BLOCKCHAIN: A Cyber Defense Force Multiplier

Dorian Belz

What is Blockchain?

At its core, a blockchain is simply a database for storing digital information where each *block* of time-stamped, published data is *chained* together with all preceding and subsequent blocks. What makes blockchain unique from traditional data storage is that data is not stored or controlled within a centralized database, but rather database management is shared by a decentralized network of trustless nodes that each maintain an identical copy of the blockchain. Before data can be published to the blockchain, it must first be validated by a majority of network nodes—typically referred to as *miners* or *validators*, depending on the consensus methodology used. This concept of "distributed consensus" makes the blockchain inherently tamper resistant and ensures that only verified transactions will be published to the blockchain.[1] The two primary consensus methodologies used in blockchain technology today are *proof-of-work*, first popularized in 2008 by the founder(s) of the Bitcoin[2] blockchain, and *proof-of-stake*, which has been used extensively in the development of derivative blockchain projects to help solve the issues of scalability and energy consumption associated with proof-of-workbased blockchains.

Both proof-of-work and proof-of-stake consensus protocols have associated strengths and weaknesses that must be considered when determining what type of blockchain to potentially use for Department of Defense applications. For proof-of-work blockchains, a considerable amount of CPU processing power is required to solve algorithmic puzzles before a block of data is published to the blockchain. The need for significant computational capacity and the security of distributed consensus make it fundamentally difficult for a dishonest node to manipulate data within a proof-of-work blockchain; however, the energy consumed by this protocol presents concerns from an environmental standpoint, as well as substantial challenges to scalability. By comparison, proof-of-stake blockchains do not require nodes to supply a large amount of computational power to validate transactions, but instead rely on a network of validators that hold a specified stake in the tokenized digital currency associated with the proof-of-stake blockchain. In this sense, proof-of-stake blockchains may be more vulnerable to

1 Samantha Ravich, "Leveraging Blockchain Technology to Protect the National Security Industrial Base," July 10, 2017, https://www.fdd.org/analysis/memos/2017/07/10/leveraging-blockchain-technology-to-protect-the-national-security-industrial-base/

2 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, https://bicoin.org/bitcoin.pdf

doi: 10.18278/gsis.7.1.8

data manipulation or denial-of-service attacks if bad actors are to accumulate a sufficient stake to serve as a trusted node on the network; however, methods such as "checkpointing"—where new transactions are verified against a master copy of the blockchain before being accepted onto a node's local reference version—can be used to rapidly identify and correct for these anomalies.[3]

Why is Blockchain Important to the DoD?

Our current defensive cyber architecture is rapidly becoming insufficient to establish and maintain battlespace superiority in the cyberspace domain of tomorrow. A report for Congress published in March 2020 by the Value Technology Foundation ,in collaboration with subject matter experts from the U.S. technology industry, stated this problem clearly as follows:

> The next generation of emerging technologies, which includes Artificial Intelligence, smart drones, robots, and additive manufacturing, will make the U.S. military even more dependent on digital technology. In this environment, the U.S. military has become critically dependent on secure, timely, accurate and trusted data. Yet, as data has grown in importance, cyber warfare has emerged to challenge the U.S. in the digital space. Today, key U.S. defense assets, ranging from communication systems to supply chains, can be disrupted by bad actors attempting to degrade U.S. capabilities.[4]

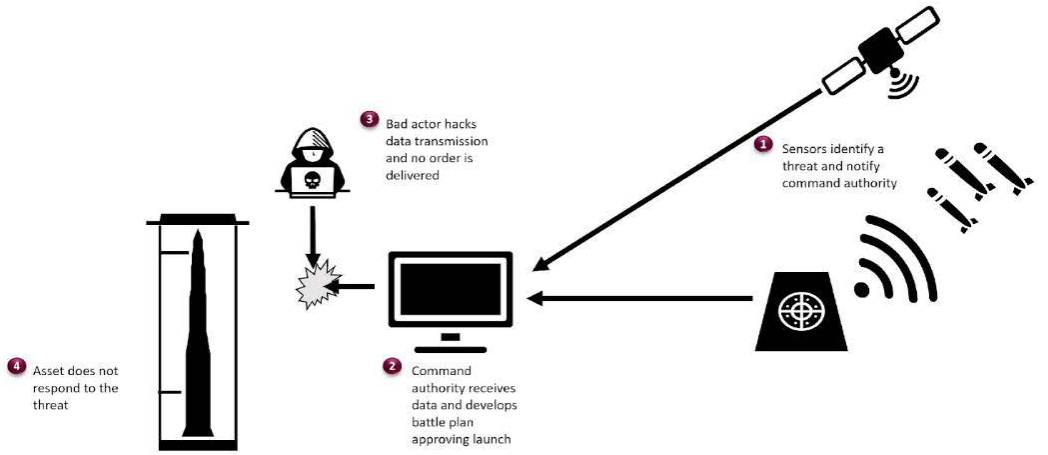
Mounting an effective cyber defense against potential bad actors is no longer as simple as installing firewalls and updating virus protection software. The exploitation methods used by our adversaries in the Cyberspace Domain are becoming increasingly sophisticated[5] and require novel solutions that redefine the landscape of the battlefield. Blockchain technology is the we need to accomplish this objective and has already proven to be invaluable across dozens of use cases for the U.S. Government and our industry partners. The Department of Defense, intelligence community, and our allies must act now to incorporate the latest advancements in blockchain technology into our existing cyber defense strategy and TTPs if we have any hope of establishing and maintaining strategic advantage in the Cyberspace Domain.

