Data You Can Trust

Blockchain Technology

Col Vincent Alcazar, USAF, Retired

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the Air and Space Power Journal requests a courtesy line.

> *They say that coming events cast their shadows before. May they not sometimes cast their lights before?*
>
> —Augusta Ada King–Noel, Countess of Lovelace

The Case for Change

America's military continues its wait for network-centric warfare (NCW) breakthroughs to deliver technological leadership and war-fighting advances that revolutionize the American way of battle. Instead, in the past decade the US military got artifacts: Internet access, laptop computing, the introduction of smartphones, and so forth. The artifacts of technological advancement are often misidentified as the anticipated NCW breakthroughs. At their core, those artifacts are iterative device and machine productivity improvements. If NCW has an insidious weakness, it is its hardware orientation. The focus on artifacts begs a question: what about the data that is transported within the hardware, devices, networks, and associated infrastructure? Despite advancements in technologies and processes, today's software and hardware shells—the things that surround and distribute data—remain chronically vulnerable. Among history's recurring insights is that a military's vulnerabilities—hidden or acknowledged—can become linchpins in an opponent's campaign of surprise. However, surprise need not be strategic to impede the American way of battle. What is to be done?

Against the backdrop of US data vulnerabilities and potential susceptibility to cyberspace surprise, warriors and warrior leaders need a different approach, a big idea—a viable technology that can mitigate the weakness in the DOD's paradigm of centralized data protection. The better (big) idea should not be a continued near-exclusive focus on iterative military computing machine improvements. Instead, this better idea ought to outline a design for the enhanced security of what military information technology (IT) equipment processes, stores, and distributes: data. The better idea exists; it is blockchain technology. Concisely stated, blockchain is a technology that stores data in a way that makes it incorruptible, doing so via its integrated data ledgers. The reasons to adopt blockchain's leap-ahead technology are twofold:

avoiding downside disruption risk and maximizing upside war-fighting opportunity. Regarding downside risk, warriors need to mitigate the operational disruption and degradation resulting from an absence of authentic data, because so many of our weapons systems require data to function effectively, if at all. Blockchain's upside is that the US military could take data corruption and compromise off the table as things an enemy could do to its data. The first reason is important; the second reason is game-changing in warfare.

The development of a blockchain big idea, along with machine improvement, suggest significant growth in DOD IT costs in an era of resource limitations. However, blockchain already exists, and that saves millions of dollars in research and cuts years off a development program. Basically, blockchain is a data management and distribution technology compatible with existing DOD networks. Its game-changing design secures and inscribes data, protecting it from tampering and corruption. Blockchain frees our military from continued competition against state and nonstate actors, who as attackers have vast incentives and agile exploitation development loops that yield an uneven playing field. The unevenness of that playing field is the result of tremendously disadvantageous and deeply inefficient geometry that pits enterprise hardware/software threat mitigation that must be right all the time against a threat security environment where a determined attacker need only succeed briefly. To tilt the playing field in a way that favors America's military, the ideal solution points toward a union of blockchain technology and American computing machine/system ingenuity.

Problem, Thesis, Hypothesis

Data has become the modern military organization's critical dependency. In practice, the lack of timely, accurate data condemns a force and its leaders to operations via a method of guesswork. Generally, the guesswork method of sensing and decision making poses problems. It was a problem when the force was led by a single man sitting on horseback overlooking a battlefield. In this century, a lack of assured data opens any force to traumatic defeat in multiple domains. The paradox is that America's distributed warfare model attains its full potential when its vast, growing data appetite is fed regularly by vetted data known to be secure. The data edge users in the DOD know the problem is not the data appetite of our machines or the scale of that appetite.[1] Rather, any problem statement about the status quo would not be a one-liner but a circle drawn around a cluster of interrelated questions: what is the reliability of the data floating around in our IT systems, the data that warriors need to prosecute the fight? Has that war-fighting data been tampered with, in part or whole? Is that data truly authentic or only authentic in appearance yet actually bogus, planted by a clever attacker? Is the sender a credible entity, or is the alleged source really a system mole seeking to cause havoc? Which of those questions as problems should be solved, and in what order? Actually, warriors do not care, but the answers they hear from IT experts is to attend to all of those matters, simultaneously. And so, each of these matters is worked using separate approaches in separate silos.

