Securing Distributed Simulation and Training using Blockchain Technologies

Shawna Boucher, Mohammed Elshennawy, Spencer Frazier, Joshua Jacobs, Heather Kurtz, Benjamin Noble
Lockheed Martin Corporation (RMS)
Orlando, Florida
shawna.d.boucher@lmco.com, mohammed.elshennawy@lmco.com, spencer.j.frazier@lmco.com, joshua.m.jacobs@lmco.com, heather.kurtz@lmco.com, benjamin.noble@lmco.com

ABSTRACT

Modern simulations and distributed training methods such as BYOD (Bring Your Own Device) pose unique challenges of security and data management. Problems in the space include: maintaining a common and standardized ledger of trainee data, securing individual BYOD hardware, securing application communications, and securing delivery of training content.

Using blockchain technology can address these challenges. Blockchain technology is defined as a distributed ledger of transactions made practically immutable by algorithmic consensus of encrypted data across multiple nodes on the network. It is possible to create blockchain records of simple transactions or advanced, Turing-Complete, computation (smart contracts). Smart contracts are open, trustless pieces of code which are deployed in a distributed system and computationally verified. Combining these smart contracts with advances in homomorphic encryption and cryptographic signing would allow system designers to address the aforementioned challenges in flexible ways appropriate to the training domain.

There are drawbacks and limitations to consider with blockchain technology as well. An immutable ledger comes with a large data footprint due to ever increasing historical data. Participating anonymously is often considered an important feature of blockchain; however, this anonymity may not be desired for access-controlled environments. Energy requirements with a traditional blockchain can be significant. There are several emerging techniques to address these issues such as ledger pruning, closed access blockchains and energy efficient algorithms.

We'll explore these technologies in greater detail and then review the existing implementations and assessments of these techniques along with their drawbacks to validate their potential. Design recommendations will be provided to existing training solutions based on blockchain technology and finally, we'll audit our recommendations to quantify the value these technologies would add in terms of security and auditability.

ABOUT THE AUTHORS

Shawna Boucher is a senior lead mechanical engineer at Lockheed Martin working in flight simulation. She has supported multiple programs/projects from conceptual design phase through production. She also has experience with systems integration and test at Lockheed Martin with software and hardware flight training devices. She has over six years of experience in mechanical design, systems integration and test, manufacturing, quality, and aerospace engineering.

Mohammed Elshennawy is a staff specialty engineer at Lockheed Martin focusing on system safety, Reliability/Maintainability/Availability (RMA) and Logistics/Life Cycle Cost (LCC) at Lockheed Martin. He has experience working software safety for maintenance management systems and has been leading multiple Failure Reporting and Corrective Action System (FRACAS) efforts at Lockheed Martin since 2015. He has 8 years of experience working simulation and training.

Spencer Frazier is currently a senior lead software engineer at Lockheed Martin working on human performance-based assessment, emotionally intelligent agents, trustless federated learning, and deep compositional frameworks. He has spoken and demoed at I/ITSEC and AAMAS with publications in AAAI and AIIDE for work studying multi-agent systems. He has had research sponsored by AFRL, ONR, NSF and DARPA.

Joshua Jacobs is a Software Engineer Sr. at Lockheed Martin with over six years of experience in flight simulation. He's developed simulations at various qualification levels for over 60 different aircraft varieties in 16 different countries. He currently supports a United Kingdom program as a software lead. With a background in game development, he strives to bring modern technology and the concept of gamification to the simulation industry to bring about the next generation of training and simulation.

Heather Kurtz is a flight simulation test and design engineer and is currently a senior lead systems engineer at Lockheed Martin. She has developed, tested and trained in the flight simulation domain for over 9 years and specializes in bringing system engineering processes into Lockheed's simulation and training programs. She has been studying and researching blockchain technology for the past year.

Benjamin Noble is a Senior Software Engineer at Lockheed Martin and has been working in simulation and training for over 5 years. During that time, he has served as Lead Software engineer, technical SME, and customer liaison. He has been published in genetic algorithms research. He has also spent considerable time in research of blockchain technology and participated in beta testing of the BitShares blockchain.

All six are currently members of the Lockheed Martin Rotary and Mission System (RMS) Advanced Technical Leadership Program (ATLP) from Orlando, Florida.