3 Rong Zhang and Wai Kin Chan, "Evaluation of Energy Consumption in Block-Chains with Proof of Work and Proof of Stake," , 2020, https://iopscience.iop.org/article/10.1088/1742-6596/1584/1/012023/pdf

4 Value Technology Foundation, "Potential Uses of Blockchain by the U.S. Department of Defense," March 2020, https://www.valuetechnology.org/_files/ugd/be4f79_17bfc382080f45edace0318ff0d70059.pdf

5 Victoria Adams, "Why Military Blockchain is Critical in the Age of Cyber Warfare," March 5, 2019, https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619

The scope of potential military applications for blockchain in defensive cyber operations is vastly expanding as the technology continues to mature. Use cases can be found throughout all facets of warfare ranging from protecting the integrity of military supply chain data to the prevention of adversary intrusion into our Joint All-Domain Command and Control (JADC2) infrastructure. This point is perhaps best illustrated by considering the damage a malicious actor can inflict by simply interrupting a data transmission from a command-and-control system to a weapons system, effectively preventing the weapon from responding to an incoming threat. Under our current system of centralized command-and-control, a single vulnerability may be sufficient to take a weapons system offline at a critical point in a commander's decision cycle.

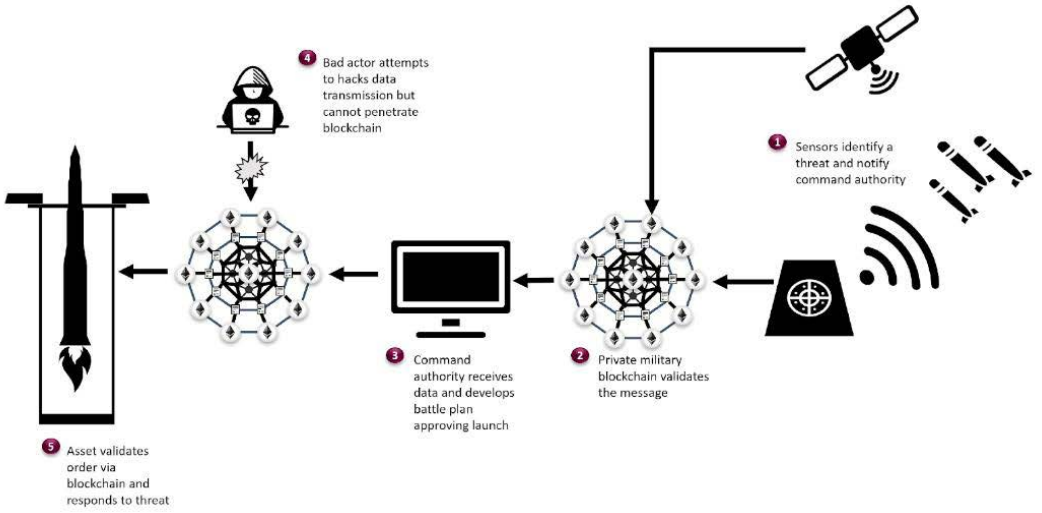


Now consider a similar scenario, but instead we substitute a blockchain-based, decentralized command-and-control infrastructure. In this case, the bad actor would need to not only access one computer system, but in essence the entire network of interconnected blockchain nodes simultaneously to interrupt the data transmission. In addition, any attempt to manipulate the data transmission or publish errant data to the blockchain would be immediately rejected by the honest nodes on the network through the chosen distributed consensus protocol.[6]

This hypothetical scenario is not entirely farfetched. Despite our best efforts to modernize and harden our command-and-control systems from a cybersecurity standpoint, many of our weapon systems have been in service for over a decade and continue to operate on outdated, legacy technologies. As bad actors continue to improve the complexity of their methods, it will become increasingly more difficult for cy-

6 Victoria Adams, "Why Military Blockchain is Critical in the Age of Cyber Warfare," March 5, 2019, https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619

ber defenders to protect our cyberspace terrain without the aid of advanced technologies like the blockchain.



