *smart contracting*, which hinges on blockchain technology, has the potential to implement policy meaningfully into intelligence processes [7]. Meaningful in that we verify compliance with set policy without the need for an independent team of trusted lawyer-engineers capable of policing complex and evolving systems. Smart contracts act as a virtual inspector, checking new blocks in the chain against acceptable standards for data confidence level, data timeliness, or nearly anything else that a specific application requires.

3.2 Distributed and decentralized access

The final part of the modern intelligence system is the availability of access to both raw data and finished intelligence in real-time and on-demand from anywhere. A unit's ability to dynamically self-determine which information and intelligence is most relevant to the current mission will be critical to enabling force-multiplying dynamic employment options.

Ever evolving adversaries in cyberspace [17], however, influence our ability to adopt the easiest solutions for distributed access. Cyber vulnerability vectors increase as access points to a network increase, giving adversaries more opportunity to disrupt, deny, and degrade the intelligence process. Here again, blockchain technology offers an advantage in overcoming some cyber vulnerabilities. The sophistication, computational requirement, and number of attack vectors required to mount an impactful attack against a blockchain is withering. Especially, when we look at the opportunities to use blockchains to protect not just databases but computer software itself, extending and expanding from the additive manufacturing study previously mentioned [2], rendering it far more difficult to insert malicious code. There is also strong initial evidence that blockchain based systems can contribute to malicious node detection schemes in small scale and relatively simple network environments [18]. Such an application might be beneficial immediately in similarly small-scale sensor networks, with interesting but yet uncertain potential applications in networks of larger scale and complexity.

Finally, there is promising research into blockchain technology's ability to enable *decentralized* artificial intelligence for the first time [7]. Rather than a single super computer sharing results with many watch floors, each intelligence center contributes to the process. The primary advantage to this is that the calculations necessary for sophisticated artificial intelligence processes distribute across the computational resources of all participants, preventing the need for significant investment in a single highly capable site and redundant backups. With distribution, as long as enough other participants maintain computational capability, graceful degradation might be possible.

3.3 Ethical accountability

As distribution gives more users access to sensitive data, ethical considerations also arise. Our intelligence apparatus must be able to assure a concerned public that we are working for justifiable military intelligence purposes. Here again both the cyber behavior profile and

data-to-analysis blockchain previously discussed protect a more auditable record of intelligence activity.

Returning to the cyber profiles from Ford, et. al., [16], the patent describes a mechanism for using blockchain technology to understand every individual's unique "cyber behavior profile" by tying a complete history of "suspect" and "good" behavior to each of us, which could help prevent both the theft of credentials and insider threat from continuing to plague intelligence networks.

4. Initial system design considerations

As the hype around blockchain settles, many efforts are underway to help potential adopters decide whether blockchain technology is right for them. The following subsections present two paths to helping make that call. First, we survey guidance from literature regarding blockchain technology applicability for the points most pertinent to military intelligence applications. Second, we propose using queueing theory to do initial feasibility analysis to ensure blockchain technology is capable of meeting system performance requirements.

4.1 Military intelligence-specific guidance

We surveyed seven examples of guidance regarding blockchain applicability for points that would need to be included, expanded, or deleted in our draft framework tailored for military intelligence use [19],[20],[21],[22],[23],[15],[3]. Although vocabulary varied, there were several dominant considerations that most of the authors included, as tallied in Table 1.

Six of the seven models focus on identifying problems for which blockchain in *not* well suited by offering disqualifying criteria or a flow chart with many ramps toward disqualification. At this early juncture, for our models, we have made efforts to balance avoidance of false application to problems not well matched to distributed ledger solutions with a desire to be flexible enough to explore new potential. As such, the key mandatory quality we have identified at this juncture is that the process must be collaborative in nature, which many of the authors filed under *shared control*. One example of flexibility in potential employment came from the model put forward by Peck [19], which suggests that even in the presence of other disagreeable

Table 1. Trends in specific consideration points regarding blockchain applicability, highlighted columns indicate those of particular interest in military intelligence applications