Securing Distributed Simulation and Training using Blockchain Technologies

Shawna Boucher, Mohammed Elshennawy, Spencer Frazier, Joshua Jacobs, Heather Kurtz, Benjamin Noble
Lockheed Martin Corporation (RMS)
Orlando, Florida
shawna.d.boucher@lmco.com, mohammed.elshennawy@lmco.com, spencer.j.frazier@lmco.com, joshua.m.jacobs@lmco.com, heather.kurtz@lmco.com, benjamin.noble@lmco.com

CHALLENGES IN THE TRAINING DOMAIN

In the modern simulation and training era, demand has significantly risen for data with quicker access, improved security and sustained reliability to power an ever-increasing variety of use cases. Bring Your Own Device (BYOD) is an emerging trend (French, et. al 2014) across the spectrum of both government and commercial network types but poses specific challenges in the training domain. When accessing training data through consumer purchased hardware, measures are required to be taken to ensure proper access is granted to that data. Specialized Training, regardless of classification, can be sensitive in nature and therefore access by unintended parties is highly undesirable. Security of current and archived data must also be considered so that personally identifiable information is not accessed by third parties.

Learning management systems have their own set of familiar challenges. Turnkey training programs require precise resource management while also having the flexibility to accommodate a varying number of participants as the program continues over time and the need to accommodate changes in training demands due to schedule changes, varying trainee progress and asset availability arises. When training with the intent to certify, accurate records keeping is necessary to ensure students have been properly trained before being placed in a working environment with safety concerns for active users and the ability to address the required training throughput. An example of this would be aircraft maintenance. An aircraft maintainer should be properly trained and certified before being requested to make repairs on a system where even the simplest mistake has the potential to jeopardize lives.

Aircraft maintenance data itself has an impact in the training domain and presents challenges to overcome. Due to the safety critical nature of many aircraft parts it is important to ensure that maintenance alerts are being raised at the appropriate thresholds and that all maintenance actions are recorded real-time and traceable to all parts. This data would need to be recorded, uploaded and monitored real-time using the most efficient, traceable and reliable methods to ensure fleet readiness and maximize safety. Aircraft maintenance data can be of a considerable size. With the volume of data available, machine learning techniques can be used to improve prediction of part failures (Wade, et. al 2015). In addition, it may be possible to use this data to provide improved and focused training to the aircraft maintainers.

With all these challenges in the training domain, modern techniques and the latest technology can be used to improve efficiency, security, and reliability. One of these emerging technologies that we believe can be leveraged to significant benefit is blockchain. Blockchain has just begun to be researched in earnest and has been applied to many use cases; however, blockchain has yet to be significantly utilized in the training domain. With a technology that has been as disruptive as blockchain, we believe that it is important to consider its potential utility.

INTRODUCTION TO BLOCKCHAIN

Blockchain was introduced by Satoshi Nakamoto (Nakamoto, 2008) in a published whitepaper. It is a digital ledger in which transactions are recorded chronologically and publicly. Blockchain is not simply a database for information but instead a transaction network that can be used to transfer data of varying sizes. Once a transaction request is submitted it is broadcasted to a group (of variable size depending on the transaction) or network of participants. From there the transactions are verified across the network and the data is pushed forward creating a new “block” or consensus representing that transaction. Once a block is verified the transaction is complete. The blockchain method

provides a simple, secure, and traceable source in which to request, transmit and validate digital data. As the transactions are processed they are authenticated through various network consensus methods.

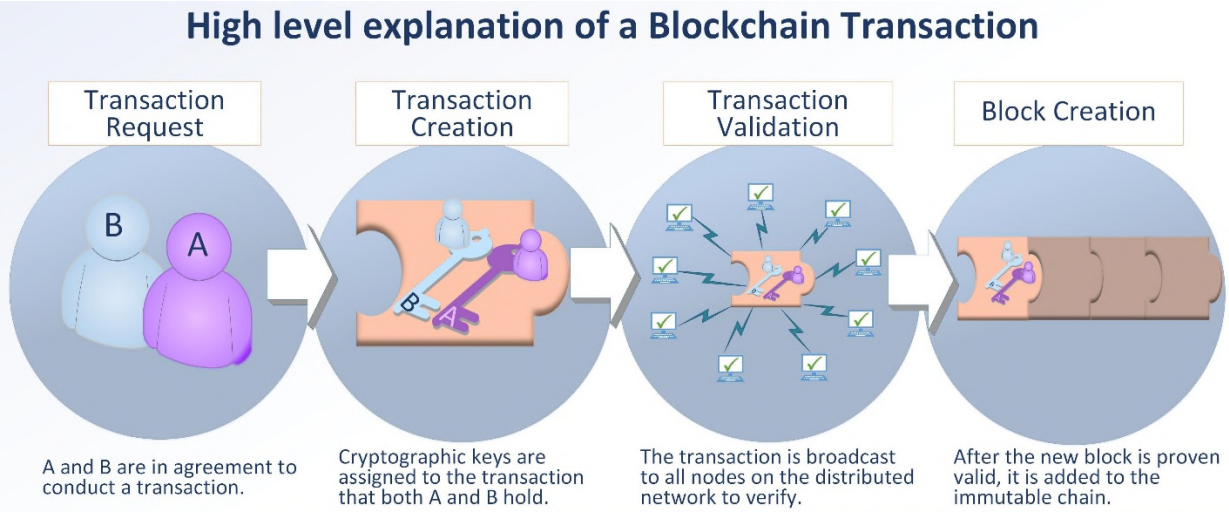

Figure 1. How a simple Blockchain transaction works.