Winning the fight to protect and control our IT systems requires a tremendous outlay of resources. But what if we could push all the above questions and the problems they suggest off the table by shifting the focal point of the answer? Instead of asking what could be done anew to IT systems, what if something could be done anew to the data itself? Enter blockchain—it focuses the question and answer on data. Given that, this article's thesis is that if the DOD deploys blockchain—a new and radically different data management technology—then the data attacks of today become much less damaging, with the key benefit being that the data in warriors' hands becomes exponentially more dependable by being virtually incorruptible.

Next, this article's hypothesis is that to best protect war-fighting data in US military networks, the best-known data technology solution is blockchain. Put another way; blockchain can help war fighters escape the hamster wheel of mitigating the cyber attacks we experience while incurring damage from the predation of unanticipated, undocumented, unmapped, and unknown IT hardware/software vulnerabilities.

Blockchain—An Overview

In 2008, an individual using the pen name Satoshi Nakamoto published a now well-circulated whitepaper that outlined the Bitcoin concept and its enabling bedrock system, blockchain technology.[2] Blockchain might be the first technology truly worthy of the label of disruptive data technology. Blockchain is not just a generational improvement over current data logging and documenting technologies. Its importance is its ability to remove a crucial vulnerability in our present network designs: compromise of network trust-management policies. Trust-management functions are a frequent attack target owing to the vital role they play in all cyber networks, including the ones used by the military. The trust manager controls two vital functions: user credentialing and access control. Trust management relies on a hardware device and its software to play the role of the middleman to ensure users and their data transactions remain trustworthy.[3] By targeting user credentials, an attacker can gain network entry to get at the ultimate data target set to attain the objectives of his or her attack.

The founding designers of blockchain understood the limitations inherent in the network design paradigm that require the existence of a trust manager. In creating blockchain's underlying form and logic, they pioneered a technology within a new operating framework that sets aside the numerous weaknesses of the DOD's system-based computing as warriors know it today. The following points are an overview of how and why blockchain qualifies as a disruptive technology.

Blockchain Is a New Source of Strength

Traditional secure network design vests trust-relationship management and gatekeeping roles in a central actor with complete authority within the hierarchy of the network. Blockchain removes the requirements for centralized authority by removing the need for the trust management middleman role. The absence of central control confers a scalability that makes a blockchain network capable of functioning with the same effectiveness and efficiency at any size threshold; that is, a raiding party, a large joint task force, and so forth. Another advantage of blockchain is that its decentralized structure (flatter organizations) and less centralized logic (less top-down) decrease latency. More horizontal and less vertical overcomes many of the challenges in military networks fraught with the risks of the loss of the centralized trust manager(s). In other words, making blockchain strong is not something you do to blockchain; it is blockchain.

Blockchain Flips the Data Centralization Paradigm

Advanced persistent threats (APT) and state and nonstate actors all exert substantial influence on American military network design. Those threats compel a broad defensive response that hoards data behind ever more elaborate protective walls sheltered within more layers of security. What results from this mindset of threats, defenses, and responses is a constantly expanding multiplicity of data silos. The security of data becomes its own end, and from that end flows an unintended result: the balkanization of data. To data managers, this construct reads both right and appropriate. However, to the warriors who fight battles in multiple domains and from increasingly distributed battlespace positions, silos put data—a tool of warfare—farther away and not where it ought to be in warfare, close at hand.