				Problem			*Transaction*					*Participant*					*Solution*				*External Factors*	
Author	Sector	Type (C: Criteria, F: Flow Chart)	Year	Solvable without Blockchain	Intermediaries	Centralization	Rate	Size/Data Volume	Digital Nature	Privacy Expectations	Strict Immutability Required/Possible	Interdependency	Quantity	Shared Control	Integrity Motivations	Trust Level	System/Software Control	Stand-Alone System	Current Capability	Permission Type	Likelihood of Attack	Regulation Compliance
Greenspan [19]	Blockchain Development	C	15	X	X	X						X	X	X		X				X		
Birch, Brown, Parulava [20]	Finance	F	16										X	X	X					X		
Meunier [21]	Blockchain Development	C	16		X		X	X		X	X		X	X		X	X	X				
Lewis [22]	Blockchain Development	C	17		X	X						X		X								
Peck [23]	Electrical Engineering	F	17	X			X			X			X			X	X			X	X	
Wüst-Gervais [15]	Computer Science	F, C	17		X	X	X						X			X	X			X		
Mulligan [3]	Finance	F	18		X		X	X	X	X	X			X	X	X	X		X	X		X

factors blockchain technology may be worth considering in cases where the database is likely to be attacked, pointing to the previously discussed potential for blockchain technology to help overcome cyber vulnerabilities related to centralized services and single points of failure. This is of particular interest to military intelligence where some systems must actually be optimized for performance in the worst case, wartime scenario when cyber, electromagnetic, and physical attacks attempt to disrupt system operations as this is when they will be needed most. Thus, for critical functions, it can be worth investigating new technology enhancements even when requirements are currently met by more established technology.

To expand on this point for our purposes, we suggest careful consideration of whether the mitigation is capable of enabling the overarching process. For example, if distributed access is partially cut off or partitioned in a blockchain based system, the blockchain might continue to operate but would fork in each of the isolated networks. Although resolution is possible upon full system restoration, the implications of such forks in context of the service the ledger provides matter. It is not enough to give users the appearance of system durability during attack without the ledger actually continuing to enable the intended process.

The next consideration relates to how the collaboration unfolds. The literature highlights that optimal blockchain employment is in database systems with strong interactions or interdependencies between entries, as in the cryptocurrency that changes hands during a transaction. We highlight this to help intelligence system designers think about how a system of interest might be abstracted into a series of interrelated transactions and how that might help solve a performance or reliability issue.

Many of the models also attempt at least a preliminary handling of blockchain permission models so that if blockchain is assumed to be applicable, the a recommendation is given as to which permission model best fits a given problem [21]. Leveraging the advice given, we broadly discard the permissionless blockchain model for military applications as a fully public shared ledger has no obvious use in intelligence processes.

We absorbed both of the types of permissioned models given in the taxonomy by BPP, as there are likely to be both the permissioned and double permissioned applications [21]. For example, a raw intelligence data collection database, which takes input from a wide variety of sources and sensors, results in shared integrity contribution by all users while finished intelligence analysis databases are accessed by many, with the integrity maintained by only a few deputized experts.

Other considerations that carry over and even gain emphasis in a heavily hierarchical system like the military are the considerations of how chain of command and regulation impact the ability to “turn over” certain system controls to a decentralized service. Smart contracts may offer a mechanism for overcoming apparent disconnects, but it is still an important consideration even from the earliest design phases. If decentralization is not congruent with applicable command philosophy, i.e., the central figure in charge of the process wants to retain complete control, blockchain technology may not be the path to problem solving.

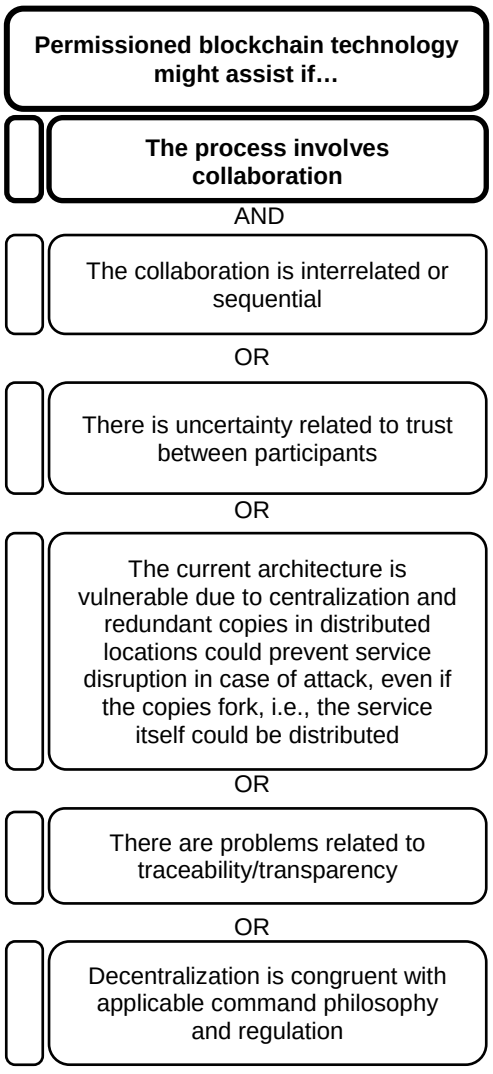

Figure 3. Critical factors in determining when blockchain technology might apply to military intelligence processes.