A variety of blockchain structures can be used to allow data to be viewed during the transaction at different security levels based on requirements established within the group. The structures include: public, encrypted, anonymous, and programmable. The public structure allows all parties involved to have complete access to the data while the encrypted structure can be secured so that the ledger can be viewed only as allowed by the original author. The anonymous blockchain protects the identity of all participants so that individuals cannot be identified based on their inclusion in the group. In addition to these variety of blockchain structures there are some aspects which are common to all blockchains. Consensus is one of the main innovations of blockchain. To reach consensus all participants must agree and validate the entries in the ledger. Once consensus is reached immutability can be achieved. Data entries are preserved and carried forward to the next verification participant. Using mathematical algorithms, the history of data cannot be changed. Programmable blockchains or smart contracts allows an autonomous code or script to run to validate the information--this may be beneficial when considering automation of the transactions. Smart contracts would allow for infinitely configurable, consensus-based distributed computing; they work by using a predefined set of terms (the "contract") that acts as the ledger; once a triggering event is hit—this may be a variable like price or an expiration date—the contract executes itself according to the predefined set of terms. For more information on smart contracts and blockchain see Kosba's work on the Hawk smart contract system (Kosba, et al 2016).

IDENTIFYING ADVANTAGE AND DISADVANTAGES OF BLOCKCHAIN

Blockchain technology is a powerful, decentralized, immutable, ledger of data. This leads many to inquire, what are the advantages of using blockchain technology over a traditional database solution?

There are a few key benefits of using decentralized and smart contract-based databases over a standard, centralized database. The main benefits distinguishing a blockchain from a normal database are the pre-defined rules on how to put data into the database, blockchain's immutability, traceability and accountability of transactions, it's replicability and availability. Blockchain is an immutable audit trail where trust is placed on the technology and its processes instead of an individual, governance or corporation.

Used in conjunction with other technological advances, blockchain technology utilizing smart contracts, will allow for more efficient decision making based on a large amount of reliable data from an immutable, distributed ledger. Although blockchain has the potential to be a foundational technology to future developments, the technology is still in its infancy and with that, problems and confusion exist and will remain for a considerable amount of time. While

our portrayal of blockchain presents an emerging, opportunistic and potentially disruptive technology, a counter conversation needs to be discussed, as well as potential risks identified.

Emerging and Foundational Technology

As with any new and quickly emerging technology, there are several risks to consider while the technology is growing from infancy. True blockchain-led transformational technology applied to any domain, and specifically simulation and training, is still many years away (Iansiti, 2017). Every day challenges and lessons learned are building the knowledge base of how to use this technology effectively. While the impact blockchain will have is expected to be significant, it may take decades for blockchain to influence the economic and social infrastructures in place. Trust must be developed in a system that is touted as "trustless." To say that a system is trustless means that there is no trust needed in third parties. All central authorities have been replaced by autonomous and verifiable code. It will take time for convincing proofs to emerge that these systems truly do not require trust.

Blockchain has recently been getting a lot of attention in the media and tech communities are claiming that blockchain is over-hyped leading those outside of the community to believe it can solve all technical problems (Iansiti, 2017). Based off this, pre-development and design analysis must be thorough to ensure a blockchain implementation is appropriate per the use case and there is not a push to implement new technology when a secure database is sufficient.

Resource Usage

As with most advancements where potential is identified, the blockchain technology is rapidly growing. Because of the growing community, we have already discovered solutions for blockchain that were once unachievable. One of those identified is the utilization of the resources. Traditional Blockchain Consensus revolved around a process called mining. Transactions are recorded into a blockchain, with consensus achieved by a proof-of-work system (mining). This proof-of-work system inflicts a significant computational cost on network participants for maintaining the blockchain (The World Bank, 2017). In this, users must dedicate vast amounts of computing resources to verify their transactions. Not only does this require massive amounts of computational resources, it also has effects on performance as well as downstream effects such as an increased carbon footprint.

