Using Chia Blockchain Technology for Department of Defense Systems

Ethan Schofield and Mark Reith
Air Force Institute of Technology, Wright Patterson Air Force Base, USA

ethan.schofield.1@au.af.edu
mark.reith.3@au.af.edu

Abstract: The United States faces an escalating cybersecurity challenge, with national assets increasingly vulnerable to sophisticated attacks. The ever-reducing barriers to entry in the cyber realm, coupled with advanced persistent threats, underscore the critical imperative to fortify the defense of U.S. assets. Blockchain technology, pioneered by Satoshi Nakamoto over a decade ago, emerges as a resilient cryptographic solution capable of safeguarding data and assets from threats both within and outside a network. This paper delves into the potential of the Chia blockchain as a strategic ally for the Department of Defense (DoD) in bolstering its cybersecurity measures. Beyond a theoretical exploration, the paper provides tangible use cases that illustrate the practical application of Chia within the DoD framework. Notably, the examination extends to crucial areas such as financial auditing, identification management, and supply chain oversight, showcasing the versatility and efficacy of Chia in addressing multifaceted challenges faced by the DoD.

Keywords: Blockchain, Government, Defense, Chia, Security, Applications

Disclaimer: The views expressed are those of the author and do not reflect the official policy or position of the US Air Force, Department of Defense or the US Government.

1. Introduction

Cyberspace today is a warfighting domain where actors from around the globe converge. Battles in cyberspace have few barriers to entry, allowing adversaries and threats, ranging from near-peer competitors to economically disadvantaged ones, to harm the United States and its resources. This necessitates the United States and the Department of Defense (DoD) to safeguard its assets with the latest advancements in cryptography and cybersecurity. Blockchain technology, as one of the latest cryptographic techniques, will be explored in this paper. It will delve into the basics of blockchain technology and argue why the Chia blockchain should be a strong candidate for adoption by the DoD. This is due to its ability to leverage the advantages of both public and private blockchains through Virtual Private Blockchains, and its capability to repurpose old Department of Defense data storage into new technological assets. The paper will also present a use case of Chia for DoD supply chain management.

The blockchain was first introduced in 2008 by Satoshi Nakamoto when he published the Bitcoin paper, 'Bitcoin: A Peer-to-Peer Electronic Cash System.' This paper outlines how cryptographic techniques on a peer-to-peer network can create an immutable, decentralized, and secure storage of data (Nakamoto, 2008). This creates data storage that has greater integrity than a traditional database, which after updating could have little to no evidence of any change. An analogy that illustrates how a blockchain works compares it to a small village where villagers traded frequently with one another (Khan, 2021). However, with how much trade was happening, they required a bookkeeper to keep track of all the trades and promises made between parties. After some time, the bookkeeper became corrupt and started accepting bribes to change what was owed. When the village discovered that the bookkeeper was corrupt, they implemented a new way to keep track of all the trades and promises between parties. The proposed solution was for every villager to keep a record. Throughout the day, villagers would meet in the town square to trade and write down what prices were agreed upon. Then, once a week the villagers would meet to check for discrepancies amongst the ledgers. If there were any, all ledgers would be crosschecked and the most frequently entered record would be assumed correct. The blockchain works similarly to every villager keeping a ledger. Every computer or node that is a part of the network keeps a record of what was sent, received, and stored on the blockchain. Generally, every node on the network can see what is on the blockchain but cannot change it without approval from the majority of nodes on the chain.

2. Blockchain Technology Overview

Every blockchain has three layers: consensus, smart contracts, and application. Consensus is how all the nodes on the blockchain decide to agree on the order of transactions submitted by clients in the form of requests (Clavin et al, 2020). In essence, it ensures that only one sequence of transactions is deemed correct. In cases of disagreement among nodes, the consensus method is referenced, and the correct sequence of transactions is

selected based on the accumulated information. Next, smart contracts serve as the interface between consensus protocols and application layer-level implementations. This enables developers to create applications to run on the blockchain. Lastly, applications represent the user-facing aspects of the blockchain. Examples of application layers include the Philippine banking system, the Walmart/IBM supply chain initiative, and Malaysia's blockchain city.