Applying these basic adjustments as a lens, we propose the check list in Figure 3 to military intelligence process owners considering adoption of blockchain technology. If a system meets the first, mandatory tenet identified in bold and at least one of the others, it may be a reasonable candidate for a permissioned blockchain technology model. It represents a draft that will continue to evolve over the course of research.

Figure 3 is qualitative in nature. As research continues, we will pursue more quantitative measures to understand the specific tipping points in various factors including network overhead, computational requirements, and system robustness. The next section describes our effort to move toward that quantitative analysis.

4.2 Feasibility analysis via batch queues

To aid with initial system design, it is helpful to abstract above the blockchain, examining how it will fit into the wider system model. We propose applying batch queueing theory to understand how the blockchain-based portion of a process will perform. In the subsequent discussion, we will follow standard queueing notation, A/B/X, wherein A denotes interarrival-time distribution, B denotes service-time distribution and X denotes the number of service providers. Essentially, the blockchain-based process is a black box that accepts incoming transactions and performs the service of incorporating those transactions into a block.

All blockchain processes will be A/B/1 processes, as only a single block of the chain generates at once. Even if multiple nodes build on blocks in parallel, the overall system will only keep one of these blocks as forks are resolved. Further, because incoming individual data join the chain as a batch, all blockchain processes will be $A/B^Y/1$ processes with the superscript Y denoting that service is conducted in batches of some size. Working from queueing theory, we can begin to understand the relationship between transaction arrival rate and block generation rate, observing how various tradeoffs in encryption complexity, block size, data latency, and other factors will affect the process.

As an example, because the POW difficulty alters in Bitcoin to maintain a constant block creation rate, Kawase and Kasahara [24] make a strong case for modeling Bitcoin as an $M/G^B/1$ queueing service. In this case, Bitcoin transaction inter-arrivals are exponentially (M) distributed, as expected with such a large system of independent actors. Bitcoin service rate is generally distributed (G), parametrized by the set maximum block size, B, and the efforts to maintain constant block creation rates.

Breaking apart intelligence processes, many also have exponentially distributed inter-arrivals, particularly true in the case of persistent sensors. In some cases, because of intermittent sensor availability, connectivity, or event-driven reporting, data instead arrive in bursts, requiring the system to handle widely varying arrival rates of limited predictability.

Borrowing from Bitcoin practices, we remark that controlling a combination of block size and block creation rate will also make sense in many intelligence applications. First, these factors enable system designers to ensure that data is added to the chain with no more than an acceptable maximum delay, even during periods of unusually low activity. Further, these factors make network requirements more predictable to ensure that blockchain participants are equipped to handle the increased communication load necessary to participate in the peer-to-peer network used for transaction broadcast and block synchronization. This becomes especially important in military applications where communications networks often need to be flexibly able to operate in intermittently denied and degraded environments. It also makes computational requirements more predictable as the expected block size and generation rate will give us solid footing for understanding the cryptographic load the system will need to support, though this becomes less important if we depart from a POW model.

As such, both $M/G^B/1$ and $G^B/G^B/1$ systems are likely to fit many intelligence-related blockchain technology solutions. Understanding of both models is likely to serve analysts well in initial feasibility assessments for proposed blockchain technology systems.

5. Preliminary analysis

For the near term, the primary objective is to understand the hurdles specific to military intelligence adoption of this technology to ease wider adoption as more and more applications are developed. As the first known case study toward military intelligence adoption of blockchain technology, we are evaluating how it might improve an order of battle database that U.S. Pacific Fleet naval units use for situational awareness and the development of intelligence briefings. The research hopes to emphasize how blockchain technology makes this and similar systems less reliant on centralized data solutions.

Generally, order of battle databases hold the latest available geolocation of air, surface, and subsurface units of interest to enable analysts to monitor changes in traffic patterns and understand the disposition of current threats. The data arrives from a multitude of intelligence sources, but for feasibility analysis we propose using the

Automated Identification System (AIS) as a starting point for system design because the data is publicly available and thus friendlier to academic research than other intelligence data.