Opportunities are evolving, and new consensuses methods have been identified to remedy this issue. One of the solutions to this is called Proof-of-stake. For an example of this see Kiayias' work on the Ouroboros method (Kiayias, et al 2017).

Association to Cryptocurrencies

The word "blockchain" cannot be discussed with novice individuals without a mention of Bitcoin and cryptocurrencies. Blockchain technology started as the innovation that powered the cryptocurrency Bitcoin. Being the first well known and heavily publicized application of blockchain, Bitcoin quickly made blockchain a tech buzz word. With that positive push from Bitcoin, there has been an influx of industries looking to advance blockchain technology and subsequently the knowledge and training of blockchain outside of cryptocurrency has been advancing exponentially. On the negative side, massive fluctuations and extreme volatility in the cryptocurrency market and the negative publicity associated with cryptocurrency has caused recurrent hysteria and the spread of misinformation. Due to the lack of knowledge that Bitcoin and blockchain are not synonymous, the blockchain reputation and discussion can often be seen parallel to that of Bitcoin.

Design and Development

Architecture design and software development of a blockchain has proven to be challenging. As with any new technology, the community has not developed consistent standards. In addition, development must be a slow, well-thought out process that creates a dependable system to ensure all databases are consistent. For a profit-driven business where results are expected immediately, the development time could result in loss of revenue. However, forward thinking companies that can afford to push innovation, will benefit due to proper software development standards implemented instead of pushing "fix issues post-production" applications. There are some early attempts at defining a standard, notably the Hyperledger framework started by the Linux foundation (https://www.hyperledger.org) and

advanced by the Hyperledger Fabric system developed by IBM (Androulaki, et al 2018). These early attempts have only just started gaining traction and will take time to determine if they will be adopted on a wide scale.

Immutability

Immutability can be defined as something that is unchangeable. When we apply this definition to the context of blockchain technology, immutability refers to the unalterable nature of all data that is included in a blockchain. For example, once a transaction and all its corresponding data has been recorded on a blockchain, it can no longer be changed. This has huge implications in terms of the inability to change or hack data. To the inverse of that, blockchain just proves the data has not been tampered with, it does not prove that the data was correct at the point of entry.

Anonymity

Participating anonymously is considered an important feature of blockchain because of the peer-peer network technology with each user acting as a node on the network. The core technology behind blockchains are the nodes working together anonymously to validate the transitions, removing the need for a centralized authority. However, this means that all nodes participating on the blockchain network, have visibility to all previous transactions that have been stored in a block on the chain.

When working in secured simulation and training environments, especially those that allow for BYOD, anonymity and visibility to all data may not be ideal or legal. To remediate this dilemma, blockchain technology can currently be developed and utilized in two distinct ways; public blockchains (also referred to as unpermissioned) and private blockchains (also known as permissioned).

In public blockchains, such as Bitcoin, all participants engaging in the network have full visibility to see all transactions. In contrast, private or permissioned blockchains are closed and only accessible for a those chosen to enter the network will have permissions to engage in the blockchain. The transparency is therefore only given for permissioned participants and are more beneficial for those environments with sensitive or classified data.

Bring Your Own Device Environment

An additional benefit to using blockchain is that it can support the Bring Your Own Device (BYOD) environment. This environment allows users to connect to the network with their own computer and participate in available transactions when needed. This type of setup can be particularly useful when it comes to using blockchain as a distributed training system. However, the BYOD environment increases security risks and challenges to keeping the transaction network secure and restricted.

BLOCKCHAIN SOLUTIONS

We have discussed the risks of blockchain, however, the future technological advancements have the potential to change the way societies exchange value and data. Specifically, the training and simulation industry can benefit from researching and developing prototypes utilizing smart contracts and other advanced techniques.

Smart contracts are one component of aforementioned blockchain technology – implemented in the Solidity language on Ethereum or Fabric on solidity. How can this transparent, distributed ledger be used not only for information assurance but also for information security? It is possible by augmenting the ledger computations with three other techniques: secure multi-party computation, federated learning and homomorphic encryption. The combination of these techniques allows third parties to access and manipulate encrypted data while producing an auditable trail on the blockchain where the smart contract is implemented.

To review, smart contracts allow exchange of data in a transparent, conflict-free way without a middleman. Nearly-Turing complete computation occurs on the distributed ledger by multiple parties who execute the same deployed smart contract code and compare results. The result is stored on the blockchain or can be output/modified further. While some secure or anonymous computation can be accomplished with particular blockchain technologies (e.g. ZK-Snarks for Ethereum) it is not strictly required that these implementations are used to assure anonymity of data. Information security can be achieved by encrypting information before it is put into the ledger.