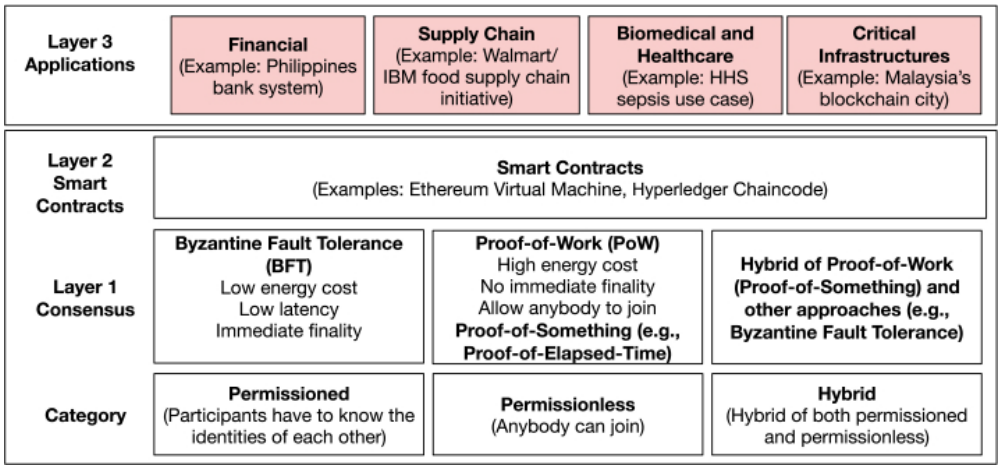

Figure. 1: Overview of Blockchain Technology with Potential Examples (Clavin et al., 2020)

2.1 Consensus Methods

Consensus or proof methods are how nodes on the blockchain verify that the newly added block is correct. There are various methods of proving that the next block should be added, each with unique attributes, such as power requirements, time to find the next block, and resource intensity. The two most prominent proof methods are proof of work and proof of stake.

The proof of work method is a computationally intensive operation where computer processing time is used to prove the next block on the chain. As explained by Satoshi Nakamoto, "The proof of work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits" (Nakamoto, 2008). While each blockchain has a specific algorithm that determines valid hash values, the underlying principle remains consistent. The computed value is quick to verify by other nodes as it can be verified by executing a single hash. Upon verification, nodes add the new block to their copy of the blockchain. Rival blockchains are addressed by this proof method, as the copy of the blockchain that is longer and verified by more nodes becomes the accepted or 'master' copy.

Proof of stake is an alternative method of proofing designed to address the 51 percent attack vulnerability inherent in proof of work and reduce overhead energy costs. The 51 percent attack occurs when an attacker gains control of the majority of nodes in a proof of work network, granting them complete control over the acceptance of transactions as correct. Proof of stake mitigates this risk by introducing the concept of 'coin age' (King & Nadal, 2012).

Coin age represents the financial investment in the blockchain and is calculated based on the time a coin is held and the amount held. For instance, if Bob possesses 50 coins held for 100 days, he accumulates 5000 coin-days of coin age. This concept is integral to proof of stake, as it limits the search space for the next hash. Specifically, the search space is constrained to "one hash per unspent walletoutput per second." (King & Nadal, 2012) In other words it is one hash per unit coin age. This is much more efficient than the unlimited search space of proof of work. Consequently, individuals with more coin age possess greater decision-making power, aligning decision influence with investment levels in the blockchain. This strategic integration of coin age in the proofing process enhances the security and efficiency of the proof of stake consensus mechanism.

2.2 Public, Private and Hybrid Blockchains

Public and private blockchains, also known as permissionless and permissioned blockchains, dictate access levels for reading, writing, and editing data on the blockchain. Public blockchains typically allow public access to both read and write data (Lewis, 2015). This openness promotes decentralization, immutability, and a diverse and

large participant base. Consensus methods for public blockchains typically take the form of ”proof of” models, like proof of work or proof of stake. These consensus methods are ideal for solving disputes on a trustless network and creating confidence in the transactions made on the network. However, challenges for public blockchains such as scalability and transaction speed may arise due to the extensive participation and competition among nodes for block validation.

In a private or permissioned blockchain, every participant on the network must receive approval from a central authority, enabling control over who can view, edit, or publish to the blockchain. For example, specific nodes may have publishing privileges, others may be limited to read-only access, or perhaps only designated nodes can access the blockchain (Yaga et al., 2018). Because all nodes require authorization to participate in the blockchain, a level of trust is established between them. Any misconduct can lead to the revocation of membership in the blockchain. Various consensus models can be employed in a permissioned network, depending on the level of trust among nodes. While both permissioned and permissionless blockchains implement smart contracts and the application layer similarly, the addition of a central authority in private blockchains sacrifices decentralization and immutability in order to ensure only authroized individuals have access to data on the chain.