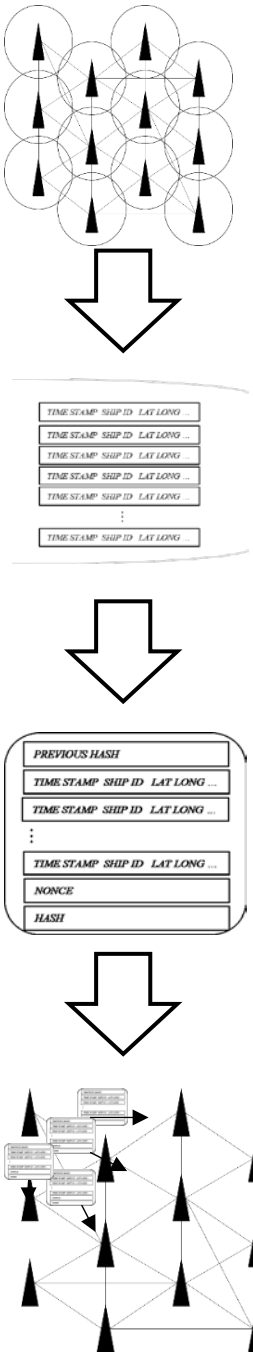

Figure 4. Nominal blockchain-based archival system for AIS reports

AIS was developed to provide ship operators with integrated displays of all ships within their very high frequency (VHF) radio range to improve safety. It is an especially interesting starting point for analysis of blockchain applications to intelligence because it represents a system where individual reporting units have no reason to trust one another, yet the majority of ships participate cooperatively anyway, much like the trust relationships that exist (or not) in cryptocurrency applications.

The system is now required on almost all vessels by international regulation. Each vessel makes a 256-bit position report every 2-30 seconds depending on vessel class. Based on the AIS communications standard promulgated by the International Maritime Organization, the system must support reports at a minimum rate of 2,000 per minute, yet based on VHF range limitations, any one station usually sees a much lower report volume [25]. For a station in San Francisco harbor, for example, an average of 132 reports per minute were observed during the first week of June 2018 with reception distance averaging 8 nautical miles [26].

As an experimental model, we will explore a blockchain-based archival system with 12 participants located in an area of significant traffic flow such that while each station may observe lower rates, the combined traffic interarrival rate to the blockchain-based process can be assumed to be a Poisson random variable with an expected value of 25 reports per second. With no prioritization applied, reports are simply added to the next block in order of arrival as soon as B reports are in the queue, resulting in a batch-based service model following the $M/G^B/1$ queueing model. Figure 4 offers a simplified diagram of the process. The batch processing rate must maintain an overall average above 25 reports per second for system stability, which is well within permissioned blockchain performance capability quantified by Pongnumkul, et. al. [27]. Thus, the block size and block creation rate boundaries begin to take shape since together they will drive overall system service rate.

With preliminary analysis in hand, the next step in the research will be applying the existing body of $M/G^B/1$ research to this model to help quantify the trade-offs and design decision points in system performance.

6. Conclusion

Blockchain technology presents an interesting opportunity to solve some of the well documented problems in military intelligence systems. By drafting guidance toward applicability and feasibility studies, we hope to drive successful exploration of well-matched use cases both in our own research efforts and those in fields with similar priorities. This paper represents the

earliest of progress in a wider and more systematic review of blockchain technology. As such, we present our research approach and justification, with much more to follow in subsequent works as we gain headway in understanding and eventually quantifying the specific impediments and benefits to incorporation of blockchain technology in military intelligence systems.

7. References

[1] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: Jun. 13, 2018].

[2] McCarter, John, "DON Innovator Embraces a New Disruptive Technology: Blockchain," *Naval Innovation Advisory Council*, Secretary of the Navy, June 2017. [Online]. Available: http://www.secnav.navy.mil/innovation/HTML_Pages/2017/06/BlockChain.htm [Accessed: Jun. 13, 2018].

[3] Mulligan, C., J. Z. Scott, S. Warren, and J. P. Rangaswami, "Blockchain Beyond the Hype: A practical framework for business leaders," white paper of the World Economic Forum, April 2018.

[4] Joint Chiefs of Staff, *Joint Publication 2-0 Joint Intelligence*. Washington, DC: Department of Defense, 2013.

[5] Pellerin, C., "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," U.S. Department of Defense, 21 July 2017. [Online]. Available: https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/ [Accessed Jun. 13, 2018].

[6] Work, B., "Remarks by Deputy Secretary Work on Third Offset Strategy," Brussels, Belgium, Address to North Atlantic Treaty Organization, 28 April 2016.

[7] Asharaf, S. and S. Adarsh, *Decentralized Computing using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities*, Hershey, Pennsylvania, IGI Global, 2017.

[8] Tosh, D.K., S. Shetty, X. Liang, C. Kamhoua and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, New York City, NY, 2017, pp. 469-474.