Federated Learning involves sending a model to a source of data and updating the model locally before sending it back to the creator of the model. When a model is initialized, however, it can be initialized in such a way that allows reconstruction of the training data upon receipt of the model with updated weights. This can be overcome by initializing a model spec "in the blind" using a trustless third party. Smart contracts can be that trustless third party. Multi-Party Computation enables parties to jointly compute a function over their inputs while keeping those inputs private. Homomorphic encryption allows computation on encrypted data; the outcome of this computation is an encrypted result that can be subsequently decrypted to produce the same result as if the computations had been performed on unencrypted data. Fully Homomorphic Encryption, first described by Gentry, means that any computational operation is possible where other somewhat homomorphic encryption schemes are limited to certain operations. FHE is computationally intensive but careful implementation allows certain operations to be computed in tractable amounts of time (Gentry et. al 2011) (Damgard et. al 2008). Homomorphic Proxy Re-Encryption allows a third party to re-encrypt data that has been encrypted by one party and change it without introspecting to make it decryptable by another party.

Various combinations of these techniques provide powerful tools for data brokerage and analysis – data can come from multiple sources with those sources retaining privacy of their data even when stored in a distributed ledger. Why not just use a database filled with encrypted data? The delegation and distribution provide information assurance and fault-tolerance in the way that distributed version control is preferred to centralized repository structures – so called "privacy preserving classification" or encrypted, federated machine learning ("OpenMined", 2017). Homomorphic encryption allows a smart contract to become a trustless 3rd party where data can be tracked, transformed, proxy re-encrypted, or transferred in the open while preserving the privacy of the content. Certain classification methods satisfy privacy requirements without the need for HE (Bost et. al 2015) but any type of computation can occur as long as fully homomorphic encryption is used to realize a blind Turing machine. Not every type of classification or analysis will require encrypted federated learning, but it provides a concrete example of how and why blockchain smart contracts fundamentally change how data can be utilized. There is transparency, non-repudiation and delegation of transaction information but also assurances for data confidentiality and data integrity.

DESIGN RECOMMENDATIONS

Now that we have discussed blockchain technology and its advances as well as advances in cryptography we can apply these technologies to an example use case. We believe that these technologies are well suited to benefit many use cases, but we will focus on the use case of aircraft maintenance data archival and processing. As stated earlier, this use case has a central authority who processes aircraft sensor and usage data to provide meaningful analysis such as maintenance recommendations, preventative maintenance suggestions, and focused training exercises. This central processor interfaces with several sovereign entities who each have an interest in keeping sensitive maintenance data secure and private from each of the other sovereign entities that have their data processed by the central authority.

Standard Methods For Maintenance Data Storage and Analysis

In a typical setup for the aircraft maintenance data processing use case, a secure database would be set up to contain all the data. The central authority would manage that database, likely housed in a remote secure data storage facility. Each sovereign entity would also have a secure database to house their specific data and need to be able to securely transfer that data between entities while preserving the data integrity; the incorporation of the required security checks and data preparation prior to sending requires an investment of both time and computational resources. This increased complexity adds insertion points for failures to occur in the data transfer process that will be discussed later in this section as well as their impacts.

At regular intervals each sovereign entity would need to set up a meeting with the central authority for a secure data transfer. This transfer could happen through encrypted network traffic but in the most secure settings it may happen by physical media transfer such as an external high capacity hard drive. An average amount of data needing to be transferred at such a meeting could be on the order of Terabytes, especially if meetings cannot be coordinated often enough. Transfer of that data varies but may be on the order of hours in certain situations based on the amount of data being transferred, the resources available between sites and availability of a reliable, always-on connection for wireless transfers—for large loads or lower reliability setups, this can take a significant amount of time, on the order of hours for data transfer alone.

Furthermore, while much time is spent on the required and expected tasking (i.e. meeting coordination, data transfers), an even greater amount of time may be spent addressing unintended consequences such as data corruption, failure to send/receive data and any subsequent data mismatch resulting in fragmented and inconsistent data between entities. These failures may arise from several different factors including errant code, improper tagging of data prior to sending/receiving, lack of data receipt confirmation or even user error resulting in errant transfers. Depending on the failure mode causing the errant/missing data, the discrepant entities may not be aware of a mismatch and, through normal use, allow subsequent data to be added to the pre-existing errant ledger, exacerbating the issue by propagating the failure (in this case, errant data) throughout the data history as more and more data is collected at each entity. Over time users or the system may raise alerts identifying discrepant data, resulting in a vast consumption of human and computational resources in order to review records across several different entities, identify the point of fragmentation/misalignment, make the proper adjustments then refeed the data back into the system and resynchronize the entities consuming unanticipated time and resources; downstream impacts include the loss of trust in the management system as this additional investment of resources grows over time and may have impacts beyond usability, particularly safety concerns with regards to usage data for safety critical parts