Blockchain Reshapes Defense of Data

Blockchain does not make all conceivable actors and threats irrelevant; no affordable military network design can. However, blockchain's structure of network miner proof of work and its distributed ledger of data transactions greatly reduce the possibility of data theft, data corruption, and sender identity compromise.[4] Additionally, blockchain's data encryption standard, SHA–256, makes backward exploitation of sender message content expensive and time-consuming. Even if an opponent could economically break the SHA–256 encryption standard, it is highly unlikely that it could do so at the speed of war; that is, fast enough to matter in a fight.[5]

Blockchain Data as a Woven Fabric

In the current vision of US military data management, data aggregates in data sinks. The very existence of storehouses of data invites attack. If one creates a construct where data is gold, one puts that pile of data at constant risk. Blockchain stands the data-hoarding paradigm on its head. Sure, data is still king, but blockchain entombs data within its arrangement of data blocks, as each is added to the blockchain network's ledgers. Altering the data contained in each block is impossible after a completed block is added to all network ledgers.

Blockchain's Decentralized Structure Complements Distributed Warfare

When temporarily disconnected from their native blockchain network, miners are not disabled, only idling as they await the next data transaction.[6] When a blockchain network reconnects to overarching networks, a block proof of work synchronization occurs. All completed data blocks are exported to every ledger. This routine is designed to ensure that when a network's miners and related machines restart, they do so in unison, on the same new data transaction. This design of blockchain is important to warriors who know that it is not a matter of if but when connectivity falters.

Blockchain, An Option to Manage a Battle Network of Objects

Blockchain's structure lends itself to management of a conceptual battle network of objects (BNO)—a militarized version of the civil Internet of things. Rather than a discreet command path for objects in the BNO, objects would connect to thousands of other BNO devices, all in a blockchain network to send and receive data that, when decrypted, is added to each object's ledger, or perhaps, to machines that host a ledger for clusters of related BNO devices. Blockchain becomes the synchronization mechanism for BNO devices in a network, regardless of its population. Blockchain eases the warrior's burden of maintaining high awareness in a battlefield full of networked objects. With blockchain, each device does not have to be prompted to affiliate with a network to learn; rather, blockchain's ledger structure ensures any device connected to the blockchain network previously learned what it needs to know.

Blockchain, An Option to Control Device Swarms

Blockchain's distributed form, coupled with the algorithms that will be engineered into swarm devices, unlocks authentic swarm behavior, thus realizing a more fully militarized potential. Blockchain could accomplish this in two ways: first, provide for a swarm memory to form a bedrock of swarm actions, and second, provide the means for swarm-to-swarm connectivity and communication. Perhaps most exciting, blockchain technology could enable varying levels of human–robot interaction. Blockchain could accomplish this through swarm memory as described above and the dynamics of emergence (swarm self-organization; both could boost swarm awareness). With elevated awareness, swarms could attain high levels of autonomy, a useful attribute in tactical scenarios where direct operator control is impractical or when operator-swarm connectivity is interrupted.[7]

Blockchain—How Does It Work?

The first Internet-public version of blockchain debuted in different places at different times, starting in late 2008 and early 2009.[8] A blockchain network can be any size, and features interconnected machines termed miners, ledger host machines, and connection points to other networks. Miners are computing machines whose task is to calculate the solution to a sophisticated equation.[9] Elliptic curve digital signature algorithm (ECDSA) is the arithmetic of blockchains, and asymmetric key cryptography is the means by which data transactions are encrypted by a sender and decrypted by a receiver using the paired public/private key method.[10] Once an ECDSA solution is successfully determined by a miner, it is converted by an algorithm into a data string 256 bits in length.[11] The data string is the payload of any given data transaction ordered by blockchain block technology. As the transaction moves from point A to point B in the network, miners in their role as receivers use their individual computing power to solve a transaction's ECDSA equation by repeatedly calculating the equation until its solution output data string matches the data string in the sender's data transaction. Once that match is made, the data block is almost complete and will quickly be eligible to be added to the ledgers—the record of all completed transactions—of every network miner and ledger host machine.[12] Paired public/private key technology protects the solution such that an attacker cannot steal or corrupt solution data within the network. One does not have to be a computer science engineer, a network administrator, or a National Security Agency cryptologist to understand what blockchain is doing: using complex ideas in simple ways to produce something more important than mere data.