[9] Yaga, D., P. Mell, N. Roby, and K. Scarfone, "Draft NIST Interagency Report: Blockchain Technology Overview," *National Institute of Standards and Technology*, January 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8202/draft [Accessed: Jun. 13, 2018].

[10] Cachin, C., "Blockchains and Consensus Protocols: Snake Oil Warning," *2017 13th European Dependable Computing Conference (EDCC)*, Geneva, 2017, pp. 1-2.

[11] Rowden, T., P. Gumataotao, and P. Fanta, "Distributed Lethality," *Proceedings of the U.S. Naval Institute*, Jan. 2015, pp. 18-23.

[12] Vrist Ronn, K., "Intelligence Ethics: A Critical Review and Future Perspectives," *International Journal of Intelligence and Counterintelligence*, 29, no. 4, Oct. 2016, pp. 760–784.

[13] Raab, C. W., J. W. Glatfelter, and K. C. Hill. "On-Board Backup and Anti-Spoofing GPS System," U.S. Patent Application No. 20170357009, Jun. 8, 2016.

[14] Extance, A, "Could Bitcoin technology help science?," *Nature*. 18 Dec 2017. [Online]. Available: https://www.nature.com/articles/d41586-017-08589-4 [Accessed: Jun. 13, 2018].

[15] Gervais, A. and K. Wust. "Do you need a Blockchain?," Cryptology e-Print Archive of the International Association for Cryptologic Research, 2017/375. [Online]. Available: https://eprint.iacr.org/2017/ [Accessed: Aug. 29, 2018].

[16] Ford, R. A., B. L. Swafford, C. B. Shirey, M. P. Moynahan, and R. H. Thompson, "User behavior profile in blockchain," U.S. Patent no. 9,882,918, Sep. 29, 2017.

[17] Ferdinando, L., "U.S. Faces Evolving, Emboldened Adversaries in Cyberspace, Officials Warn," *Department of Defense*, Apr. 11, 2018. [Online]. Available: https://www.defense.gov/News/Article/Article/1491086/us-faces-evolving-emboldened-adversaries-in-cyberspace-officials-warn/ [Accessed: Jun. 13, 2018].

[18] Strobel, V., E. C. Ferrer, and M. Dorigo, "Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario," in *Proc. Of the 17th International Conference on Autonomous Agents and Multiagent Systems*, Stockholm, Sweden, Jul. 2017.

[19] Greenspan, G., "Avoiding the Pointless Blockchain Project," Nov. 22, 2015. [Online] Available: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/ [Accessed: Aug. 29, 2018].

[20] Birch, D.; R. G. Brown and S. Parulava, "Towards ambient accountability in financial services: Shared ledgers, translucent transactions and the technological legacy of the great financial crisis," *Journal of Payments Strategy and Systems*, vol. 10, no. 2, pp. 118-131, Mar. 11, 2016.

[21] Meunier, S. "When do you need blockchain? Decision models." [Online]. Available: https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1. [Accessed: Aug. 29, 2018].

[22] Lewis, A., "Avoiding blockchain for blockchain's sake: Three real use case criteria," *Bits on Blocks*. Jul. 24, 2017. [Online]. Available: https://bitsonblocks.net/2017/07/24/avoiding-blockchain-for-blockchains-sake-three-real-use-case-criteria/ [Accessed: 29 Aug 2018].

[23] Peck, M. E., “Blockchain world - Do you need a blockchain?," in *IEEE Spectrum*, vol. 54, no. 10, pp. 38-60, Oct. 2017.

[24] Kawase Y., S. Kasahara, “Transaction-Confirmation Time for Bitcoin: A Queueing Analytical Approach to Blockchain Mechanism,” *Queueing Theory and Network Applications 2017*, Qinhuangdao, China, 2017, pp 75-88, in *Lecture Notes in Computer Science*, vol. 10591. Springer; Cham, Switzerland.

[25] Automatic Identification System overview. *U.S. Coast Guard Navigation Center*. [Online]. Available: http://navcen.uscg.gov/?pageName=AISmain [Accessed: Jun. 13, 2018].

[26] MarineTraffic.com, San Francisco Bay Area OAK – Station 1563, [Online]. Available: https://www.marinetraffic.com/en/ais/details/stations/1563 [Accessed: Jun. 8, 2018].

[27] Pongnumkul, S., C. Siripanpornchana and S. Thajchayapong, "Performance Analysis of Private Blockchain Platforms in Varying Workloads," *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, Vancouver, BC, 2017, pp. 1-6