Once data has finally been transferred to the central authority data processing can finally occur. The result of the analysis of the data will then need to be coordinated to be returned to each sovereign entity. Due to the time involved in this round trip process the analysis provided can be days or even weeks after the data was originally collected. Figure 2 gives a high-level comparison through a series of steps for a distributed database approach and makes the comparison to blockchain. Due to blockchain's high data security and fault tolerance, it's performance is slightly below that of a traditional database solution but has the advantage of requiring less intervention by the system/user in order to complete the same operations as a traditional database using a centralized ledger that is viewable by all parts of the system rather than needing to be downloaded by all parts in the system as is the case with a traditional database.

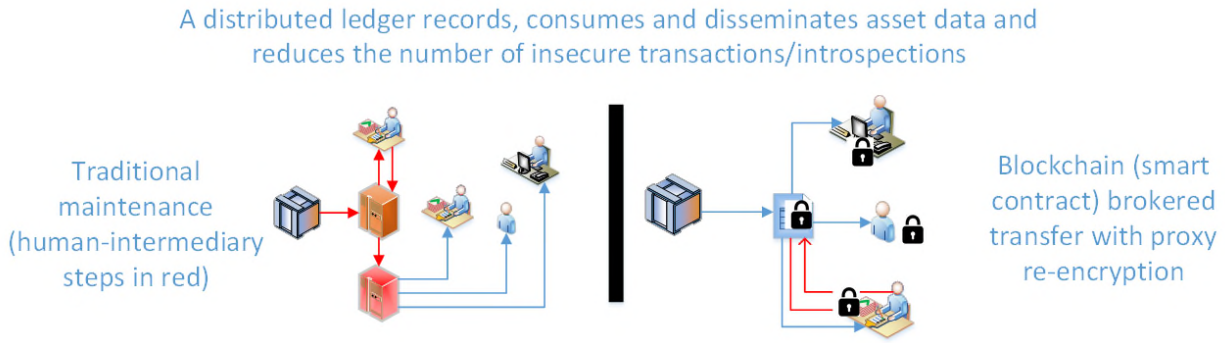

Figure 2. Traditional Maintenance Data Transfer vs. Blockchain Approach

PROPOSED SOLUTION

We propose a blockchain solution with homomorphic encryption for this use case to significantly reduce round trip data analysis time and increase data transfer success rate. Rather than each sovereign entity controlling its own private disconnected database, it would control a connected but homomorphically encrypted blockchain node. As data is collected it can be loaded directly onto the blockchain which is shared between the sovereign entity and the central authority.

Imagine an aircraft has just completed a sortie. At this time the data is fresh and ready to be uploaded. Typically, data would be loaded into a local database and over the course of days/weeks this process would be repeated to collect a significant amount of data, then the synchronization to the central authority would be coordinated. Instead, that data can be immediately loaded onto the shared blockchain for processing to occur. Since data is now collected, encrypted and transferred to all nodes at a greater frequency, the size of each data transfer is greatly reduced resulting in shorter data load times. When dealing with large databases, historical data can get corrupted or lost. With a blockchain, all historical data is constantly being verified so that if one local database is corrupted, it can be corrected with the accurate

data from all the other local databases, eliminating the need for additional resources to return the data to normal in the event of an anomaly or discrepancy.
In an attempt to quantify the advantage of a blockchain-based solution over traditional database solution for maintenance data transfer, a sample set of calculations will be performed using the following set of assumptions and the results summarized in Table 1:

- The comparison will assume a 256 Gigabyte (GB) data transfer using a 75 Megabits per second (Mbps) transfer rate. Using a free-to-use file transfer speed calculator, this transfer is estimated at 8.1 hours
- Due to the current performance barriers of blockchain technology, blockchain transfer speeds will be assumed to be 75% of the speeds of a traditional database:

$$\frac{8.1\ hours}{0.75} = 10.8\ hours\ to\ transfer\ 256\ GB\ using\ 75\ Mbps\ transfer\ rate\ for\ a\ blockchain\ solution$$

- Database will transfer to a single centrally located server that receives the data then redistributes to all assets in the field

Table 1. Quantitative Comparison of Traditional Maintenance Data Transfer vs Blockchain Approach

