Potential Applications of Blockchains in the Air Force

Kelly Fam and Claudia Richoux
Information Assurance Interns,
AFRL Information Directorate

23 June 2017

This report describes blockchains, their organization within a network, and their applicability in three scenarios to assess the potential of blockchain technology for the Air Force.

1 Introduction

Electronic transactions traditionally use a trusted third party that (1) ensures the validity of the transaction and (2) records the transaction into a permanent record. Bitcoin uses blockchains to remove the need for third parties, or intermediaries altogether, that reinvents how we view trust in a cyber context. In 2008, Satoshi Nakamoto introduced blockchains, a distributed ledger of digital records saved in chains of blocks. The process to create and append a block to the chain uses a significant amount of computational power, so a hacker cannot feasibly amass enough computational power to change data in the blockchain. [1] Nodes partake in the creation of a proof-of-work for a block, and essentially determine the credibility of a block to add to the blockchain through hash comparisons and node consensus. The low probability of a successful attack on hash functions and the inter-dependency of previous blocks allow verifiable nonrepudiation of recorded transactions. Blockchains present a solution to the Byzantine Generals Problem, where a number of nodes in a network may be hacked or broken. [2] Blockchains make the network resilient to Byzantine faults as long as at least half of the nodes remain healthy. [3] Currently, blockchains apply to finance, smart contracts, and situations where one must verify that events occupied certain state at a certain time. With this in mind, the military may use blockchains to create a revolutionary, decentralized approach to guarantee information integrity in Air Force missions.

2 Blockchain Metrics

In this section, we examine the Bitcoin proof-of-work blockchain, created by a network of peer nodes with a zero-trust relationship.

2.1 Proof-of-Work

In the Bitcoin blockchain and other proof-of-work chains, block N includes the hash of block $N-1$, a block header with the time, and a hash called a Merkle root that represents the transactions in the block. Every node in the system works to calculate a number called a "nonce" which when hashed with the other data in the block, yields a hash beginning a

certain number of zeroes to set the difficulty. The process to verify hash correctness takes one hash operation, but the process to compute a correct hash exhibits exponential complexity with respect to difficulty. The node that finds a nonce that works for block N can add its block to the chain once the majority of the nodes verify the solution, and then the node receives a Bitcoin reward. Subsequantly, since the new blockchain is of length N, the rest of the nodes accept the new longest chain and begin searching for another nonce for block $N + 1$ with the hash of block N. [1]

2.2 Blockchain Integrity

Strong cryptography ensures the integrity of the blockchain because rewriting block M in a chain of length N takes the work of $N - M$ blocks. While an attacker performs this work, the chain continues to grow. Since nodes only accept the longest chain they see, an attacker cannot change a block without at least as much computational power as the rest of the network combined. Though unlikely, a 51% attack may render a blockchain vulnerable. The Bitcoin network as a whole exhibits vulnerability to attacks on the network and hardware, including Man-in-the-Middle or Denial-of-Service on nodes and wallets, but as long as more than half of the nodes remain honest, the system as a whole retains its integrity. [4]

2.3 Contribution to a Blockchain

A Bitcoin node may contribute to the chain when it presents data that proves computations occurred. Therefore, it takes a lot of computational power to rewrite the chain. [5] The difficulty of the chain adjusts every 2,016 blocks so that the time to add a block remains at an arbitrarily chosen 10 minutes. Since the block time remains constant and the length of the chain constantly increases, the time for a 51% rewrite attack also constantly increases. Currently, it would take a year to rewrite the Bitcoin blockchain while holding the same amount of computing power as the entire rest of the network. This rewrite time is linearly increasing from about six orders of magnitude longer than the time it takes to add one block to the chain. [6]

3 Applications of Blockchains

3.1 Cryptocurrency

As explained in the last section, cryptocurrency relies on blockchains. They solve the double-spending problem in decentralized cryptocurrency, where without a trusted third party, a buyer holds the ability to duplicate and send the same money to multiple sellers. A blockchain cryptographically ensures the legitimacy of Bitcoin transactions with a transparent and public ledger of ownership representing the entire life of the currency. [7]

3.2 Virtual Ledger

Blockchains offer a solution to uncertainty in virtual records. For example, the Republic of Georgia uses blockchain to keep a ledger of government activities and land transactions to

fight corruption and land disputes. [8] In addition, Estonia protects the healthcare record of their citizens inside a blockchain. The military may use blockchains to keep track of events on systems where many organizations must collaborate at various trust levels. This could be applicable to humanitarian efforts, where a public and trustworthy ledger may be useful for negotiating collaboration between many nation-states and organizations. From a cybersecurity perspective, blockchains may also store Common Access Card (CAC) data to prevent card duplication or reactivation after being destroyed. [9]

3.3 Data Validation

Blockchains allow for the verification of the state of data at a certain time. If hashes of sensitive data go into the blockchain at a certain time, the owner of the data can check back later and validate malicious actors performed no changes in data after the date of its addition to the chain. This is useful for forensics after an attack, or to immediately detect malicious changes and fall back to a verified uncompromised backup system, or to ensure that communications between systems remain unchanged between sending and reception. DARPA recently made a contract with a company called GuardTime to provide a service that does exactly this. In this context, blockchains provide data validation for computer security and forensics. [10]

4 Conclusion

Blockchains provide powerful new technology to allow verification of data in a distributed system without trust through cryptographic measures. Potential military applications include verification of communication and events among diverse organizations, and validation of data and logs for improved cybersecurity. [11]

References

[1] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." n.p. 2009. Web. 22 June 2017.

[2] Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 382-401. Retrieved from http://www-inst.eecs.berkeley.edu/ cs162/fa12/hand-outs/Original_Byzantine.pdf

[3] Driscoll, K., Hall, B., Sivencrona, H., & Zumsteg, P. (n.d.). Byzantine Fault Tolerance, from Theory to Reality. Retrieved June 22, 2017.

[4] "Weaknesses." *Bitcoin Wiki*. Bitcoin Community, n.d. Web. 22 June 2017.

[5] Lopp, Jameson. "A Gem I Found in @pwuille's Code: Amount of Time It Would Take for an Attacker W/100% of Current Hashrate to Rewrite the Entire Blockchain. Pic.twitter.com/CfxgRXOhAe." *Twitter*. Twitter, 17 Nov. 2016. Web. 22 June 2017.

[6] Wuille, Pieter. "What Keeps the Average Block Time at 10 Minutes?" Bitcoin Security. *Stack Exchange*, n.d. Web. 22 June 2017.

[7] PricewaterhouseCoopers. "Making Sense of Bitcoin, Cryptocurrency, and Blockchain." *PwC*. N.p., n.d. Web. 22 June 2017.

[8] Shin, Laura. "The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project." Forbes. Forbes Magazine, 07 Feb. 2017. Web. 22 June 2017.

[9] Barnas, N. B., Major, USAF. (2016, June). Blockchains in National Defense: Trustworthy Systems in a Trustless World. Retrieved June 22, 2017.

[10] "Black Lantern Cybersecurity Platform." Guardtime. Guardtime, n.d. Web. 22 June 2017.

[11] Kulshrestha, S. (2016, November 23). Military Applications of Blockchain Technology. Retrieved June 22, 2017, from http://www.claws.in/1666/military-applications-of-blockchain-technology-sanatan-kulshrestha.html