


See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/325385235>

Blockchain Benefits and Risks

Article in Military Engineer · May 2018


CITATION
1

6 authors, including:




Igor Linkov
Engineer Research and Development Center - U.S. Army
430 PUBLICATIONS 7,257 CITATIONS
[SEE PROFILE](#)


READS
159



Benjamin Trump
Engineer Research and Development Center - U.S. Army
47 PUBLICATIONS 263 CITATIONS
[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:

- 

Side projects [View project](#)
- 

Tradespace Tools [View project](#)



Blockchain Benefits and Risks

As the Defense Department evaluates the implementation of blockchain technologies, proactively developing related governance now will help ensure that their long-term impacts are consistent with the military's needs and missions.

By Igor Linkov, Ph.D., M.SAME, Emily Wells, Benjamin Trump, Ph.D., Zachary Collier, Simon Goerger, Ph.D., and James H. Lambert, Ph.D.

Blockchain technologies are being considered as solutions to various cybersecurity and information technology threats and challenges. The Department of Defense (DOD) is evaluating blockchains for current and potential uses. However, before such decentralized technologies can be widely adopted, it is essential to understand how they align with military command structures and missions.

Blockchain methods—formally referred to as distributed ledger technologies—enable live, interconnected transaction records with data access and disclosure to all members of a network. Built upon a cryptographic framework, blockchains can provide an audit trail that is irreversible, preventing past transactions from being modified. Blockchains are decentralized.

This novel approach has become known through informal currencies such as Bitcoin; but in any application, it revolutionizes the visibility of transactional data by increasing transparency and security while decreasing opportunities for improper use of a network.

No longer exclusively used by innovative cryptocurrencies, the 2018 *National Defense Authorization Act* mandates an assessment of the offensive and defensive cyber applications of blockchains for intelligence and homeland security purposes. Some defense blockchain applications are already underway. Research and assessment has current DOD support—and many possible future options pose interest.

DOD is considering whether to harness

blockchains to facilitate operational capacities in domains such as active supply chain management, equipment replacement and repair, and communications and messaging. Blockchain technologies may also be viable in helping establish microgrids on military bases. This could help meet service energy consumption reduction goals. While this approach may increase transparency and security across DOD and other U.S. government networks,

Technologically, blockchains require frequent system updates, which requires users to continuously update their ledger in tandem with the larger system.

overhauling the current system with blockchains will introduce new governance challenges and potential concerns for the command structure and established military doctrine. Clearly, significant discussion is needed regarding whether such technologies align with military objectives, and decision support may be required to adequately evaluate various tradeoffs associated with the use of these emerging technologies and complex infrastructure.

Senior DOD officials may reserve the right to decide, but the involvement of multiple stakeholders in industry, academia, and other sectors can add visibility into technological and administrative limitations and advances blockchain systems will face in the near future.

These considerations are critical for DOD and other agencies to assess, as the potential challenges associated with

the development and implementation of blockchains are likely to be quite different from other types of innovation.

RECENT IMPLEMENTATION

DOD has already funded projects that utilize blockchain technologies across various domains, including supply chain management, equipment and energy management, and communications and messaging. As the first U.S. defense contractor to incorporate blockchain networks into development processes, Lockheed Martin contracted with Guardtime Federal to integrate cyber-related elements to systems-engineering processes, supply-chain risk management, and software development efforts. Lockheed Martin and Guardtime Federal are designing non-traditional cyber security systems into DOD business transactions through a concept known as cyber-aware systems engineering, with the stated intent to “enhance data integrity,

speed problem discovery and mitigation, and reduce the volume of regression testing.”

Incorporating blockchains within the military supply chain will streamline the system by allowing agencies to order only the components they need to enhance front-end operations, rather than expending funds and wait-time on full assemblies. Known as additive manufacturing, DOD can harness 3D printing capabilities to produce military-standard parts on site.

In conjunction with additive manufacturing, the U.S. Navy is turning to blockchain technologies that could resolve issues surrounding intellectual property rights when producing military-standard parts in the field. 3D printing has enabled DOD to print parts and equipment on location; blockchain ledgers would help securely log every print that is produced in the field. The ledger ensures that the



contactor is fully paid for their print, respecting commercial intellectual property while supporting the warfighter.