Why Must We Act Now?

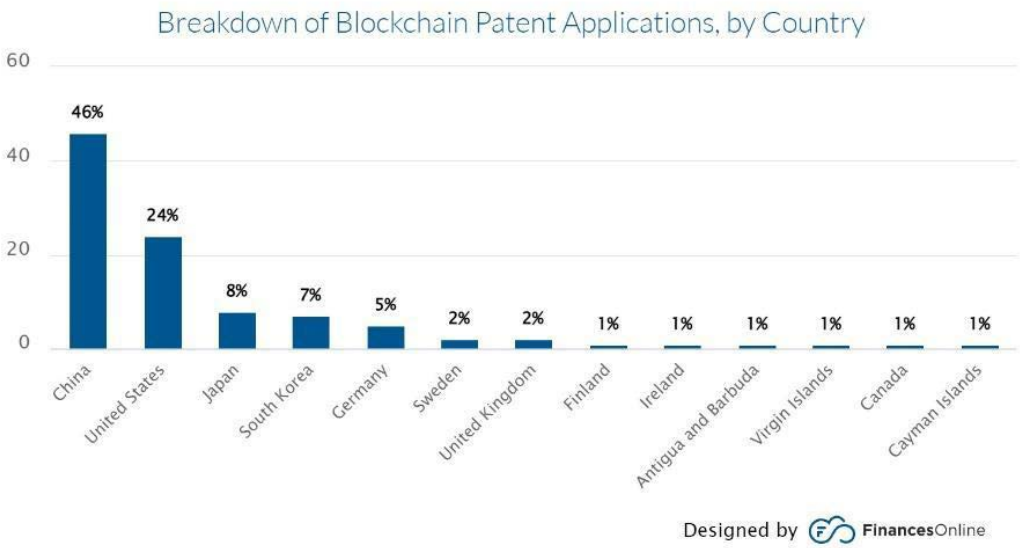
In an era of Great Power Competition, the U.S. Department of Defense is quickly falling behind our near-peer competitors when it comes to incorporating blockchain technology at scale. As of January 2020, Chinese companies had filed over 10,000 blockchain related patents with the China National Intellectual Property Administration (CNIPA)—the Chinese equivalent of the U.S. Patent and Trademark Office (USPTO).[7] This equates to roughly 46% of global patent applications related to blockchain technology and is nearly double the number of patents filed in the United States.[8]

Additionally, in March 2020, the Chinese Government along with a consortium of Chinese banks and technology companies launched the Blockchain Service Network (BSN)—one of the first blockchains globally to be built and maintained by a central government.[9] Unlike the majority of early blockchains that operate publicly under a decentralized and permissionless system, access to China's BSN blockchain will be limited to only parties which have been granted appropriate permissions and transactions on the blockchain will not be publicly viewable to all participants. While a permissioned setup makes sense for an access-controlled, hardened classified network in use by a government organization like

7 Forkast News, "China is leading the global blockchain patent race," January 2020, https://forkast.news/china-is-leading-the-global-blockchain-patent-race/

8 Nestor Gilbert, "51 Critical Blockchain Statistics," January 2022, https://financesonline.com/blockchain-statistics/

9 Nick Stockton, "China Launches National Blockchain Network in 100 Cities," March 2020, https://spectrum.ieee.org/china-launches-national-blockchain-network-100-cities



the U.S. Department of Defense, the BSN is instead marketed as a solution for broad commercial use cases. The lack of transparency over BSN blockchain transactions and overt control by the Chinese central government presents a significant risk that this medium will be used as a tool to collect on network participants, including potentially logistics and supply chain vendors of the U.S. defense industrial base.[10] It is no secret that President Xi Jinping intends to expand the BSN abroad, with a goal of creating a Chinese-controlled, blockchain-based, global infrastructure network—complete with its own central bank controlled cryptocurrency[11]—to give China a "new industrial advantage"[12] in the modern era. A delay by the U.S. Department of Defense to invest in the development and incubation of blockchain technologies will allow near-peer competitors like China to establish significant global market share and quickly propel them into a position as the partner of choice among countries in key strategic locations around the globe.