Hybrid blockchains aim to combine the strengths of both public and private blockchains, seeking to strike a balance between the openness of public networks and the controlled access of private ones. To achieve this, they adopt specific measures to avoid shortcomings and enhance their capabilities. Hybrid blockchains strive to overcome the limitations of both public and private models by implementing a nuanced approach. They often involve integrating public and private elements selectively, tailoring the blockchain to meet specific use cases. Typically hybrid blockchains aim to harness the benefits of public blockchains, like decentralization, while also implementing features like controlled access from private chains for increased efficiency. For example, a hybrid blockchain might employ a public network for broader data access while using private channels for specific transactions or confidential information. Hybrid blockchains are tailored for specific use cases to take advantage of specific traits from public or private chains.

3. Smart Contracts

Smart contracts are coded instructions written into the blockchain, automatically executing when nodes reach consensus. The term ”smart contracts” is derived from their resemblance to traditional business contracts, as they fulfill agreements made by multiple parties. The ”smart” aspect refers to their seamless execution without disrupting blockchain operations. Developers can write a new smart contract that includes a set of functions. Once the contract is deployed on the blockchain, authorized users can call the contract to use those functions without interrupting other ongoing blockchain services. (Clavin et al, 2020)

However, the introduction of smart contracts also introduces potential vulnerabilities to the blockchain. As noted by J. Clavin, ”Since all blockchain transactions are included in the hash chain,and therefore unchangeable,having a bug in the contract,or a flaw that can be exploited, introduces risk into the system. It is also worth noting that the use of smart contracts will likely degrade the performance of the system.” (Clavin et al, 2020)

Smart contracts, while powerful and versatile, demand careful consideration and thorough testing to minimize the risk of introducing vulnerabilities to the blockchain system. The immutability of blockchain transactions amplifies the importance of ensuring that smart contracts are error-free and secure before deployment. Researchers have observed that the utilization of smart contracts may impact system performance, underscoring the need for ongoing research and optimization in this critical aspect of blockchain technology (Gueta et al., 2019).

4. Blockchain Applications

Blockchain applications represent the uppermost layer of the blockchain, encapsulating the tangible outcomes and functionalities that the blockchain system aims to achieve. All the underlying layers of consensus, smart contracts, and data structures converge to fulfill these applications. The scope of blockchain applications is broad, spanning critical infrastructure, healthcare, online gaming, and various other domains. Many large-scale blockchain applications are still in their early stages of development. For instance, the Chinese-funded tourist city in Malaysia’s Melaka Straits (Property Report, 2019) and Canada’s pilot on blockchain digital credentials are notable examples (Leal, 2022). In the Malaysian project, blockchain is employed to enhance the tourism

experience and infrastructure, showcasing the versatility of blockchain in real-world applications. Canada's pilot program, on the other hand, explores the use of blockchain for maintaining permanent, independently owned copies of identification credentials by employees. These examples illustrate the diverse range of applications where blockchain technology is being explored and implemented.

5. Chia Blockchain

Chia, founded by Bram Cohen, is a blockchain platform that shares similarities with Bitcoin but distinguishes itself through its consensus model. Chia's consensus mechanism is known as "proof of space and time," a departure from Bitcoin's proof-of-work. This model leverages excess disk space, repurposing old hard drives from data centers to solve proofs for the blockchain (Cohen & Pietrzak, 2019).

While decentralization is a core principle of the Bitcoin blockchain, unintended centralization occurred, with a few large mining companies, such as NiceHash, controlling the majority of block mining on the network (Chia Network, 2021). This concentration of control poses challenges to the trustworthiness of a decentralized network, as increased influence by a single entity can impact decision-making on the blockchain. Proof of space in Chia resembles proof of work but with a new approach to finding the next hash value. Instead of processing various hashes, it involves storing cryptographic hash values on unused disk space. When the blockchain signals the need for a new block, it issues a challenge. Farmers, participants in the network, scan their disks to find the hash closest to the challenge. The probability of a farmer possessing the correct hash is proportional to their share of disk space in the entire network.

Proof of time is coupled with proof of space to enhance security. As proof of space is relatively quick to solve compared to proof of work, there is a risk of attackers with substantial storage creating competing long transaction chains. In most consensus models if there is a discrepancy between two chains the longer of the two is accepted as the correct history and the other is discarded. To address this, proof of time ensures consistent block additions over time, so parties that want to verify their own elections cannot.

Verifiable Delay Functions, (VDFs), are crucial for proof of time and are executed by servers known as "Timelords." These functions prevent fast completion and add assurance that the next block's validator will be chosen unpredictably. The blockchain only requires one trustworthy Timelord because the fastest Timelord will always execute the proof first. In order to help keep Timelord servers trustworthy Chia partnered with Supranational to produce an open-source proof of time VDF. Proof of time further adds confidence that the selection of the next block's validator will be highly unpredictable, reducing the likelihood of a party interested in a specific transaction becoming the next validator (Chia Network, 2021). This combination of proof of space and time establishes a robust and secure consensus mechanism in the Chia blockchain.