Task	Traditional Database		Blockchain	
	Required Task?	Associated Time (hours)	Required Task?	Associated Time (hours)
Pull data from asset(s) of interest	Y	1	Y	1
Wired data transfer into maintenance tracking platform	Y	1	Y	1
Review newly updated data for anomalies and finalize	Y	1	N	-
Data upload to central database/ledger	Y	8.1	Y	10.8
Centralized data redistributed to local platforms for synchronization	Y	8.1	N	-
TOTAL TIME	19.2 hours		12.8 hours	

Based on the sample analysis, a blockchain-based data transfer solution from the scenario above requires only 67% of the time required by a traditional database solution. This calculation did not factor in the potential for data transfer errors and associated rectification times that can occur in a traditional database system but are not present in blockchain-based solutions due to their high fault tolerance, security and use of a single managed ledger. The time savings would be even greater as the number of database portals increases in a traditional database solution as well as blockchain technology continues to evolve and performance improves over time. Furthermore, the decreased demand on bandwidth allows other data transfer tasks to be performed in parallel with a blockchain-based solution rather than serially, which may be the case for a database solution.

With the guarantee of accurate data and the near instantaneous access of it at the central authority, data analysis can happen continuously. Results of the analysis can be posted back to the blockchain for quick and easy access back to the sovereign entities. One of the main concerns of this approach would be the sensitive nature of the data provided to the central authority as well as the sensitive nature of the analysis itself. This is where the application of homomorphic encryption becomes beneficial. Using homomorphic encryption before adding data onto the blockchain, analysis can occur without exposing data to third parties. It is possible via this method for the sovereign entity to keep its data private from the central authority itself but use it as a broker to manage analysis or model initialization ("OpenMined", 2017). A smart contract, crucially functioning as a trustless 3rd party, enables a variety of interchanges of sensitive data which would otherwise be impossible. A secondary blackbox could be used to selectively re-encrypt data coming from one source for use by another source; there is some research which suggestions this can be implemented as a decentralized key-management-store privacy layer for blockchains (Egorov et. al 2017).

Consider this simplified example using fictitious data:

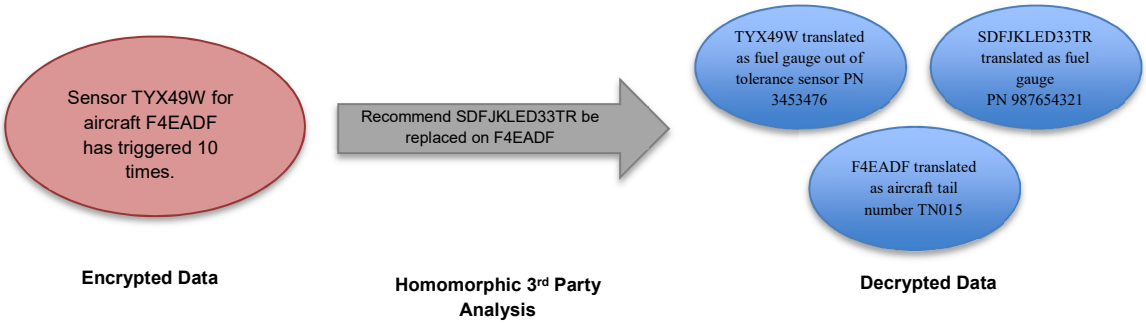

Figure 3. Example of blockchain encryption approach

With this technique of homomorphic encryption in combination with a blockchain new analysis methods become possible. Federated learning also becomes possible for creating models on the anonymously provided data from multiple similar entities. Rather than simply providing maintenance recommendations, more efficient analysis across the larger data set can allow for increased prediction of maintenance needs and suggest preventative maintenance actions based on identified trends in the data superset.

In addition to preventative maintenance suggestions, the data could be analyzed to provide better and more focused training to aircraft maintainers where shortfalls in maintenance actions or design issues identified in the performed advanced data analytics have been fed back into the system CONOPS improving system reliability and maintainability as well as maximizing the value in an already existing resource--data. For example, a machine learning algorithm could even learn to recognize what the early warning signs for a malfunctioning fuel gage are and suggest training.

Beyond securing maintenance data in an operational context, one can imagine securing human performance data in a training context. Various types of input from operators could be secured and marshaled to end users with smart contracts. This information could also be securely distributed in similar way for a general distributed simulation context. Other applications might include a trustless, immutable management of distributed simulation hardware and user access audit data.

While a variety of approaches/implementations may be used to address the maintenance collection and analytics issue, the implementation of a blockchain-based data transfer system and ledger will allow for agile and reliable data consumption, tracking and processing from a single, trusted ledger that not only can be used to improve aircraft maintenance, but eliminates the overhead associated with data correction and allows for a highly available system for use in the field.