Security is a cornerstone of blockchain. The digital cryptography in blockchain is so robust it would take a single desktop workstation an extensive period of time to calculate all the possibilities to hack a sender's data string.[13] The complexity of blockchain encryption can be modulated; that is, dialed up or down.[14] For military blockchain applications, this rheostat feature may prove instrumental in providing flexibility in expeditionary operations; sometimes more encryption complexity is needed, other times less complexity is more appropriate. In routine practice, it takes an average of 10 minutes for current generation blockchain network miners to solve for the standard SHA-256 encryption equation.[15] However, newer blockchain technology can reduce this computation time to three minutes. With next-generation chip speeds and the commercialization of quantum chips, it is conceivable that even today's most rapid computing velocity could be reduced by another order of magnitude (six to eight seconds). At the end of the current 10-minute calculation period, the network performs what amounts to a community synchronization process whereby all networks ledgers are updated in unison. A completed blockchain data block from the miner first to solve the equation and match the data strings—termed a proof of work—is exported to network machines as a copy and to add to each's ledger—the record of all network data transactions since its inception. Imagine the blockchain network in action; a technology that enhances our warfare style, not making that style less flexible and more brittle as we continue our pursuit of digitization.

What occurs when a data block is completed is what makes blockchain unique and superior to data management approaches in today's networks. Recall that corruption of a network's trust management function can bring network users and data into question. However, once a blockchain block is complete, the block's contents are sealed, and its data payload becomes incorruptible. The mechanics of this process are simple: a completed block is published in unison to every network machine's ledger. Concerning attack, the bottom line is that there is no convenient method for an attacker to corrupt transaction data so his recourse would be to attack an entire network. However, short of outright destruction, that network is, at worst, short-term hampered, not long-term defeated.

In military applications, it is likely that blockchain miners would work on different transactions at differing speeds, disconnect, and reconnect to their network at different times and rates. The reasons for this could be machine computational performance differences, communications instabilities, emissions control measures, or attack effects on the network. In any of these conditions, it is possible for multiple blockchains to develop—chains that could compete with the single chain of blocks. In and of themselves, multiple chains cannot be allowed to persist because of the potential for contradictory transactions of data to form in the network's data ledgers. The method to mitigate this problem is simple: miners and participating network machines identify the longest chain of blocks and seek to add future blocks only to that chain. Given the amount of data crunching that occurs on a blockchain network, miners can utilize a logic tool to keep the chain of blocks at a predetermined length. This tool eases machine demand on machine memory as the chain of blocks lengthens. Use of this tool helps to ensure that in military operations, blockchain data transaction flow rates remain at the highest possible speed.[16] The takeaway is that blockchain not only fortifies data but is sensitive to network performance.

Blockchain—What Use Could Look Like?

The following are select examples of how blockchain's organic design can be applied to broad military mission sets:

- **Operations orders and planning documents**. Blockchain's decentralization hints at a network's democratization of sorts when it comes to data. For warriors in a fight, there is nothing more democratic and pressing than the need to know the fight plan and keep up with its changes. Putting relevant aspects of a fight plan like these into the hands of war fighters is a goal of preparation and execution. Blockchain's leap ahead is its technology that ensures that data, in this case operational points, is pushed out horizontally; data is preserved in the stone that is data blocks. If some portion of the network suffers a connectivity break with a headquarters network, that senior network need only pass data blocks to a single miner of a subordinate network. In that scenario, that receiving miner will push that block and others as required to every data ledger in that blockchain network. The so-what is that fight situational awareness is reboosted, and the mission continues.
- **Device swarm control**. Designers are working on carriage systems for swarming devices—a war-fighting method that has attracted the attention of the US military—and engineers are identifying swarm device applications. The biggest challenge to swarm employment is not device design or packaging; it is control.[17] One of the key limitations of the control of hundreds, indeed thousands of devices, within a swarm is what experts call global knowledge. In other words, it is an awareness of not only adjacent devices but also shared awareness among all of the devices within the population.[18] Combined with simple operating routines programmed into each device but managed and orchestrated by the open, distributed design of a blockchain network, all that a swarm sensed would be known and knowable to all devices at the same time. The result is a swarm's ability to act as a single entity. Blockchain technology unlocks the military possibilities of swarms.
- **Logistics**. With so much logistics supply and demand data exchanged between military providers and civilian counterparts, the assurance that data is authentic—not tampered with—is paramount. Blockchain's ledger logic ensures that what is transmitted by credible senders and received by authorized