6. Why Chia for the DoD

Chia presents itself as a robust candidate for blockchain implementation by the DoD due to several compelling reasons. First, Chia offers a Virtual Private Blockchain. A unique technology native to Chia which combines the strengths of both public and private blockchains. This includes the decentralization of the entire Chia chain, but also allows to be uniquely programmable for the DoD's applications, have central governance over DoD operations and have permissioned access onto DoD applications. The flexibility to have the decentralization offered by a public blockchain, but the central governance and privacy of information of a private blockchain is crucial for DoD applications.

Chia's consensus layer, proof of space and time, is particularly conducive to the DoD. Given the DoD's possession of large quantities of old storage devices, repurposing these devices to support the blockchain is a sustainable and resourceefficient approach. Instead of discarding outdated hardware, the DoD can leverage its existing infrastructure to contribute to the blockchain's functionality.

Decentralization is a key aspect as to why Chia would be so powerful for the DoD. Decentralization offers strong reliability and trust in the information kept on the blockchain, and the applications executed on top of it. With a higher number of participating nodes, it becomes more challenging for malicious actors to gain control over the network and alter data. At the time Chia published their business whitepaper they claimed that they had "already become the most decentralized blockchain by node count ever." (Chia Network, 2021) This strong decentralization would create a trustworthy platform by ensuring data integrity and immutability.

The combination of decentralization and the Virtual Private Blockchain provides a secure and reliable environment for the DoD. Transactions within the Virtual Private Blockchain are verified by nodes on the entire Chia chain, enhancing security and integrity. Additionally, the permissioned access control further safeguards sensitive DoD applications. This unique combination of public and private chains is exactly what the DoD would need to have for blockchain adaption.

Some may suggest that public blockchains like Ethereum or Cardano may be a better choice for DoD use. However, there are several issues with both of these chains for use by the DoD. First, both are proof of stake, this is not ideal for DoD use because an adversary would only need to buy up a large share of the asset to have substantial voting power on the network. An adversary having control over decisions that affect DoD assets would not be secure. Next, Ethereum's smart contract language and programming environment makes it very difficult for projects to scale. (Chia Network, 2021) Projects launched on their network suffer the same security issues all around, making it a familiar attack surface. Finally, Cardano's network consists of only about 6000 nodes, this is relatively small compared to other public chains. For activities involving national security this is not enough decentralization for a blockchain.

Others may suggest that if public blockchains are not ideal, then the DoD should use a private blockchain like Ripple or Stellar. The primary issue around using a private blockchain is it would remove benefits from public blockchains, with the most important being decentralization. If the blockchain is not decentralized, then it is almost the same as storing data and doing transactions on a standard database. Switching from a standard database that is in use today, to a private blockchain would not be worth the taxpayer money, or the time to implement for such a marginal gain.

7. DoD Chia Use Cases

The existing auditing and funding procedures within the DoD, including the Army Financial System, involve multiple stages such as contract awardation, invoices, receipts, and payment requests. This intricate process introduces several vulnerabilities, including the potential for incorrect accounting, embezzlement, or mismanagement of funds. Transitioning to a blockchain-based system offers a transformative solution. By migrating the current system onto a blockchain, the DoD can publish and maintain contracts with the confidence that the data recorded at the contract's inception remains immutable. The blockchain's inherent immutability ensures that once the contract data is stored, it cannot be altered in the future, providing a secure and transparent foundation for auditing and funding processes. This shift holds the promise of minimizing errors, enhancing accountability, and mitigating the risks associated with financial mismanagement within the DoD.

In a thesis exploring blockchain use to track DoD auditing and funding it was determined that a private permissioned blockchain would be the best use for the DoD and its vendors (Prasanna, 2022). Permissionless public blockchains were not ideal because anyone, including foreign adversaries could join and read, write, and edit data. Next, permissioned public blockchains were not chosen over permissioned private blockchains because the Freedom of Information Act Exemption 4 states that trade secrets and financial information between contractor and government agency can be made confidential (Congress, 2016). If all vendors and contractors are added to the same permissioned public chain then all vendors could see contracts between the DoD and other vendors.

Chia's Virtual Private Blockchain can address the challenge posed by the Freedom of Information Act Exemption 4, allowing trade secrets and financial information between the DoD and contractors to remain confidential. By setting up individual virtual private blockchains between each vendor and the DoD, sensitive information can be protected without compromising transparency within the network. This would enable the decentralization benefits of the Chia blockchain at the cost of additional setup.