Benefits of a Blockchain Approach.

By reducing the human component in the maintenance data game, there can be significant savings in both time and money! The earlier that a blockchain can be set up in the aircraft lifecycle, the greater the savings that can be seen. With encryption of the data, various customers with sensitive sensor data can be transmitted to the blockchain to be processed with trust that their data will not be compromised. Due to the sensitive nature of the data, any changes to this process comes with elevated risk. This elevation of risk requires increased focus on the data which in turns means more time must be spent processing it. Since the data is currently sent in large chunks, the time required to process the data is extremely high. This automated trust-based system removes the human factor which could cause errors to occur and allows for the end user to get faster results from the data processing. Currently companies expend large amounts of resources on maintaining standard database systems for storing and transferring aircraft maintenance data; between debugging issues, storing data and uploading that data to be processed there are many possibilities for even the smallest error to pop up causing the process to increase significantly in length and therefore cost. A blockchain-based data transfer and collection solution helps to reduce this risk from both a security and productivity standpoint; these efficiencies are gained through reduced time in transfers, round trip analysis and improved preventative maintenance recommendations. There would also be enhances in training for aircraft maintainers through efficient

collection and analysis of data. Given the financial investments made by companies and governments in air vehicles and defense overall, even a marginal increase in efficiency would result in substantial cost savings to all invested parties.

CONCLUSION

Blockchain is an emerging and foundational technology with capabilities that extend beyond its current cryptocurrency institutionalization. It's ability to stand as a secure and decentralized transactional infrastructure that allows for traceable data transactions of varying types, complexity and permissions has allowed for a large number of use cases to emerge in today's digital world. Advances in encryption techniques have made the technology more viable to a growing number of industries where secure data transfers are pivotal to daily operations, sustainment and reputation. Further research into the emerging use cases will help develop better methods for the technology which in turn will help make for a better tomorrow. This paper has highlighted use cases specific to the defense industry, but the reality is that the significant applicability of this technology has the potential to have global-scale impacts with how data is moved between entities; a key performance parameter in an ever-growing digital landscape.

REFERENCES

Andrew Trask et al. Openmined/docs. Retrieved from https://github.com/OpenMined/Docs, 2017

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Muralidharan, S. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference (p. 30). ACM.

Bost, R., Popa, R. A., Tu, S., & Goldwasser, S. (2015, February). Machine learning classification over encrypted data. In NDSS (Vol. 4324, p. 4325).

Damgard, I., Geisler, M., & Kroigard, M. (2008). Homomorphic encryption and secure comparison. International Journal of Applied Cryptography, 1(1), 22-31.

Egorov, M., & Wilkison, M. (2017). NuCypher KMS: Decentralized key management system. arXiv preprint arXiv:1707.06140. French, A. M., Guo, C., & Shim, J. P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). CAIS, 35, 10.

Furukawa, J., Lindell, Y., Nof, A., and Weinstein, O. "High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority" https://eprint.iacr.org/2016/944 5.

Gentry, C. (2009). A fully homomorphic encryption scheme. Stanford University.

Gentry, C., & Halevi, S. (2011, May). Implementing gentry's fully-homomorphic encryption scheme. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 129-148).

Iansiti, Marco & Lakhani, Karim. (2017). The Truth About Blockchain, *Harvard Business Review, January-February Issue.* Retrieved from https://hbr.org/2017/01/the-truth-about-blockchain.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual International Cryptology Conference (pp. 357-388). Springer, Cham.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Security and Privacy (SP), 2016 IEEE Symposium on (pp. 839-858). IEEE.

Miller, E. K., & Buschman, T. J. (2015). Working memory capacity: Limits on the bandwidth of cognition. Daedalus, 144(1), 112-122.

Naehrig, M., Lauter, K., & Vaikuntanathan, V. (2011, October). Can homomorphic encryption be practical?. In Proceedings of the 3rd ACM workshop on Cloud computing security workshop (pp. 113-124). ACM.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Springer, Berlin, Heidelberg. Chillotti, I. et al. "Improving TFHE: faster packed homomorphic operations and efficient circuit bootstrapping" https://eprint.iacr.org/2017/430 4.

The World Bank. (2017). Distributed Ledger Technology (DLT) and Blockchain (pp.6). Retrieved from http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

Van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V. (2010, May). Fully homomorphic encryption over the integers. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 24-43). Springer, Berlin, Heidelberg.

Wade, D., Lugos, R., & Szelistowski, M. (2015, February). Using Machine Learning Algorithms to Improve HUMS Performance. In Proceedings of the 5th American Helicopter Society CBM Specialists Meeting.