recipients can be inherently trusted. Blockchain works especially well in the world of logistics given its contracts, agreements, order forms, requisition documents, etc. Whether those logistics documents are computer generated or not, blockchain's organic logic ensures that each document remains reliable, accessible, and incorruptible.

Blockchain—Some Limitations

Vulnerabilities discovered in early laboratory experimentation were recognized and addressed; one such was the selfish miner. The selfish miner problem is based on a situation where a group of miners colludes to prevent or divert transactions for their gain; a challenge in some civilian blockchain environments. In the worst-case example of a selfish miner, a minority of rogue miners seek to recruit other miners to gradually gain the upper hand to eventually control a network. Researchers discovered two aspects of this phenomenon: first, the selfish miner problem has an upper limit whereby the rogues eventually take over the network to become the network reinvented. The second discovery was that a simple coding modification to blockchain logic eliminated selfish miner outbreaks at the outset.[19]

Engineers identified another vulnerability, a Sybil attack. This attack results when an actor adds rogue miners to a network's minor population; not to speed equation solving but to steer honest miners in that network population away from solving certain transactions. The impact of the Sybil attack is twofold: it decreases the network's pooled computational power and slows network ledger updating. Sybil attack vulnerability can be proactively eliminated by altering the single-longest blockchain preferencing behavior of miners; the logic that compels miners to add ledger blocks to only the longest existing chain. In something of a contradiction to normal operating logic, the antidote for a Sybil attack is to divide the miner population such that all miner output blocks are segregated into two discrete chains until one emerges as the longest chain—typically by a single block. When the single chain emerges, the Sybil attack is halted, the shorter chain is discarded, and the miner population resumes normal operation.

Blockchain—Answers to Limitations

To tailor blockchain best to military application, developers will map to insights learned from blockchain's infancy. Advances in artificial intelligence (AI) could be cross-leveraged to deter and suppress selfish mining as an alternative to modifying blockchain logic. Another use for AI algorithms will lie in locating anomalous miner behavior, such as the early formation of selfish mining groups.

Blockchain as a technology continues to evolve, yielding new types and potential uses. An example of such innovation, an alternative blockchain is a variant that creates blockchain networks that only look for and process specific data transaction types. Another blockchain variant is a sidechain, a special cluster of miners to solve specific kinds of transactions in purpose-built networks. In military use, alternative blockchains likely have utility in networks that carry intelligence data transactions.

AI, miners, and machines could team to filter transactions at differing classification levels in alternative blockchain networks. To expand this idea, intelligence blockchain networks would provide data to users using binned access permissions on the same network instead of using separate networks side-by-side for users cleared to different levels and programs. An added security feature would be an anonymizing browser that masks user information and other pertinent data.[20]

In field operations, block sidechains likely have a significant role. Examples include missionized networks that perform data transfer and exchange functions in support of specific missions, such as raids, occupations, high-value-target strikes, and so on. However, an important contrast must be made: current DOD networks reach down (top-down, centralized) to the tactical level. Blockchain is different; it is decentralized (horizontal). Attackers know how to defeat centralized networks and cripple the military mission—that is today's problem. Blockchain takes that problem off the table and ensures that missions are not jeopardized because of data security issues.

A future evolution, blockchain 2.0, arrived several years ago and spawned the rise of more than a dozen new commercial blockchain providers, each customizing blockchain technology to work in specific business applications that ride on various blockchain types. One such entity, ADEPT—a joint development of IBM and the Ethereum foundation—is developing blockchain for civil Internet of Things applications.[21] Ethereum's blockchain variant would overhaul the Internet from its current state to an alternative state where records, titling documents, contracts, and the like are no longer stored and possessed by third-party government or commercial entities. In this perspective, blockchain storage and accessibility applications become the twenty-first century data storage location of choice.[22] To warriors, all of this means blockchain is already taking on new forms and is sufficiently developed for tailored military applications that support our diverse missions.