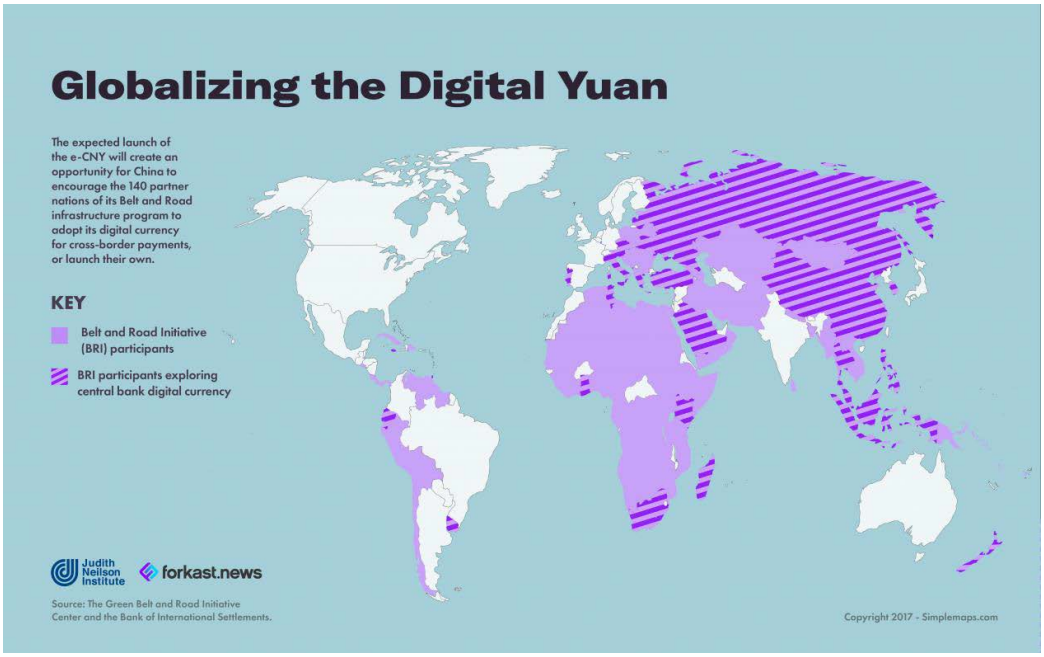
On May 13th, 2021, the People's Republic of China released their 14th Five-Year Plan for National Economic and Social Development, which for the first time indicates blockchain as a key accelerator for future economic development.[13] China's heavy invest-

10 Trevor Logan and Theo Lebryk, "America and its Military Need a Blockchain Strategy," April 2021, https://www.c4isrnet.com/opinion/2021/04/05/america-and-its-military-need-a-blockchain-strategy/

11 Alexander Zaitchik, Jeanhee Kim and Kelly Le, "Globalizing the Digital Yuan," June 2021, https://forkast.news/video-audio/part-ii-the-new-silk-road/

12 Miranda Wood, "Chinese President XI Jinping Emphasizes Importance of the Blockchain," October 2019, https://www.ledgerinsights.com/chinese-president-importance-of-blockchain/

13 Center for Security and Emerging Technologies, "Outline of the People's Republic of China



ments into blockchain technology over the past five years, and now stated intensions to continue investment for the next five, should serve as a warning to U.S. cybersecurity and defense officials. We are quickly yielding precious battlespace in the cyberspace domain of tomorrow with each passing day by delaying Department of Defense investment into developing blockchain technologies as a part of our defensive cyber infrastructure.

Recommendations & Conclusion

For the Department of Defense, the intelligence community, and our allies to maintain strategic technological advantage in the Cyber Domain, we must begin to invest our time and resources into developing blockchain-based technology solutions for military applications. To the maximum extent possible, we should examine and leverage best practices and lessons learned from other federal agencies, the defense industrial base, and our partners/allies in cases where blockchain technologies have already been implemented successfully. Additionally, in the traditions of ARPANET and SpaceX, we should continue to foster the Department of Defense relationships with public/private universities and technology companies to accelerate development of the blockchain-based cybersecurity infrastructure of the future.

14th Five-Year Plan for National Economic and Social Development," May 2021, https://cset.georgetown.edu/publication/china-14th-five-year-plan/

LCDR Dorian Belz holds a BS in Systems Engineering from the U.S. Naval Academy and is a graduate of the U.S. Naval War College and Joint C4I/Cyber Course at the Joint Forces Staff College. His 15-year naval career includes aircraft carrier deployments as an SH-60F helicopter pilot, headquarters assignments on the Korean Peninsula and at the Pentagon, and several years serving as an operations briefer for the Chief of Naval Operations and Secretary of the Navy. He transitioned to the Navy Reserves in early 2019 and began a civilian career as a technology consultant working for Ernst & Young, LLP. His professional focus areas include data management and analytics, data governance and quality controls, data privacy and security, and architecture design.