Beyond supply chain risk management and additive manufacturing, blockchain technologies have been proposed to fundamentally transform the energy grid. Private sector firm LO3 Energy implemented a peer-to-peer energy transaction system, the Brooklyn Microgrid, that uses blockchain technology to support a small utility grid that can function even if the standard utility grid experiences an outage. Energy users that opt in to this grid are interconnected. Users share and consume local, green energy (such as energy derived from a user's solar panel) through decentralized neighbor-to-neighbor transactions. A localized energy grid application of the technology could be implemented on military installations to establish more resilient renewable energy production and consumption, in the event base facilities are connected through a blockchain network.

AWARENESS OF CHALLENGES

Despite the security and resource benefits that blockchains may offer, the technology introduces various concerns to DOD command and control operational practices. These challenges are generally manifested in implementation, governance, and technological limitations associated with proposed blockchains. Technologically, blockchains require frequent system updates, which requires users to continuously update their ledger in tandem with the larger system. Interoperability, especially with legacy systems, is another critical technological issue necessitating new communications protocols and business models.

Administratively, such frequent updates may require rule changes to blockchain governance, something that is complicated due to a lack of a central command structure with the responsibility to identify and implement such tactical or strategic changes. These rule changes require a semi-democratic voting process, where each individual's vote is grounded in perception of technological limitations and system needs within an environment of high uncertainty and human judgment.

Though distributed ledgers can help

provide greater transparency and security within certain sensitive processes, these potential limitations must be addressed to head off any potential degradation of military operations and readiness.

Beyond the technical implementation and limitations, governance and oversight of blockchains may challenge the current DOD decision-making structure. While decentralization may benefit systems such as Bitcoin, it is contrary to the traditional military structure that is inherently hierarchical. Starting a new decentralized structure may disrupt operations when DOD needs to quickly respond to a threatening situation.

Blockchain technology requires agreement across multiple nodes (users), which could either speed or slow an operative system that currently relies on rapid-response hierarchical decision-making. Prior to relying on blockchains, DOD should consider how to quickly patch across multiple nodes to ensure that the response of a system to a threat is not burdened by the structure of the system itself. Moreover, network-wide transparency, which is an important benefit in civilian applications, can become a concern when sensitive information is transmitted. Proper controls and access must be built into the network to ensure only those with proper credentials can access and update the blockchain.

THE NEED FOR GOVERNANCE

While blockchain technologies offer exciting possibilities for data transparency, DOD and any government agency involved with the current assessment mandated by Congress must consider the limitations and risks imposed by this technology.

Experts recommend that DOD proactively develop governance of

SECURED COMMUNICATIONS

In addition to enhancing physical supply chains and equipment capabilities, DOD is interested in incorporating blockchains into communication and messaging systems. A 2016 notice from the Defense Advanced Research Projects Agency (DARPA) called for a secure messaging platform that enables participants to send and receive secure messages using a “decentralized backbone.” Decentralization would allow any member of the network to send a secure message or other transaction across multiple traceable channels.

One such 2017 DARPA grant was awarded to Indiana Technology and Manufacturing Companies to develop a secure messaging application that integrates a blockchain network. The goal of the application is to be robust, efficient, and more secure for DOD communications, including communications between active troops in the field and headquarters, as well as between intelligence officers and those working in the Pentagon. Because the application is designed to be decentralized, it is more secure from hackers as all messaging and transaction can be traced across multiple channels.

Blockchain technologies may also be viable in helping establish microgrids on military bases.

blockchain technologies and ensure that they are consistent with the military's needs and missions, especially those that promote readiness and resilience. If governance is not developed prior to implementation, blockchains may significantly alter command structure, potentially disrupting the department's operations.

TME

Igor Linkov, Ph.D., is Risk and Decision Science Team Lead, Emily Wells, is Environmental Engineering Researcher, Benjamin Trump, Ph.D., is Oak Ridge Institute for Science and Education Postdoctoral Research Fellow, and Simon Goerger, Ph.D., is Director of the Institute for Systems Engineering Research, U.S. Army Engineer Research & Development Center. They can be reached at igor.linkov@usace.army.mil; emily.m.wells@usace.army.mil; benjamin.d.trump@usace.army.mil; and simon.r.goerger@usace.army.mil.

Zachary Collier is a Doctoral Candidate, and James Lambert, Ph.D., is Research Professor of Systems & Information Engineering, University of Virginia. They can be reached at zac4nf@virginia.edu; and lambert@virginia.edu.