Blockchain miners require extensive computing power. Adequate facilities to host miners most likely exist at steady state bases, ports, and hubs. To position miners farther forward, near war-fighting forces, militarized miner machine designs must consume less power, take up less space, and become appropriately ruggedized. There is some work to do to make blockchain components deployment ready.

Adoption—What Got Better?

Blockchain is a preexisting cryptography technology expressed in a new concept of application with a chief benefit of ensuring that war fighters maintain high confidence in the authenticity and security of the data they get from DOD networks. The bottom line is that blockchain gives war fighters what they need—trustworthy data. As a benefit, trustworthy data speaks to a concern of the war fighter—data that others cannot corrupt. Putting this notion into practical terms: in the fight, can I trust data to help mitigate cyber vulnerability and preserve operational momentum?

Is the US military aggressively pursuing blockchain development? No. The reasons are loosely rooted in skepticism of new ideas and an unclear development path. Despite the DOD's fascination with innovation, too often a "not invented here" attitude closes minds and doors to thinking and things that challenge status quo norms; think *The Structure of Scientific Revolutions* by Thomas Kuhn. Still, other DOD critics find a reason to eschew new ideas because at first glance they are not mature; neither were radar and jet propulsion technologies when they first burst onto the scene. The insight, of course, is that sometimes you must look beyond present constraints to see what a technology could eventually become. Elsewhere, the idea of better protecting the DOD's data, or at least more of it, is not viewed as credible as pouring billions of more dollars into the hardware side of America's massive military data enterprise.

Finally, there is one thing we can state categorically: acquiring data for military application is important; protecting that data is essential. Develop blockchain, then deploy it to boost data security and enhance the operating performance of every DOD weapons system it touches. ✪

Notes

[1] *Edge users* include all users outside of static command and control nodes with an emphasis on tactical users—*warfighters*, in expeditionary settings.

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," accessed 1 September 2016, http://www.bitcoin.org/bitcoin.pdf.

[3] Michael Crosby, et al., *Blockchain Technology*, Sutardja Center for Entrepreneurship and Technology, 16 October 2015, 3. Outside of the operators of networking systems, many users do not practically recognize *trust* activities in networks. Crosby, et al., cite familiar activities as the products of network middleman trust activity: verification that one's e-mail is delivered to an inbox, Facebook's verification that one's posts are only shared with friended contacts, etc.

[4] In this essay *authenticity* refers to the assurance of a given user's identity.

[5] The *Secure Hash Algorithm* (SHA)–256 standard contains a high confidence order of digits up to 256 bits in length. The SHA methodology has its roots in NSA work to improve the integrity of data strings transmitted via message protocols. By using a string of digits 256 bits in length, equivalent to 2,256 possible digital variations, a message receive can run a simple routine that looks at the SHA–256 data string of a specific file before/after transmission. The power behind the SHA–256 standard is the arithmetic power of 2,256. To get transaction processing time down to minutes, network miners compete but ultimately cooperate to pool their computational power to get the correct match—the solution. Future military blockchain applications could leverage even more robust SHA data strings, 512, 1,064, etc.

[6] Blockchain miners are special-purpose designed machines with a robust processing power to calculate the unique solution to each SHA–256 transaction data string.

[7] Blockchain will not cause devices to operate as a swarm; rather, blockchain is the means by which the swarm can attain the global knowledge within machines innate to swarming creatures in nature.

[8] Crosby, 5.