The implementation of Chia's Virtual Private Blockchain holds significant potential for managing independently owned identification within the Department of Defense (DoD). By incorporating all DoD members into the virtual private blockchain, a robust and verifiable platform for identification verification can be established. This strategic use case not only enhances security measures but also ensures the integrity of identification information by rendering it tamper-proof. Shifting DoD identification onto the blockchain introduces a powerful deterrent against malicious actors attempting to spoof or steal DoD identification cards. The utilization of unique private keys for each individual on the blockchain becomes a crucial security feature. Without possessing the designated private key, unauthorized individuals would be unable to impersonate someone else. This innovative approach not only bolsters the security of military bases but also enhances protection for areas requiring security

clearance access. The adoption of Chia's Virtual Private Blockchain in this context reflects a proactive measure to elevate the overall security posture of DoD identification systems.

Supply chain management within the Department of Defense (DoD) can leverage Chia effectively. In addressing concerns raised by the Government Accountability Office in its report to Congress, which highlighted vulnerabilities to counterfeit parts within the DoD supply chain (United States Government Accountability Office, 2016), the implementation of a Chia-powered blockchain becomes crucial. Establishing a virtual private blockchain that involves all relevant vendors enables comprehensive tracking of parts, their conditions, and shipping information. Not only would this blockchain solution allow the DoD to monitor the entire supply chain but it also facilitates accountability, transparency, and honesty on part of the vendors providing what was agreed upon. Specifics that could be monitored by the DoD include, monitoring parts modifications en route, identifying potential breakages during transportation, and ensuring product authenticity (Pun et al., 2018). Chia's blockchain technology emerges as a robust tool to effectively address these challenges and fortify the integrity of the DoD's supply chain.

8. Conclusion

The examination of Chia's applicability in key DoD use cases, such as financial auditing, identification management, and supply chain oversight, underscores its versatility and effectiveness. The Virtual Private Blockchain's integration into these scenarios not only aligns with the DoD's security requirements but also introduces a higher level of transparency and reliability in critical processes. Chia's decentralized architecture, combined with the tailored approach of the Virtual Private Blockchain, positions it as a strong candidate for securing and managing sensitive information within the DoD. While this paper provides insights into the potential applications of Chia's Virtual Private Blockchain, future research could delve deeper into the nuances of its implementation across various use cases. Exploring the intricacies of financial auditing, identification management, and supply chain oversight with Chia's blockchain technology would contribute valuable insights into its real-world efficacy. Understanding how the Virtual Private Blockchain enhances security benefits compared to traditional blockchains and private permissioned blockchains could pave the way for more informed decisionmaking within the DoD. Future investigations can illuminate the specific advantages and considerations of adopting Chia in different DoD contexts, and providing a comprehensive roadmap for its successful integration into the nation's cybersecurity framework.

References

Abraham, I., Gueta, G. G., Grossman, S., Malkhi, D., Pinkas, B., Reiter, M., ... Tomescu, A. (2019). *Sbft: A scalable and decentralized trust infrastructure.*

Chia Network. (2021). *Chia network inc. business whitepaper.*

Clavin, J., Duan, S., Zhang, H., Janeja, V. P., Joshi, K. P., Yesha, Y., ... Li, J. D. (2020). *Blockchains for government. Digital Government: Research and Practice, 1, 1–21.*

Cohen, B., & Pietrzak, K. (2019). *The chia network blockchain.*

Congress, 114th. (2016). *The Freedom of Information Act, 5 U.S.C. § 552, Jun.*

Doherty, N., & Delener, N. (2001). *Chaos Theory: Marketing and Management Implications. Journal of Marketing Theory and Practice, Fall, 9(4), 66–75.*

Khan, D. (2021). *3 analogies that explain how blockchain technology works.*

King, S., & Nadal, S. (2012). *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. Self-published paper, August, 19(1).*

Leal, N. (2022). *Canada pilots blockchain staff records.*

Lewis, A. (2015). *A gentle introduction to blockchain technology.*

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

Pun, H., Swaminathan, J. M., & Hou, P. (2018). *Blockchain adoption for combating deceptive counterfeits.*

Prasanna, P. (2022). *The use of blockchain to track dod funding and auditing.*

Property Report. (2019). *Malaysia is building Asia's first blockchain city.*

United States Government Accountability Office. (2016). *Dod needs to improve reporting and oversight to reduce supply chain risk report to congressional committees.*

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview.*