[9] Erik Rykwalder, "The Math behind Bitcoin," Next World with Michio Kaku, 19 October 2014, http://www.coindesk.com/math-behind-bitcoin/. 10. Ibid., 1. Note: ECDSA as used in blockchain is related to other elliptical curve cryptographical algorithms. The principle behind ECDSA is simple: sound cryptography turns on the principle of hack-resistant mathematical work. ECDSA is leveraged because blockchain needs public/private keys to complete a data message (transaction). In blockchain, the solution is an identification of the unique solution but the message transaction is completed when that solution is matched against the solution string encrypted by the sender. This complete, the block is time-stamped and is complete. A complete block is eligible for addition to that miner's own ledger; that complete, the miner's proof of work is validated when it is added to all that specific network's ledgers.

[11] In blockchain, the principle is: digital object (ECDSA computation) that is processed in the SHA–256 algorithm for which the resulting nearly unique data output is termed a *hash*—the digital fingerprint of the original object.

12. Ibid., 6.

13. Ibid., 8–11. On a 32-bit 20MHz clock speed workstation chip (~ 224 hashes/sec.), it is estimated that the single machine would require 139,461 years to match the 256–bit input/output data strings. Shorter I/O intervals are producible with more chip computing power. The task for militarization will be strike a balance between SHA cryptographic robustness and economy of scale chip performance in light swarm devices. Already "lighter" blockchain technologies are commercially viable with computation intervals reduced from 10 to three minutes.

14. The encryption standard of basic blockchain that supports Bitcoin is the Secure Hash Algorithm (SHA) that is 32 bytes (256 bits) in length.

15. In blockchain systems in the payments industry, the time associated with this synchronization cycle is synthetic. In military applications, it could be increased or reduced. *Litecoin* uses a 2.5-minute synchronization cycle.

16. This logic tool referred to as a *Merkle Tree*. To recover used computer disk space—memory utilized for previous computations—when the chain reaches a given length, the miner's built-in length limiter goes to work trimming the chain from older blocks. There is a deeper relationship at work here that is related to the hash coding inherent in the blocks at the bottom—where the trimming begins. As computing power at each miner node increases, the number of chains that can be retained in its respective *Merkle Tree* differs than other miner memory; however, the quantity of blocks removed from memory never exceed the minimum required to ensure undisrupted network operation.

17. Peter Coy and Olga Karif, "This Is Your Company on Blockchain," Bloomberg Businessweek, 25 April 2016, 8, accessed 2 September 2016, http://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain.

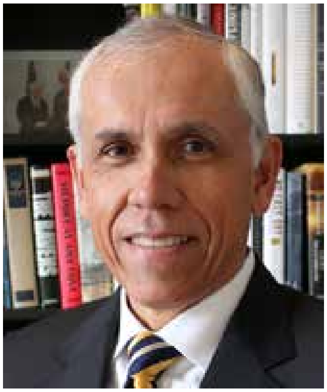
18. Eduardo Castelló Ferrer, "The Blockchain: A New Framework for Robotic Swarm Systems," (Cambridge, MA.: MIT Lab, 3 August 2016), 3, https://www.researchgate.net/publication/305807446_The_blockchain_a_new_framework_for_robotic_swarm_systems.

19. This fix is accomplished by decreasing the number of miners required to attain network consensus. In this scenario, the overall threshold is lowered; this acts as a tool to prevent selfish miners from colluding.

20. The TOR anonymizing browser is one such example.

21. *Ethereum* is a Swiss nonprofit organization, www.ethereum.org.

22. Cellabz, "Blockchain and Beyond," Cellabz, Inc., Paris, France, November 2015, Version 1.0, 16.



Col Vincent Alcazar, USAF, Retired

Colonel Alcazar retired from active duty in December 2014. During his career, he was a fighter pilot with 3,800 hours in various fighter aircraft, a joint specialized undergraduate pilot training instructor, an F-15 formal training unit instructor pilot, and commander of the 479th Flying Training Group and 479th Operations Support Squadron at Moody AFB, Georgia. A veteran of Operation Desert Storm combat missions and of Operation Iraqi Freedom deployments, he is also a former air attaché to Iraq. Colonel Alcazar is the former Air Force lead for Air-Sea Battle and a former planner and strategist with Headquarters Air Force staff experience.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

http://www.airpower.au.af.mil